Приложение № 2
к приказу ГБОУ гимназии № 1 г. Новокуйбышевска
от 20.10.2020 г. № 85/02 -од
«О порядке хранения и эксплуатации
средств криптографической
защиты информации (СКЗИ)
в ГБОУ гимназии №1 г. Новокуйбышевска»

УТВЕРЖДЕНО
приказом ГБОУ гимназии №1
г. Новокуйбышевска
от 31.12.2019 г. № 104/06-од
Директор
_____ **Л.Г. Слепцова**

Инструкция
по обеспечению безопасности эксплуатации СКЗИ

1. **Общие положения**

1.1. Настоящая Инструкция по обеспечению безопасности эксплуатации СКИЗИ (далее – Инструкция) определяет порядок учета, хранения и использования СКЗИ, криптографических ключей и документов, а также порядок смены, уничтожения криптографических ключей в целях обеспечения безопасности эксплуатации СКЗИ в государственном бюджетном общеобразовательном учреждении Самарской области гимназии № 1 им. Н.И. Ферапонтова города Новокуйбышевска городского округа Новокуйбышевск Самарской области (далее – образовательная организация).

1.2. Настоящая Инструкция разработана в соответствии со следующими нормативными правовыми актами Российской Федерации:

- Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности (утв. приказом ФСБ России от 10.07.2014 № 378);

- Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (утв. приказом ФСБ России от 09.02.2005 № 66);
- Инструкция 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 (утв. приказом ФАПСИ от 13.06.2001 № 152).

1.1. В образовательном учреждении используются только сертифицированные СКЗИ, предназначенные для защиты информации, не содержащей сведений, составляющих государственную тайну.

1.2. В образовательной организации приказом руководителя (директора) образовательной организации назначается ответственный за хранение и эксплуатацию СКЗИ - ответственный за организацию обработки персональных данных.

1.3. Подписывая лист ознакомления с настоящей Инструкцией, ответственный за организацию обработки персональных данных подтверждает, что также ознакомлен с 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 (утв. приказом ФАПСИ от 13.06.2001 № 152).

1.4. Ответственный за организацию обработки персональных данных осуществляет:

- поэкземплярный учет СКЗИ, документации к ним, ключевых носителей и ключевых документов;
- учет пользователей СКЗИ (далее – Пользователи) и представление на утверждение руководителю (директору) образовательной организации списка пользователей СКЗИ;
- контроль за соблюдением условий использования СКЗИ;

- расследования и составление заключений по фактам нарушений условий использования СКЗИ;
- обеспечение мер по предотвращению возможных нежелательных последствий таких нарушений;
- обучение Пользователей правилам работы с СКЗИ и правилам хранения СКЗИ, ключевых носителей и ключевых документов.

1.5. Список Пользователей утверждается приказом руководителя (директора) образовательной организацией.

1.6. Пользователь обязан:

- не разглашать конфиденциальную информацию, к которой он допущен, в том числе: сведения об СКЗИ, ключевых документах к ним и других мерах защиты;
- соблюдать требования по обеспечению безопасности конфиденциальной информации при использовании СКЗИ;
- хранить ключевую информацию в сейфах и помещениях, гарантирующую ее сохранность и конфиденциальность;
- сообщать ответственному за организацию обработки персональных данных о попытках посторонних лиц получить сведения об СКЗИ или ключевых документах к ним;
- незамедлительно уведомлять ответственного за организацию обработки персональных данных о фактах утраты или недостачи СКЗИ, криптографических ключей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений;
- сдать СКЗИ, документацию к ним, криптографические ключи ответственному за организацию обработки персональных данных, в соответствии с порядком, установленным настоящей Инструкцией, при прекращении использования СКЗИ (увольнении, перевода на другую должность, уничтожении СКИЗИ и в иных подобных случаях).

1.7. К работе с СКЗИ Пользователи допускаются только после соответствующего инструктажа.

2. Учет СКЗИ, хранение и передача криптографических ключей

2.1. СКЗИ, документация к ним, ключевые документы и ключевые носители подлежат поэкземплярному учету. Программные СКЗИ учитываются совместно с аппаратными средствами, на которых осуществляется их штатная эксплуатация. Учет осуществляется ответственным за организацию обработки персональных данных в Журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов (далее – Журнал).

2.2. Единицей поэкземплярного учета ключевых документов считается отчуждаемый носитель с записанными криптографическими ключами.

2.3. Все полученные экземпляры СКЗИ, документация к ним, ключевые документы выдаются Пользователям под роспись в Журнале. Пользователи несут персональную ответственность за сохранность СКЗИ и ключевых документов.

2.4. Дистрибутивы СКЗИ, документация к ним хранятся у ответственного за организацию обработки персональных данных.

2.5. Ключевые носители с криптографическими ключами хранятся у Пользователей.

2.6. Хранение осуществляется в сейфе индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

2.7. В случае отсутствия у Пользователя индивидуального хранилища, ключевые носители с криптографическими ключами по окончании рабочего дня сдаются ответственному за организацию обработки персональных данных.

2.8. Ключевые носители с неработоспособными криптографическими ключами ответственный за организацию обработки персональных данных принимает от Пользователя и делает соответствующую запись в Журнале. Неработоспособные ключевые носители подлежат уничтожению.

2.9. Аппаратные средства, с которыми осуществляется штатное использование СКЗИ, должны быть оборудованы средствами контроля за их

вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ и аппаратных средств должно быть визуально контролируемым.

