|  |  |
| --- | --- |
|  | УТВЕРЖДАЮДиректор ГБОУ СО «Верхнесинячихинская школа-интернат» \_\_\_\_\_\_\_\_\_\_\_\_\_ О.А. Бурухина «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_2020 г.  |

Инструкция по эксплуатации средств криптографической защиты информации в информационных системах персональных данных
ГБОУ СО «Верхнесинячихинская школа-интернат»

# Общие положения

Настоящая Инструкция разработана в соответствии с требованиями Федерального закона № 152-ФЗ от 27.07.2006 г. «О персональных данных», приказа ФСБ России от 10 июля 2014 г. N 378 "Об утверждении Состава и содержания 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" положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации от 09.02.2005 (Положение ПКЗ-2005), 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, утвержденной приказом ФАПСИ от 13 июня 2001 г. № 152.

Настоящая инструкция определяет порядок учета, хранения и использования средств криптографической защиты информации (далее – СКЗИ), а также порядок их изготовления, уничтожения и действий работников при компрометации или поломки, в целях обеспечения безопасности эксплуатации СКЗИ в информационных системах персональных данных
(далее - ИСПДн) ГБОУ СО «Верхнесинячихинская школа-интернат» (далее – Учреждение).

Все действия с СКЗИ осуществляются в соответствии с эксплуатационной документацией. Лицо, ответственное за эксплуатацию СКЗИ, назначается соответствующим приказом директора Учреждения. Для работы с СКЗИ допускаются только работники, перечень которых утвержден соответствующим приказом директора Учреждения
(далее – Пользователи СКЗИ, пользователи).

Учреждение использует сертифицированные ФСБ России СКЗИ, предназначенные для защиты информации, не содержащей сведений, составляющих государственную тайну.

# Обязанности ответственного за эксплуатацию средств криптографической защиты информации

 Ответственный за эксплуатацию СКЗИ осуществляет:

* поэкземплярный учет, эксплуатационной и технической документации к ним;
* контроль за соблюдением условий использования в соответствии с эксплуатационной и технической документацией, и настоящей Инструкцией;
* расследование и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению требуемого уровня безопасности информации;
* разработку и принятие мер по предотвращению возможных негативных последствий подобных нарушений.

Пользователь СКЗИ обязан:

* не разглашать конфиденциальную информацию, к которой допущен, рубежи ее защиты, в том числе сведения о криптографических ключах;
* соблюдать требования к обеспечению безопасности защищаемой информации при использовании СКЗИ;
* сдать СКЗИ, эксплуатационную и техническую документацию к ним, криптографические ключи в соответствии с порядком, установленным настоящей Инструкцией, при прекращении использования СКЗИ;
* незамедлительно уведомлять ответственного за эксплуатацию СКЗИ информации о фактах утраты или недостачи СКЗИ, криптографических ключей, ключей от помещений, ключевых носителей хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений, а также о причинах и условиях возможной утечки таких сведений.

Обучение пользователей правилам работы с СКЗИ осуществляет ответственный за эксплуатацию. Непосредственно к работе с СКЗИ пользователи допускаются после обучения.

Текущий контроль, обеспечение функционирования и безопасности СКЗИ возлагается на ответственного за СКЗИ.

Ответственный за эксплуатацию СКЗИ и пользователи должны быть ознакомлены с настоящей Инструкцией под расписку.

# Учёт и хранение СКЗИ

СКЗИ, эксплуатационная и техническая документация к ним, криптографические ключи подлежат поэкземплярному учету.

 Поэкземплярный учёт СКЗИ ведет ответственный за эксплуатацию в журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним (далее – журнал). При этом программные СКЗИ должны учитываться совместно с аппаратными СКЗИ, с которыми осуществляется их штатная эксплуатация. Если аппаратные или аппаратно-программные СКЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие СКЗИ учитываются также совместно с соответствующими аппаратными средствами.

