Приложение № 4
к приказу от 31.08.2017 г. № 132 о.
Утверждаю
Директор ЛГ МАОУ «СОШ № 4»
Т.А. Панферова
«___» _____ 2017 г.

ИНСТРУКЦИЯ

по работе с электронной цифровой подписью
в ЛГ МАОУ «СОШ № 4»

1. Общие положения

Инструкция разработана для сотрудников ЛГ МБОУ «СОШ № 4»в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи», Типовыми требованиями по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСБ РФ 21 февраля 2008 г. № 149/6/6-622) и иными нормативными правовыми актами Российской Федерации.

2. Пользователи средствами электронной цифровой подписи обязаны:

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

обеспечить сохранность личных печатей, ключей от помещений и хранилищ;

обеспечить конфиденциальность ключей электронных подписей;

выполнять указания ответственного пользователя;

не разглашать информацию об средствах ЭЦП, 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 цифровой подписи (далее - пользователей), эксплуатационной и технической документации к ним, ключевых документов;

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

по окончании рабочего дня режимное помещение и установленные в нем хранилища закрыть, хранилища опечатать. Находящиеся в пользовании ключи от 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 ЭЦП, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием средств ЭЦП;

немедленно сообщено ответственному пользователю о возможном несанкционированном проникновении в режимные помещения или хранилища посторонних лиц;

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

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

3. Ответственный пользователь обязан:

обеспечить функционирование и безопасность средств ЭЦП;

осуществлять текущий контроль за организацией и обеспечением функционирования средств ЭЦП;

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

осуществлять учет лиц, допущенных к работе со средствами ЭЦП;

осуществлять контроль за соблюдением условий использования средств ЭЦП;

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

осуществлять допуск пользователей к работе со средствами ЭЦП по решению руководителя компании;

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

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

по окончании рабочего дня закрыть и опечатать режимные помещения и сейфы.

4. Учёт средств электронной цифровой подписи.

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

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

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

5. Хранение средств электронной цифровой подписи.

Хранение средств ЭЦП, 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 ЭЦП, эксплуатационной и технической документации должно осуществляется раздельно.

6. Передача средств электронной цифровой подписи.

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

Передача средств ЭЦП, 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.

7. Уничтожение средств электронной цифровой подписи.

Ключевые документы уничтожаются либо ответственным пользователем, либо пользователями на месте (по указанию ответственного пользователя) с внесением изменений в соответствующих журналах поэкземплярного учета и лицевых счетах. Уничтожение большого объема ключевых документов может быть оформлено актом.

Уничтожение средств ЭЦП (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) средств ЭЦП (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 ЭЦП уничтожают по решению руководителя, владеющего средствами ЭЦП, с уведомлением организации, ответственной за ведение поэкземплярного учета средств ЭЦП.

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

8. Компрометация и потеря средств электронной цифровой подписи.

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

В случае компрометации средств ЭЦП 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 ЭЦП, 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 ЭЦП, если при этом исключалась возможность их копирования (чтения, размножения).

В случаях потери, недостачи или непредъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

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

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

Режимные 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 режимные помещения, под расписку в журнале учета хранилищ. Дубликаты ключей от входных дверей таких помещений следует хранить в сейфе ответственного пользователя.

Окна режимных 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 режимные помещения посторонних лиц, необходимо оборудовать металлическими решетками (ставнями) и системой предотвращения просмотра извне.

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

Ответственный за обработку персональных данных **И.Ш. Андреева**