3. Использование СКЗИ

3.1. В образовательной организации СКЗИ используется с целью обеспечения конфиденциальности и целостности электронных документов, а также с целью организации юридически значимого электронного документооборота с использованием средств электронной подписи.

3.2. Для шифрования электронного документа Пользователь использует свой собственный закрытый криптографический ключ и открытый криптографический ключ.

3.3. В образовательной организации используются только те СКЗИ, которые реализуют стойкие криптографические алгоритмы, не позволяющие в разумные сроки вычислить закрытый ключ по открытому ключу.

3.4. Пользователь ежедневно проверяет сохранность технических средств и целостность печатей и пломб на них.

3.5. В случае обнаружения неразрешенного программного обеспечения или факта повреждения целостности печати (пломбы) на техническом средстве с СКЗИ, работа с СКЗИ на таком техническом средстве должна быть прекращена. По данная информация передается руководителю (директору) образовательной организации.

3.6. Вскрытие технического средства с СКЗИ для проведения ремонта или технического обслуживания осуществляется только в присутствии Пользователя.

3.7. При работе с СКЗИ запрещается:

- оставлять без присмотра (контроля) технические средства, на которых эксплуатируется СКЗИ;
- самостоятельно вносить изменения в программную часть СКЗИ;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить

ключевую информацию на дисплей, принтер и другие средства вывода информации;

- использовать ключевые носители в режимах, не предусмотренных штатными функциями СКЗИ;
- осуществлять несанкционированное копирование криптографических ключей;
- изменять настройки или пытаться изменить настройки СКЗИ или операционной системы;
- осуществлять самостоятельное несанкционированное вскрытие технических средств с СКЗИ.

3.8. С целью обеспечения непрерывности работы образовательной организации плановая замена ключевой информации должна производиться заблаговременно.

4. Действия при компрометации криптографических ключей

4.1. Криптографические ключи считаются скомпрометированными в следующих случаях:

- потеря ключевых носителей (в том числе с последующим обнаружением);
- увольнение сотрудников, имевших доступ к ключевым носителям;
- возникновение подозрений на утечку информации или ее искажение в информационной системе;
- нарушение печати на техническом средстве с СКЗИ;
- временный бесконтрольный доступ посторонних лиц к ключевым носителям или техническим средствам с СКЗИ;
- иные случаи подозрения компрометации криптографических ключей.

4.2. В случае подозрения в компрометации криптографических ключей, Пользователь должен немедленно прекратить эксплуатацию СКЗИ и продолжить ее только после замены криптографических ключей.

4.3. Скомпрометированные криптографические ключи подлежат уничтожению.

5. Уничтожение криптографических ключей

5.1. Неиспользованные или выведенные из действия криптографические ключи подлежат уничтожению.

5.2. Уничтожение криптографических ключей на ключевых носителях производятся через привлечение для таких работ на договорной основе сторонних организаций

5.3. Криптографические ключи, записанные на бумажных носителях, уничтожаются физически (сжигание, измельчение и т. д.).

5.4. Перед уничтожением криптографических ключей и/или ключевых носителей, ответственный за организацию обработки персональных данных обязан:

- установить наличие оригинала и количество копий криптографических ключей;
- проверить внешнюю целостность каждого ключевого носителя;
- идентифицировать каждый ключевой носитель в соответствии с Журналом поэкземплярного учета средств криптографической защиты информации;
- убедиться, что криптографические ключи, находящиеся на ключевых носителях, действительно подлежат уничтожению.

5.5. В Журнале поэкземплярного учета средств криптографической защиты информации делается отметка об уничтожении криптографических ключей.

6. Требования к помещениям, в которых ведется работа с СКИЗИ и/или хранятся криптографические ключи

6.1. Размещение, специально оборудование, охрана и организация режима в помещениях, где установлены СКЗИ и/или хранятся криптографические ключи (далее – спецпомещения), должны обеспечивать сохранность СКЗИ и криптографических ключей.

6.2. При оборудовании спецпомещений должны выполняться требования к размещению, монтажу СКЗИ, а также другого оборудования, функционирующего с СКЗИ.

6.3. Спецпомещения должны иметь прочные входные двери с замками, гарантирующими надежную защиту от проникновения посторонних лиц в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение посторонних лиц, необходимо оборудовать средствами, препятствующими неконтролируемому проникновению в спецпомещения. При этом, применение нераспахиваемых железных решеток на окнах запрещено, поскольку это противоречит правилам пожарной безопасности.

6.4. Мониторы рабочих станций с СКЗИ должны быть повернуты задней стороной к дверям и окнам, либо должны применяться шторы, рольставни, жалюзи или другие средства для пресечения несанкционированного просмотра содержимого, отображаемого на мониторах.

6.5. Для хранения криптографических ключей, документации, дистрибутивов СКЗИ используют металлический сейф. Ключи от сейфа хранятся у ответственного за организацию обработки персональных данных.

6.6. По окончании рабочего дня спецпомещения и установленные в них сейфы должны быть закрыты на замок.

6.7. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в спецпомещения или сейф посторонних лиц, о случившемся должно быть немедленно сообщено ответственному за организацию обработки персональных данных. Ответственный за организацию обработки персональных данных должен оценить вероятность компрометации хранящихся криптографических ключей, составить акт и принять, при необходимости, меры к локализации последствия компрометации криптографических ключей и к их замене.