Единицей поэкземплярного учета криптографических ключей, ключевых носителей, считается отчуждаемый ключевой носитель многократного использования. Если один и тот же ключевой носитель многократно используют для записи криптографических ключей, то его каждый раз следует регистрировать отдельно.

При необходимости пользователю СКЗИ выдается документация по эксплуатации СКЗИ в электронном виде.

Дистрибутивы СКЗИ на носителях, эксплуатационная и техническая документация к ним, инструкции хранятся у ответственного за эксплуатацию СКЗИ. Криптографические ключи, электронная подпись (далее – ЭП) и ключевые носители хранятся у пользователей СКЗИ. Хранение осуществляется в закрываемых на замок металлических хранилищах или сейфах, в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение или в опечатанном пенале (тубусе). Металлические шкафы (сейфы) должны быть оборудованы внутренними замками с двумя экземплярами ключей (или кодовыми замками) и приспособлениями для опечатывания.

Пользователи СКЗИ могут осуществлять хранение рабочих и резервных криптографических ключей, ЭП и ключевых носителей, предназначенных для применения в случае неработоспособности рабочих криптографических ключей, ЭП и ключевых носителей. Резервные криптографические ключи, ЭП и ключевые носители могут также находится на хранении у ответственного за эксплуатацию.

Автоматизированные рабочие места (АРМ), на которых осуществляется штатное функционирование СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования), АРМ должно быть таким, чтобы его можно было визуально контролировать.

Ключевые носители совместно с журналом должны храниться ответственным за эксплуатацию СКЗИ в 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.

На время отсутствия ответственного за эксплуатацию СКЗИ должен быть назначен работник, его замещающий.

При необходимости криптографические ключи, ЭП и ключевые носители сдаются на временное хранение ответственному за эксплуатацию.

# Использование СКЗИ и криптографических ключей, ЭП и ключевых носителей

СКЗИ используются для обеспечения конфиденциальности, авторства и целостности электронных документов.

Криптографический ключ невозможно использовать, если истек срок действия.

Для обеспечения контроля доступа к СКЗИ системный блок АРМ опечатывается ответственным за эксплуатацию СКЗИ.

Пользователь должен периодически (ежедневно) проверять сохранность оборудования и целостность пломб на АРМ. В случае обнаружения «посторонних» (не зарегистрированных) программ или выявления факта повреждения пломбы на системном блоке АРМ работа должна быть прекращена. По данному факту должен быть оповещен ответственный за эксплуатацию СКЗИ. Должно быть проведено служебное расследование, и осуществлены работы по анализу и ликвидации последствий данного нарушения. Также необходимо будет зафиксировать данное событие в журнале учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах.

При выявлении сбоев или отказов пользователь обязан сообщить о факте их возникновения ответственному за эксплуатацию СКЗИ и предоставить ему носители криптографических ключей для проверки их работоспособности. Проверку работоспособности носителей криптографических ключей ответственный за эксплуатацию СКЗИ выполняет в присутствии пользователя.

В случае, если рабочие криптографические ключи потеряли работоспособность, то по просьбе пользователя ответственный за эксплуатацию СКЗИ, вскрывает конверт (коробку) с резервными криптографическими ключами, делает копию ключевого носителя, используя резервные криптографические ключи, помещает резервные криптографические ключи в конверт (коробку), а на новый ключевой носитель наклеивает наклейку с надписью: «Рабочий».

В экстренных случаях, не терпящих отлагательства, вскрытие конверта (коробки) с резервными криптографическими ключами может осуществляться с участием комиссии с последующим уведомлением ответственного за эксплуатацию СКЗИ о факте вскрытия конверта с криптографическими ключами. На конверте делается запись о вскрытии с указанием даты и времени вскрытия конверта и подписью пользователя. Вскрытый конверт вместе с неработоспособными криптографическими ключами сдаются ответственному за эксплуатацию СКЗИ.

Вскрытие системного блока АРМ, на которой установлено СКЗИ, для проведения ремонта или технического обслуживания должно осуществляться в присутствии ответственного за эксплуатацию СКЗИ.

