Частное профессиональное образовательное учреждение
«Магнитогорский колледж современного образования»

Рассмотрено
на Педагогическом совете

Протокол № 5 от 20.04 2020

Принято
С учетом мнения родителей (законных представителей) и обучающихся
Советом колледжа

Протокол № 3 от 30.04 2020

Утверждено

Приказом № 21 от 11.04 2020

Директор ЧПОУ «Магнитогорский колледж современного образования»
_____С.А. Кузьмина

ПОЛОЖЕНИЕ

О РЕАЛИЗАЦИИ И ЭКСПЛУАТАЦИИ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ (СКЗИ) В ЧПОУ «МАГНИТОГОРСКИЙ КОЛЛЕДЖ СОВРЕМЕННОГО ОБРАЗОВАНИЯ»

Магнитогорск, 2020г.

1. Общие положения

1.1. Настоящее Положение разработано на основании:

- Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказа ФСБ РФ от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- Приказа ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции 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».

1.2. Положение определяет порядок реализации и эксплуатации средств криптографической защиты информации (далее – СКЗИ) в целях обеспечения информационной безопасности в системах электронного документооборота образовательной организации.

1.3. Криптографические ключи используются для обеспечения конфиденциальности, авторства и целостности электронных документов.

1.4. Пользователями СКЗИ являются сотрудники образовательной организации, в силу своих функциональных обязанностей участвующие в процессах работы со средствами криптографической защиты информации (далее – пользователи).

1.5. Из числа пользователей приказом руководителя образовательной организации назначается ответственное лицо.

1.6. Допуск пользователей к работе со СКЗИ осуществляется по приказу руководителя образовательной организации.

1.7. Непосредственно к работе с СКЗИ пользователи допускаются только после соответствующего обучения.

1.8. Организация обучения и контроль допуска пользователей к СКЗИ возлагаются на ответственное лицо.

1.9. К обучению пользователей с санкции руководителя образовательной организации могут быть привлечены сторонние лица и организации на основании договоров об оказании услуг.

2. Размещение, специальное оборудование, охрана и организация режима в помещениях, в которых установлены СКЗИ и/или хранятся криптографические ключи

2.1. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ и/или хранятся криптографические ключи (далее – спецпомещения), должны исключать возможность неконтролируемого доступа и использования СКЗИ посторонними лицами, а также наблюдения посторонними лицами за проходящими в спецпомещениях работами.

2.2. Спецпомещения должны иметь прочные входные двери с замками, гарантирующими надежную изоляцию в нерабочее время.

2.3. Окна спецпомещений, расположенных на первых и последних этажах зданий, около пожарных лестниц и т.п., должны быть оборудованы металлическими решетками и/или охранной сигнализацией.

2.4. В спецпомещениях для пользователей СКЗИ необходимо установить надежно запираемые шкафы/ячейки индивидуального пользования, оборудованные приспособлениями для опечатывания.

2.5. Аппаратные средства, с помощью которых осуществляется штатное функционирование СКЗИ, должны быть опечатаны (опломбированы). Место опечатывания (опломбирования) аппаратных средств должно располагаться так, чтобы его можно было визуально контролировать.

3. Правила изготовления, учета и хранения СКЗИ и криптографических ключей

3.1. Криптографические ключи формируются на отчуждаемый ключевой носитель (ruToken, eToken) в соответствии с эксплуатационно-технической документацией на СКЗИ.

3.2. СКЗИ, криптографические ключи подлежат поэкземплярному учету.

3.3. Поэкземплярный учет ведет ответственное лицо в специальном журнале учета/реестре образовательной организации установленной формы (Приложение к настоящей Инструкции).

3.4. Единицей поэкземплярного учета криптографических ключей считается ключевой носитель.

3.5. Все полученные экземпляры СКЗИ, криптографические ключи выдаются ответственным лицом пользователям под роспись в специальном журнале учета/реестре. Пользователи несут персональную ответственность за сохранность полученных СКЗИ.

3.6. Криптографические ключи совместно с описью хранятся у пользователей в сейфах (шкафах, ящиках) в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренную порчу/уничтожение.

3.7. Дистрибутивы СКЗИ на носителях, эксплуатационная и техническая документация к СКЗИ, инструкции хранятся у ответственного лица.

3.8. При необходимости (длительное отсутствие пользователя при заболевании, отпуске, командировке и пр.) криптографические ключи сдаются на временное хранение ответственному лицу.

3.9. Плановую смену криптографических ключей следует проводить не менее, чем за две недели до истечения срока действия сертификата пользователя.

