СОГЛАСОВАНО:
Председатель ПК
_____/Е.Г. Загуляева/
«30» 12 2019г.

УТВЕРЖДАЮ:
Заведующий МБДОУ-детский сад № 2 «Ягодка»
_____/Н.В. Савакова/
«30» 12 2019г.

МБДОУ-д/с № 2 «Ягодка»

ИНСТРУКЦИЯ

администратора средств криптографической защиты информации (СКЗИ)

1. Термины и определения
1.1 В настоящей Инструкции по эксплуатации средств криптографической защиты информации в Администрации применяются следующие термины и определения:
а) безопасность эксплуатации СКЗИ - совокупность мер управления и контроля, защищающая СКЗИ и криптографические ключи от несанкционированного (умышленного или случайного) их раскрытия, модификации, разрушения или использования;
б) Администратор (ответственный за эксплуатацию) СКЗИ – работник, осуществляющий организацию и обеспечение работ по техническому обслуживанию СКЗИ и управление криптографическими ключами (далее – Администратор СКЗИ).
в) Пользователь СКЗИ – работник Администрации, который использует СКЗИ;
г) средства криптографической защиты информации (СКЗИ) - совокупность программно-технических средств, обеспечивающих применение шифрования при осуществлении электронного документооборота, в том числе программное обеспечение с реализацией криптографических функций.

2. Общие положения
2.1 Настоящая Инструкция определяет:
а) порядок учета, хранения и использования СКЗИ и криптографических ключей, а также порядок их изготовления, смены, уничтожения в целях обеспечения безопасности эксплуатации СКЗИ;
б) обязанности, права и ответственность Администратора СКЗИ.
2.2 Все действия с СКЗИ осуществляются в соответствии с эксплуатационной и технической документацией на СКЗИ.
2.3 Администратор СКЗИ назначается и смещается распоряжением администрации.

3. Основные обязанности Администратора СКЗИ
3.1 Администратор СКЗИ обязан:
а) вести поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним;
б) вести учет Пользователей СКЗИ;
в) осуществлять контроль за соблюдением условий использования СКЗИ в

соответствии с эксплуатационной и технической документацией на СКЗИ и настоящей Инструкцией;
г) вести расследование и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению требуемого уровня безопасности информации;
г) осуществлять разработку и принятие мер по предотвращению возможных негативных последствий подобных нарушений.
д) не разглашать конфиденциальную информацию, к которой допущен, рубежи ее защиты, в том числе сведения о криптографических ключах;
е) соблюдать требования к обеспечению безопасности конфиденциальной информации при использовании СКЗИ;

4. Допуск к эксплуатации СКЗИ
4.1 Обучение Пользователей СКЗИ правилам работы с СКЗИ осуществляет Администратор СКЗИ.
4.2 Администратор СКЗИ должен иметь соответствующий документ о квалификации в области эксплуатации СКЗИ.
4.3 Непосредственно к работе с СКЗИ пользователи СКЗИ допускаются после обучения и выдачи соответствующего заключения. Заключение о прохождении тестирования оформляется в 2-х экземплярах. Для получения заключения необходимо зарегистрироваться на сайте Оператора и пройти тестирование на знание правил работы со СКЗИ.
4.4 Администратор СКЗИ должен быть ознакомлен с настоящей Инструкцией под роспись.

5. Учет и хранение СКЗИ и криптографических ключей
5.1 СКЗИ, эксплуатационная и техническая документация к ним, криптографические ключи подлежат поэкземплярному учету.
5.2 Поэкземплярный учет СКЗИ ведет Администратор СКЗИ в журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним (далее – Журнал) согласно приложению №1 к настоящей Инструкции.
5.3 Все полученные экземпляры СКЗИ, криптографических ключей должны быть выданы под роспись в Журнале Пользователям СКЗИ, несущим персональную ответственность за их сохранность. При необходимости Пользователю СКЗИ выдается документация по эксплуатации СКЗИ с последующим возвратом Администратору СКЗИ.
5.4 Дистрибутивы СКЗИ на носителях, эксплуатационная и техническая документация к СКЗИ, инструкции хранятся у Администратора СКЗИ. Криптографические ключи хранятся у Пользователей СКЗИ. Хранение осуществляется в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.
5.5 Резервные криптографические ключи находится на хранении у Администратора СКЗИ.
5.6 Ключевые носители подлежат обязательной маркировке (если это возможно) с изготовлением наклейки, содержащей реквизиты регистрации из Журнала и/или сертификата.

5.7 Неработоспособные ключевые носители подлежат уничтожению. Уничтожение оформляется актом (приложение №2 к настоящей Инструкции).
5.8 Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно-программные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать.
5.9 Ключевые носители совместно с Журналом должны храниться в запираемом шкафу, сейфе (металлическом шкафу), как правило, в отдельной ячейке. В исключительных случаях допускается хранить ключевые носители и Журнал совместно с другими документами, при этом ключевые носители и Журнал должны быть помещены в отдельную папку.
5.10 На время отсутствия Администратора СКЗИ распоряжением Администрации должен быть назначен работник его замещающий.

6. Использование СКЗИ и криптографических ключей
6.1 Факт готовности эксплуатации СКЗИ оформляется актом о готовности эксплуатации СКЗИ (приложение №3, к настоящей Инструкции).

7. Изготовление и плановая смена криптографических ключей
7.1 Изготовление криптографических ключей производиться Администратором СКЗИ в присутствии Пользователя СКЗИ.
7.2 Криптографические ключи изготавливаются на отчуждаемый ключевой носитель (дискету, ruToken, EToken и др.) в соответствии с эксплуатационно-технической документацией на СКЗИ и требованиями безопасности, установленными настоящей Инструкцией.
7.3 В целях обеспечения непрерывности проведения работы плановую смену криптографических ключей следует производить заблаговременно.
7.4 Переход на новые криптографические ключи Пользователь СКЗИ выполняет самостоятельно в соответствии с эксплуатационной документацией на СКЗИ. Переход на новые криптографические ключи осуществляется в сроки, указанные в сертификате ключа подписи.
7.5 При замене криптографических ключей используют программное обеспечение в соответствии с документами по эксплуатации. Пользователь СКЗИ обязан самостоятельно обновить сертификат ключ подписи. Обновление справочников сертификатов ключей производится путем добавления новых сертификатов ключей подписи из файлов, содержащих сертификаты ключей подписи, предоставляемых Администратором СКЗИ. Обновление справочников сертификатов ключей подписи осуществляется в соответствии с эксплуатационной документацией на СКЗИ.

6. Действия при компрометации криптографических ключей
8.1 Под компрометацией криптографического ключа понимается утрата доверия к тому, что данный ключ обеспечивает однозначную идентификацию Владельца и конфиденциальность информации, обрабатываемой с его помощью. К событиям, связанным с компрометацией действующих криптографических

ключей, относятся:
а) утрата (хищение) НКИ, в том числе – с последующим их обнаружением;
б) увольнение (переназначение) работников, имевших доступ к ключевой информации;
в) передача секретных ключей по линии связи в открытом виде;
г) нарушение правил хранения криптоключей;
д) вскрытие фактов утечки передаваемой информации или её искажения (подмены, подделки);
е) отрицательный результат при проверке наложенной ЭЦП;
ж) несанкционированное или безучётное копирование ключевой информации;
з) все случаи, когда нельзя достоверно установить, что произошло с НКИ (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута вероятность того, что данный факт произошел в результате злоумышленных действий).
8.2 События 6.1.(а-д) должны трактоваться как безусловная компрометация действующих ключей. Остальные события требуют специального расследования в каждом конкретном случае.
8.3 При наступлении любого из перечисленных в п. 6.1 событий Владелец ключа должен немедленно прекратить связь с другими абонентами и сообщить о факте компрометации руководителю структурного подразделения или Администратору СКЗИ.
8.4 При подтверждении факта компрометации действующих ключей Пользователь СКЗИ обязан обеспечить немедленное изъятие из обращения скомпрометированных криптографических ключей.
8.5 Для восстановления конфиденциальной связи, после компрометации действующих ключей, на Пользователя СКЗИ оформляются новые ключи ЭЦП.

9. Уничтожение криптографических ключей
9.1 Неиспользованные или выведенные из действия криптографические ключи подлежат уничтожению.
9.2 Уничтожение криптографических ключей на ключевых носителях производится уполномоченной на то комиссий с участием Администратора СКЗИ с оформлением акта актом (приложение №2 к настоящей Инструкции).
9.3 Криптографические ключи, находящиеся на ключевых носителях, уничтожаются путем их стирания (разрушения) по технологии, принятой для ключевых носителей многократного использования в соответствии с требованиями эксплуатационной и технической документации на СКЗИ. При уничтожении криптографических ключей, находящихся на ключевых носителях, необходимо:
а) установить наличие оригинала и количество копий криптографических ключей;
б) проверить внешним осмотром целостность каждого ключевого носителя;
в) установить наличие на оригинале и всех копиях ключевых носителей реквизитов путем сверки с записями в Журнале поэкземплярного учета;
г) убедиться, что криптографические ключи, находящиеся на ключевых носителях, действительно подлежат уничтожению;

д) произвести уничтожение ключевой информации на оригинале и на всех копиях носителей.
9.4 В Журнале поэкземплярного учета Администратором СКЗИ производится отметка об уничтожении криптографических ключей.

10. Права Администратора СКЗИ
10.1. Администратор СКЗИ имеет право:
а) вносить предложения по совершенствованию СКЗИ;
б) повышать уровень квалификации по использованию СКЗИ.

11. Ответственность Администратора СКЗИ
11.1. Администратора СКЗИ несет персональную ответственность за обеспечение конфиденциальности ключевых носителей.
11.2 В случае неисполнения или ненадлежащего выполнения требований настоящей Инструкции Администратора СКЗИ может быть привлечен к дисциплинарной и/или административной ответственности в соответствии с действующим законодательством Российской Федерации.