Пользователю запрещается:

* осуществлять несанкционированное копирование СКЗИ;
* использовать ключевые носители и ЭП для работы на других рабочих местах для шифрования и подписи электронных документов;
* разглашать содержимое СКЗИ или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер;
* вставлять носители криптографических ключей, ЭП и ключевые носители в устройства считывания в режимах, не предусмотренных штатным режимом работы СКЗИ, а также в устройства считывания других АРМ;
* записывать на носители с криптографическими ключами, ЭП и ключевыми носителями постороннюю информацию;
* подключать к АРМ дополнительные устройства и соединители, не предусмотренные в штатной комплектации;
* работать на АРМ, если во время ее начальной загрузки не проходят встроенные тесты, предусмотренные в АРМ;
* вносить какие-либо изменения в программное обеспечение СКЗИ.

# Изготовление и плановая смена криптографических ключей и ЭП

Изготовление криптографических ключей и ЭП может производиться ответственным за эксплуатацию СКЗИ в присутствии пользователя, при наличии такой возможности у ответственного за эксплуатацию СКЗИ и наличия соответствующего программного обеспечения. Также возможно изготовление криптографических ключей и ЭП в сторонней организации, имеющей необходимую лицензию ФСБ на оказание такого рода услуг.

Криптографические ключи и ЭП изготавливаются на отчуждаемый ключевой носитель в соответствии с эксплуатационно-технической документацией на СКЗИ и требованиями безопасности, установленными настоящей Инструкцией.

Переход на новые криптографические ключи пользователь выполняет самостоятельно в соответствии с эксплуатационной документацией на СКЗИ. Переход на новые криптографические ключи осуществляется в сроки, указанные в сертификате ключа подписи.

При замене криптографических ключей используют программное обеспечение в соответствии с документами по эксплуатации. Пользователь самостоятельно обязан обновить сертификат ключ подписи. Обновление справочников сертификатов ключей производится путем добавления новых сертификатов ключей подписи из файлов, содержащих сертификаты ключей подписи, предоставляемых ответственным за эксплуатацию. Обновление справочников сертификатов ключей подписи осуществляется в соответствии с эксплуатационной документацией на СКЗИ.

# Действия при компрометации криптографических ключей и ЭП

К обстоятельствам, указывающим на возможную компрометацию криптографических ключей и ЭП, но не ограничивающим их, относятся следующие:

* потеря ключевых носителей с рабочими и/или резервными криптографическими ключами или ЭП;
* потеря ключевых носителей с рабочими и/или резервными криптографическими ключами или ЭП с последующим их обнаружением;
* увольнение работников, имевших доступ к рабочим и/или резервным криптографическим ключам или ЭП;
* возникновение подозрений относительно утечки информации или ее искажения;
* нарушение целостности печатей на сейфах (металлических шкафах) с ключевыми носителями с рабочими и/или резервными криптографическими ключами, ЭП, если используется процедура опечатывания сейфов;
* утрата ключей от сейфов в момент нахождения в них ключевых носителей с рабочими и/или резервными криптографическими ключами, ЭП;
* временный доступ посторонних лиц к ключевым носителям, а также другие события, при которых достоверно не известно, что произошло с ключевыми носителями.

В случае возникновения данных обстоятельств пользователь обязан незамедлительно прекратить обмен электронными документами с использованием скомпрометированных закрытых криптографических ключей, по телефону информировать ответственного за эксплуатацию СКЗИ о факте компрометации используемых закрытых криптографических ключей, ЭП.

Решение о компрометации криптографических ключей принимает ответственный за эксплуатацию СКЗИ на основании данных предоставленных пользователем по телефону или других средств связи.

Данные, предоставляемые пользователем должны содержать:

* идентификационные параметры скомпрометированного криптографического ключа, ЭП;
* фамилию, имя, отчество пользователя СКЗИ, который владел скомпрометированным криптографическим ключом, ЭП;
* сведения об обстоятельствах компрометации криптографического ключа, ЭП;
* время и обстоятельства выявления факта компрометации криптографического ключа, ЭП.