3.10. Для пересылки СКЗИ помещаются в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия. Упаковка опечатывается таким образом, чтобы исключалась возможность извлечения из нее содержимого без нарушения упаковки и оттиска печати.

3.11. При пересылке СКЗИ, эксплуатационной и технической документации к ним, составляется акт приема-передачи/опись документов, в котором указывается что посылается, в каком количестве, учетные номера СКЗИ. Акт приема-передачи/опись вкладывается в упаковку, по получении сверяется.

3.12. Неработоспособные ключевые носители подлежат уничтожению.

3.13. Уничтожение производится под контролем ответственного лица в соответствии с требованиями эксплуатационной и технической документации на соответствующие СКЗИ. По факту уничтожения составляется акт об уничтожении криптографических ключей и ключевых документов, с отметкой об уничтожении в соответствующем журнале/реестре.

3.14. Криптографические ключи, в отношении которых возникло подозрение в компрометации, немедленно выводятся из действия в соответствии с правилами, изложенными в настоящем Положении. О выводе криптографических ключей из действия составляется акт с отметкой в соответствующем журнале/реестре.

4. Правила использования СКЗИ и криптографических ключей

4.1. Конфиденциальность электронных документов обеспечивается путем шифрования. Авторство и целостность электронных документов обеспечивается путем создания электронной цифровой подписи пользователя.

4.2. Пользователь может выполнять криптографические операции используя только действующие криптографические ключи.

4.3. При установке программного обеспечения СКЗИ следует использовать только лицензионное программное обеспечение и обеспечить контроль целостности и достоверность дистрибутива СКЗИ.

4.4. При использовании СКЗИ на ПЭВМ, подключенных к общедоступным сетям связи, для исключения возможности несанкционированного доступа необходимо использовать дополнительные методы и средства защиты, предпочтительно имеющим сертификат уполномоченного органа.

4.5. Права и обязанности пользователя/ответственного лица определяются Инструкцией пользователя средств криптографической защиты информации.

5. Действия при компрометации криптографических ключей

5.1.К событиям, связанным с компрометацией ключей, относятся:

- потеря ключевых носителей (в т.ч. с их последующим обнаружением);

- нарушение правил хранения и уничтожения закрытого ключа;
- возникновение подозрений на утечку информации или ее искажение в информационной системе;
- нарушение печати на сейфе с ключевыми носителями;
- отрицательный результат при проверке электронной цифровой подписи документа;
- несанкционированное копирование ключевых носителей;
- случаи, когда нельзя достоверно установить, что произошло с носителями, содержащими ключевую информацию (в том числе случаи, когда носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате злоумышленных действий) и пр.

5.2. При указанных в п. 5.1 обстоятельствах пользователь обязан немедленно прекратить обмен электронными документами с использованием скомпрометированных криптографических ключей и сообщить о факте компрометации ответственному лицу.

5.3. Использование СКЗИ может быть возобновлено только после ввода в действие другого криптографического ключа взамен скомпрометированного.

5.4. Скомпрометированные ключи подлежат уничтожению.

5.5. Расследование факта компрометации должно проводиться на месте происшествия специально назначаемой комиссией во главе с ответственным лицом.

5.6. Для восстановления конфиденциальной связи после компрометации ключей пользователь обращается к ответственному лицу для регистрации вновь изготовленных/резервных ключей. Регистрация новых ключей осуществляется как при плановой смене ключей.

6. Ответственность

Пользователи и ответственные лица несут ответственность:

6.1. За неисполнение или ненадлежащее исполнение своих должностных обязанностей, предусмотренных настоящим Положением, – в пределах, определенных действующим трудовым законодательством Российской Федерации.

6.2. За причинение материального ущерба работодателю – в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

6.3. За правонарушения, совершенные в процессе осуществления своей деятельности, – в пределах, определенных действующим административным, уголовным, гражданским законодательством Российской Федерации.

Приложение к Положению о реализации и эксплуатации средств криптографической защиты информации (СКЗИ)

Форма журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов

№	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров ключевых документов	Отметка о получении	
				От кого получены	Дата и номер сопроводительного письма.
1.	2.	3.	4.	5.	6.

Отметка о выдаче		Отметка о подключении (установке) СКЗИ		
Ф.И.О пользователя СКЗИ	Дата и расписка в получении	Ф.И.О. сотрудника, проводившего установку	Дата установки и подписи лиц, произведших установку	Номера аппаратных средств, в которые установлены СКЗИ
7.	8.	9.	10.	11.

Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Дата изъятия (уничтожения)	Ф.И.О. сотрудника, проводившего изъятие (уничтожение) СКЗИ	Номер Акта или расписка об уничтожении	
12.	13.	14.	15.