После принятия решения о компрометации криптографического ключа, ЭП принимаются меры о его изъятии из обращения в соответствии с требованиями эксплуатационной и технической документации на СКЗИ.

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

# Уничтожение криптографических ключей, ЭП и ключевых носителей

Неиспользованные или выведенные из действия криптографические ключи, ЭП и ключевые носители подлежат уничтожению.

Уничтожение криптографических ключей, ЭП на ключевых носителях производится ответственным за эксплуатацию СКЗИ.

Криптографические ключи, ЭП 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, ЭП находящихся на ключевых носителях, необходимо:

* установить наличие оригинала и количество копий криптографических ключей, ЭП;
* проверить внешним осмотром целостность каждого ключевого носителя;
* установить наличие на оригинале и всех копиях ключевых носителей реквизитов путем сверки с записями в журнале поэкземплярного учета;
* убедиться, что криптографические ключи, ЭП находящиеся на ключевых носителях, действительно подлежат уничтожению;
* произвести уничтожение ключевой информации на оригинале и на всех копиях носителей.
* в журнале поэкземплярного учета ответственным за эксплуатацию СКЗИ производится отметка об уничтожении криптографических ключей.

# Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены или хранятся СКЗИ

Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся криптографические ключи (далее - режимные помещения), должны обеспечивать сохранность СКЗИ.

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

Помещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений 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 в режимные помещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в режимные помещения.

Размещение, специальное оборудование, охрана и организация режима в помещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

Режим охраны помещений, в том числе правила допуска работников и посетителей в рабочее и нерабочее время, устанавливает ответственный за эксплуатацию. Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются, а также учитывать положения настоящей Инструкции.

Двери режимных помещений должны быть постоянно закрыты и могут открываться только для санкционированного прохода работников и посетителей. Ключи от входных дверей находятся у ответственных лиц, имеющих право допуска в режимные помещения. Дубликаты ключей от входных дверей таких помещений следует хранить в специальном сейфе.

Для предотвращения просмотра извне помещений, где используются СКЗИ, окна должны быть защищены или экраны мониторов должны быть повернуты в противоположную сторону от окна.

Помещения, в которых используются при работе криптографические ключи, ЭП как правило, должны быть оснащены охранной сигнализацией, связанной со службой охраны здания. Работникам, ответственным за охрану здания, необходимо проверять периодически исправность сигнализации.

В обычных условиях помещения, находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями или ответственным за эксплуатацию.

При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному за эксплуатацию. Ответственный за эксплуатацию СКЗИ должен оценить возможность компрометации хранящихся криптографических ключей и принять, при необходимости, меры к локализации последствий компрометации СКЗИ и к их замене.

Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего со СКЗИ, в помещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена СКЗИ осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ.

На время отсутствия пользователей указанное оборудование, при наличии такой возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае по согласованию с ответственным за эксплуатацию необходимо предусмотреть организационно-технические меры, исключающие возможность использования СКЗИ посторонними лицами.

В нерабочее время помещения, в которых осуществляется функционирование СКЗИ, должны ставиться на охрану.

**РАЗРАБОТАНО:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ответственный за организацию обработки и обеспечение безопасности персональных данных |  |  |  | А.Е. Запольских |
|  |  | (подпись, дата) |  | (инициалы, фамилия) |

**С документом ознакомлен (а):**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Директор  |  |  |  | О.А. Бурухина  |
|  |  | (подпись, дата) |  | (инициалы, фамилия) |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Администратор безопасности ИСПДн  |  |  |  |  | Н.А. Блохин |
|  |  |  | (подпись, дата) |  | (инициалы, фамилия) |

Приложение №1

**Лист ознакомления с инструкцией**

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Ф.И.О.****работника** | **Личная подпись** | **Дата ознакомления** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |