БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВОЛОГОДСКОЙ ОБЛАСТИ

«БЕЛОЗЕРСКИЙ ИНДУСТРИАЛЬНО-ПЕДАГОГИЧЕСКИЙ КОЛЛЕДЖ

ИМ. А.А. ЖЕЛОБОВСКОГО»

П Р И К А З

г. Белозерск

29.04.2019 № 127-О

Об утверждении Инструкции
по обращению с сертифицированными
шифровальными средствами
(средствами криптографической
защиты информации)

В соответствии с Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденное Приказом ФСБ России от 9 февраля 2005 года № 66 (в редакции от 12.04.2010), Приказом ФАПСИ при Президенте РФ от 13.06.2001 года № 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», 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, утвержденные руководством 8 центра ФСБ России 21 февраля 2008 года № 149/6/6-622

ПРИКАЗЫВАЮ:

1. Назначить ответственным за обращение с сертифицированными шифровальными средствами (средствами криптографической защиты информации) Комаровскую К.С., преподавателя информатики.

2. Утвердить Инструкцию по обращению с сертифицированными шифровальными средствами (средствами криптографической защиты информации) в БПОУ ВО «Белозерский индустриально-педагогический колледж им. А.А. Желобовского».

3. Настоящий приказ подлежит опубликованию на официальном сайте БПОУ ВО «Белозерский индустриально-педагогический колледж им. А.А. Желобовского».

4. Контроль за исполнением настоящего распоряжения оставляю за собой.

Директор колледжа О.Г.Бибиксарова

УТВЕРЖДЕНА
распоряжением директора БПОУ ВО «Белозерского индустриально-педагогического колледжа им. А. А. Желобовского
_____ О. Г. Бибиксарова.
от «29» 04 2019 г. № 129а-0

ИНСТРУКЦИЯ

по организации и обеспечению безопасности эксплуатации шифровальных (криптографических) средств в БПОУ ВО «Белозерском индустриально-педагогическом колледже им. А. А. Желобовского»

1. Аннотация

Настоящая Инструкция содержит описание порядка обращения с сертифицированными средствами криптографической защиты информации ФСБ России (далее – СКЗИ), рекомендации по размещению и хранению технических средств, на которые установлены СКЗИ, по проверке целостности установленного программного обеспечения (далее – ПО) СКЗИ, по использованию СКЗИ в различных автоматизированных системах.

СКЗИ эксплуатируются в соответствии с правилами пользования ими. Изменения условий эксплуатации СКЗИ, указанных в правилах пользования ими, допускаются исключительно по согласованию с ФСБ России.

Настоящая Инструкция разработана в соответствии с документами:

1. Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденное Приказом ФСБ России № 66 от 9 февраля 2005 года;

2. Приказ ФАПСИ при Президенте РФ № 152 от 13 июня 2001 года «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»;

3. Типовые требования 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, утвержденные руководством 8 центра ФСБ России 21 февраля 2008 года № 149/6/6-622.

2. Список сокращений

- **НСД** Несанкционированный доступ
- **ОС** Операционная система
- **ПО** Программное обеспечение

- **ПЭВМ** Персональная электронная вычислительная машина
- **СКЗИ** Средство криптографической защиты информации
- **ТС** Технические средства
- **ФСБ** Федеральная служба безопасности России
- **ЭТД** Эксплуатационная и техническая документации.

3. Ответственные лица

В Бюджетном профессиональном образовательном учреждении Вологодской области «Белозерском индустриально-педагогическом колледже им. А. А. Желобовского» (далее – ОУ), эксплуатирующей сертифицированные СКЗИ, должны быть назначены и закреплены распоряжением следующие лица:

Администратор СКЗИ, на которого возлагаются задачи организации работ по:

• обеспечению корректного и безопасного функционирования СКЗИ;

• обеспечению корректной и безопасной эксплуатации СКЗИ;

• выработке соответствующих инструкций и ознакомление с ними пользователей СКЗИ;

• контролю работоспособности и соблюдения правил эксплуатации СКЗИ.

Пользователи СКЗИ, на которых возлагаются задачи по:

• соблюдению правил корректной и безопасной эксплуатации СКЗИ;

• обеспечению режима сохранности СКЗИ, ЭТД и ключевых документов, переданных им.

Администратор и Пользователи СКЗИ допускаются к работе с СКЗИ только после инструктажа и обучения правилам работы с СКЗИ. Для Администратора инструктаж и обучение проводит Лицензиат. Пользователей инструктирует и обучает Администратор СКЗИ.

4. Размещение технических средств с СКЗИ

Организация режима в помещениях, где располагаются ТС с СКЗИ и ведется работа с носителями с персональной ключевой информацией, описана в правилах пользования СКЗИ.

В общем случае в отношении помещений ОУ должен быть установлен режим, определяющий:

- лицо, ответственное за помещение;
- перечень лиц, допущенных к работе в помещении и обслуживанию помещения;
- порядок доступа в помещение в рабочее и нерабочее время, в аварийных ситуациях (пожар, авария, стихийное бедствие и т.п.);
- порядок нахождения в помещении посторонних лиц (при необходимости их нахождения);
- порядок хранения основного и резервного ключей от помещения.

Окна помещений должны быть защищены от НСД посторонних лиц (в случае, если окна на 1 этаже, либо рядом с пожарными лестницами) металлическими решетками, а также от визуально просмотра ведущихся в помещениях работ (шторами или жалюзи).

Двери помещений должны быть оборудованы надежными замками, гарантирующими их надежное закрытие в нерабочее время.

Помещения должны быть оборудованы пожарной сигнализацией, для которых Учреждение установлен порядок периодической проверки их исправности.

Параметры сети электроснабжения помещений должны соответствовать требованиям инструкций по эксплуатации ТС и правилам техники безопасности.

Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать Администратору и Пользователям СКЗИ сохранность доверенных им СКЗИ, конфиденциальных документов и сведений, включая ключевую информацию, и свести к минимуму возможность неконтролируемого доступа к ним посторонних лиц.

5. Хранение СКЗИ, ЭТД, ключевых документов, эталонных CD дисков

СКЗИ, ЭТД, ключевые документы, ключевые носители или аппаратные средства, к которым подключаются или в которые устанавливаются СКЗИ, эталонные CD-диски (диски, инсталлирующие программные СКЗИ), находящиеся у Администратора и Пользователей СКЗИ должны храниться в месте, исключающем возможность НСД к ним (сейф, шкаф индивидуального пользования с замком и т.п.). За их сохранность Администратор и Пользователей СКЗИ несут персональную ответственность.

ОУ должен быть определен порядок доступа в места хранения перечисленных материалов, а также порядок хранения основных и резервных ключей от них.

6. Установка СКЗИ и программного обеспечения на ПЭВМ

Установка и настройка общесистемного, прикладного ПО и дополнительных средств защиты на ПЭВМ с СКЗИ производится в соответствии с правилами установки и настройки СКЗИ и ПО, изложенными в ЭТД.

К установке и настройке СКЗИ и ПО предъявляются следующие общие требования:

- устанавливаемое ПО не должно содержать средств разработки и отладки приложений, а также средств, позволяющих осуществить несанкционированный доступ к системным ресурсам;
- устанавливаемое ПО должно быть лицензионным;
- устанавливаемое ПО должно предусматривать организацию разрешительной системы доступа, при которой Администратор и Пользователи имеют свои атрибуты (учетную запись) для входа в систему и доступа к ресурсам;
- устанавливаемое ПО и СКЗИ, а также диски для их инсталляции должны подвергаться периодическому контролю целостности в соответствии с ЭТД;
- устанавливаемое ПО должно устанавливаться совместно с антивирусным ПО, базы которого должны своевременно и регулярно обновляться;
- устанавливаемое ПО не должно содержать возможностей, позволяющих модифицировать системные ресурсы (области памяти, программный код), передавать управление несанкционированным подпрограммам, повышать предоставленные привилегии, использовать недокументированные разработчиками возможности ОС).

7. Конфигурирование системного и прикладного программного обеспечения на ПЭВМ с СКЗИ

К ОС, в среде, которой планируется использовать СКЗИ, предъявляются следующие общие требования:

- на ПЭВМ должна быть установлена только одна лицензионная ОС, удовлетворяющая системным требованиям СКЗИ (запрещается использовать нестандартные, измененные или отладочные версии ОС);
- удаленное управление ОС должно быть запрещено или ограничено путем отключения всех служб, реализующих данные механизмы, или путем настроек, запрещающих фильтров для протоколов и портов удаленного управления ОС для всех узлов, кроме специально выделенных для этих целей;
- каждый пользователь должен иметь для входа в ОС свою учетную запись, длина пароля которой должна быть не менее 6 символов (см. п.8 Инструкции);
- учетная запись для гостевого входа (Guest) должна быть отключена;
- правом установки и настройки ОС и СКЗИ должен обладать только Администратор;
- все неиспользуемые ресурсы ОС должны быть отключены (протоколы, сервисы и т.п.);
- режимы безопасности, реализованные в ОС, должны быть настроены на максимальный уровень;
- всем пользователям и группам, зарегистрированным в ОС, права доступа к ресурсам должны быть назначены в объеме, необходимом для выполнения ими своих обязанностей;
- доступ должен быть максимально ограничен к следующим ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части):
  - системный реестр;
  - файлы и каталоги;
  - временные файлы;
  - журналы системы;
  - файлы подкачки;
  - кэшируемая информация (пароли и т.п.);
  - отладочная информация.
- регулярно должны устанавливаться пакеты обновления безопасности ОС (Service Packs, Hot fix и т.п.), антивирусных баз;
- периодически должны исследоваться информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС;
- должна быть исключена возможность открытия и исполнения файлов и скриптовых объектов (например, JavaScript, VBScript, ActiveX), полученных из сети Internet, без проведения соответствующих проверок на предмет содержания в них программных закладок и сетевых вирусов (при подключении к сети Internet);
- на ПЭВМ с СКЗИ должны использоваться дополнительные методы и средства защиты (например: установка межсетевых экранов, организация VPN сетей и т.п.) при подключению к сети Internet. При этом предпочтение должно отдаваться сертифицированным средствам защиты;

- должна быть реализована система аудита событий безопасности ОС, роводиться регулярный анализ результатов аудита;

Администратор СКЗИ должен осуществлять периодический контроль выполнения указанных требований, а также требований, приведенных в ЭТД.

Не допускается:

- обрабатывать на ПЭВМ, оснащенной СКЗИ, информацию, содержащую государственную тайну;
- осуществлять несанкционированное изменение аппаратной и программной конфигурации ПЭВМ (в том числе несанкционированное вскрытие), СКЗИ, ПО.

8. Защита СКЗИ от несанкционированного доступа

Защита СКЗИ от НСД включают в себя выполнение следующих мероприятий:

- на административном уровне (предпринимаемые руководством Администрации действия по обеспечению процессов ИБ (в частности по вопросам применения СКЗИ) ресурсами, управлением и контролем со стороны руководства);
- на организационном уровне (регламентация процессов охраны и режима допуска в отношении СКЗИ, ТС с СКЗИ, помещений, процессов обеспечения информационной безопасности (в частности при эксплуатации СКЗИ) и контроля эффективности, процессов обеспечения и поддержания компетентности персонала при работе с СКЗИ, распределение обязанностей и ответственности);
- на техническом уровне (обеспечение соблюдения правил эксплуатации и работоспособности СКЗИ).

Защита СКЗИ от НСД должна удовлетворять следующим общим требованиям:

- должна обеспечиваться на всех технологических этапах и во всех режимах функционирования СКЗИ, в том числе при проведении ремонтных и регламентных работ;
- должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль должен периодически выполняться Администратором СКЗИ на основе требований документации на средства защиты от НСД;
- должна исключать возможность несанкционированного не обнаруживаемого доступа к СКЗИ, ТС с СКЗИ, инсталлирующих и ключевых носителей изменения аппаратной части ТС с СКЗИ (путем опечатывания (опломбирования) системного блока и разъемов ПЭВМ, опечатывания замочных скважин мест сейфов, шкафов, ящиков для хранения).

Перечень сотрудников, допущенных к работе в помещениях, на ТС с СКЗИ и непосредственно СКЗИ, должен быть закреплен распоряжением по ОУ. Все они должны иметь соответствующий уровень компетентности и допускаться к работе только после инструктажа по обеспечению информационной безопасности с использованием СКЗИ и обучения эксплуатации СКЗИ.

Для регламентации входа в ОС, BIOS, при осуществления шифрования на пароле и т.д. Администратором СКЗИ разрабатывается и применяется политика назначения и смены паролей. Пароли должны формироваться в соответствии со следующими правилами:

- длина пароля должна быть не менее 6 символов;

- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ, числа, сочетания цифр и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях.

Администратор СКЗИ, а также Пользователи СКЗИ несут персональную ответственность за обеспечение режима конфиденциальности в отношении паролей доступа. Запрещается записывать пароли на материальные носители и хранить их в легкодоступных местах, в том числе на мониторе, рабочем столе или ящиках стола.

Периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 1 год. Пароль должен быть изменен раньше плановой замены в случае его компрометации. Ответственность за своевременную смену пароля несет Администратор СКЗИ.

Указанная политика обязательна для всех учетных записей, зарегистрированных в ОС. Средствами BIOS должна быть исключена возможность работы на ПЭВМ СКЗИ, если во время её начальной загрузки не проходят встроенные тесты.

9. Криптографическая защита

Порядок хранения и использования носителей ключевой информации с ключами электронной подписи должен исключать возможность несанкционированного доступа к ним.

Пользователи и Администратор СКЗИ, имеющие доступ к носителям ключевой информации, несут персональную ответственность за безопасность ключевой информации на них и обязаны обеспечивать её сохранность, неразглашение и нераспространение.

Во время работы с носителями ключевой информации доступ к ним посторонних лиц должен быть исключен.

При хранении ключевой информации СКЗИ в реестре Windows и на HDD ПЭВМ требования по хранению ключевых носителей распространяются на ПЭВМ.

В случае невозможности отчуждения ключевого носителя с ключевой информацией от ПЭВМ организационно-техническими мероприятиями должен быть исключен доступ нарушителей к ПЭВМ с ключами.

При хранении ключей на HDD ПЭВМ необходимо использовать парольную защиту.

Ключи должны обновляться с периодичностью, указанной в Правилах работы с СКЗИ.

Ключи на ключевых носителях (включая Touch Memory и смарт-карты), срок действия которых истек, уничтожаются путем переформатирования ключевых носителей средствами ПО СКЗИ, после чего ключевые носители могут использоваться для записи на них новой ключевой информации.

Запрещается:

- осуществлять несанкционированное копирование ключевых носителей;

- разглашать содержимое носителей ключевой информации или передавать ами носители лицам, к ним не допущенным
- вставлять ключевой носитель в считывающее устройство в режимах, не предусмотренных штатным режимом использования ключевого носителя;
- оставлять без контроля ТС, на которых эксплуатируется СКЗИ, после ввода ключевой информации;
- использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами СКЗИ.

10. Учет СКЗИ

Администратор безопасности ведет учет поставки, установки и обслуживания в отношении следующих материалов:

- СКЗИ (СКЗИ);
- ЭТД (Э);
- ключевые документы - физические носители определенной структуры, содержащие ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию (КД);
- ключевые носители или аппаратные средства, к которым подключаются или в которые устанавливаются СКЗИ (А);
- эталонные CD диски (Д).

Учет ведется в Журнале учета (Приложение № 1).

Журнал учета СКЗИ должен храниться в месте, исключающем возможность несанкционированного доступа к нему (сейф, личный шкаф с замком и т.п.).

За ведение и хранение Журнала отвечает Администратор безопасности.

11. Контроль соблюдения условий эксплуатации и работоспособности СКЗИ

Лицензиат осуществляет контроль соблюдения ОУ условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ, настоящей Инструкцией, а также иными нормативно-методическими документами по эксплуатации.

Лицензиат также осуществляет контроль выполнения ОУ данных ей указаний по ОУ и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации.

Контроль может быть плановым и внеплановым.

Плановый контроль осуществляется с установленной периодичностью, но не реже 1 раза в год.

Внеплановый контроль осуществляется в случае установления фактов нарушения Администрацией условий эксплуатации или работоспособности СКЗИ.

В ходе контроля оцениваются:

- организация безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации;
- достигнутый уровень криптографической защиты конфиденциальной информации;
- условия использования СКЗИ.

По результатам контроля Лицензиатом оформляется Протокол проверки в двух экземплярах (один для ОУ, другой для Лицензиата. С протоколом проверки должно быть ознакомлено руководство ОУ под расписку на экземпляре ОУ.

Сведения о контроле заносятся Администратором СКЗИ в Журнал контроля соблюдения условий эксплуатации и работоспособности СКЗИ (Приложение № 2).

Если при контроле обнаружены недостатки, то Лицензиат делает записи в Журнал замечаний по результатам контроля (Приложение № 3). На каждое замечание назначается лицо, ответственное за его устранение, а также срок устранения. По результатам работы над замечанием в Журнале замечаний по результатам контроля делается запись о статусе устранения замечания, которая заверяется подписью лица, ответственного за устранение замечания и Администратора СКЗИ.

ОУ обязано принять меры по устранению вскрытых недостатков и выполнению рекомендаций Лицензиата, изложенных в Журнале замечаний по результатам контроля.

Если в ходе контроля выявлены серьезные нарушения в эксплуатации СКЗИ, из-за чего становится реальной утечка конфиденциальной информации, Лицензиат вправе дать указание о прекращении использования СКЗИ до устранения причин выявленных нарушений.

Приложение № 1
к Инструкции по организации и обеспечению безопасности эксплуатации шифровальных (криптографических) средств в БПОУ ВО «Белозерском индустриально-педагогическом колледже им. А. А. Желобовского»

ТИПОВАЯ ФОРМА
журнала поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов

N п/п	Наименование криптосредства, эксплуатационной и технической документации к ним, ключевых документов	Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя криптосредств	Дата и расписка в получении
1	2	3	4	5	6	7	8

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф.И.О. пользователя криптосредств, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены криптосредства	Дата изъятия (уничтожения)	Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15

УТВЕРЖДЕНА
приказом директора БПОУ ВО «Белозерский индустриально-педагогический колледж им. А.А. Желобовского»
«29» 04 2019 г. № 127-О

ИНСТРУКЦИЯ

по обращению с сертифицированными шифровальными средствами (средствами криптографической защиты информации) в БПОУ ВО «Белозерский индустриально-педагогический колледж им. А.А. Желобовского»

1. Аннотация

Настоящая Инструкция содержит описание порядка обращения с сертифицированными средствами криптографической защиты информации ФСБ России (далее – СКЗИ), рекомендации по размещению и хранению технических средств, на которые установлены СКЗИ, по проверке целостности установленного программного обеспечения (далее – ПО) СКЗИ, по использованию СКЗИ в различных автоматизированных системах.

СКЗИ эксплуатируются в соответствии с правилами пользования ими. Изменения условий эксплуатации СКЗИ, указанных в правилах пользования ими, допускаются исключительно по согласованию с ФСБ России.

Настоящая Инструкция разработана в соответствии с документами:

1. Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденное Приказом ФСБ России № 66 от 9 февраля 2005 года;
2. Приказ ФАПСИ при Президенте РФ № 152 от 13 июня 2001 года «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»;
3. Типовые требования 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, утвержденные руководством 8 центра ФСБ России 21 февраля 2008 года № 149/6/6-622.

2. Список сокращений

- **НСД** Несанкционированный доступ
- **ОС** Операционная система
- **ПО** Программное обеспечение
- **ПЭВМ** Персональная электронная вычислительная машина
- **СКЗИ** Средство криптографической защиты информации
- **ТС** Технические средства
- **ФСБ** Федеральная служба безопасности России
- **ЭТД** Эксплуатационная и техническая документация

3. Ответственные лица

В Администрации БПОУ ВО «Белозерский индустриально-педагогический колледж им.А.А.Желобовского» (далее – Учреждение), эксплуатирующей сертифицированные СКЗИ, должны быть назначены и закреплены распоряжением следующие лица:

Администратор СКЗИ, на которого возлагаются задачи организации работ по:

- обеспечению корректного и безопасного функционирования СКЗИ;
- обеспечению корректной и безопасной эксплуатации СКЗИ;
- выработке соответствующих инструкций и ознакомление с ними пользователей СКЗИ;
- контролю работоспособности и соблюдения правил эксплуатации СКЗИ.

Пользователи СКЗИ, на которых возлагаются задачи по:

- соблюдению правил корректной и безопасной эксплуатации СКЗИ;
- обеспечению режима сохранности СКЗИ, ЭТД и ключевых документов, переданных им.

Администратор и Пользователи СКЗИ допускаются к работе с СКЗИ только после инструктажа и обучения правилам работы с СКЗИ. Для Администратора инструктаж и обучение проводит Лицензиат. Пользователей инструктирует и обучает Администратор СКЗИ.

4. Размещение технических средств с СКЗИ

Организация режима в помещениях, где располагаются ТС с СКЗИ и ведется работа с носителями с персональной ключевой информацией, описана в правилах пользования СКЗИ.

В общем случае в отношении помещений Администрацией должен быть установлен режим, определяющий:

- лицо, ответственное за помещение;
- перечень лиц, допущенных к работе в помещении и обслуживанию помещения;
- порядок доступа в помещение в рабочее и нерабочее время, в аварийных ситуациях (пожар, авария, стихийное бедствие и т.п.);
- порядок нахождения в помещении посторонних лиц (при необходимости их нахождения);
- порядок хранения основного и резервного ключей от помещения.

Окна помещений должны быть защищены от НСД посторонних лиц (в случае, если окна на 1 этаже, либо рядом с пожарными лестницами) металлическими решетками, а также от визуально просмотра ведущихся в помещениях работ (шторами или жалюзи).

Двери помещений должны быть оборудованы надежными замками, гарантирующими их надежное закрытие в нерабочее время.

Помещения должны быть оборудованы пожарной сигнализацией, для которых Администрацией установлен порядок периодической проверки их исправности.

Параметры сети электроснабжения помещений должны соответствовать требованиям инструкций по эксплуатации ТС и правилам техники безопасности.

Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать Администратору и Пользователям СКЗИ сохранность доверенных им СКЗИ, конфиденциальных документов и сведений, включая ключевую информацию, и свести к минимуму возможность неконтролируемого доступа к ним посторонних лиц.

5. Хранение СКЗИ, ЭТД, ключевых документов, эталонных CD дисков

СКЗИ, ЭТД, ключевые документы, ключевые носители или аппаратные средства, к которым подключаются или в которые устанавливаются СКЗИ, эталонные CD-диски (диски, инсталлирующие программные СКЗИ), находящиеся у Администратора и Пользователей СКЗИ должны храниться в месте, исключающем возможность НСД к ним (сейф, шкаф индивидуального пользования с замком и т.п.). За их сохранность Администратор и Пользователей СКЗИ несут персональную ответственность.

Администрацией должен быть определен порядок доступа в места хранения перечисленных материалов, а также порядок хранения основных и резервных ключей от них.

6. Установка СКЗИ и программного обеспечения на ПЭВМ

Установка и настройка общесистемного, прикладного ПО и дополнительных средств защиты на ПЭВМ с СКЗИ производится в соответствии с правилами установки и настройки СКЗИ и ПО, изложенными в ЭТД.

К установке и настройке СКЗИ и ПО предъявляются следующие общие требования:

- устанавливаемое ПО не должно содержать средств разработки и отладки приложений, а также средств, позволяющих осуществить несанкционированный доступ к системным ресурсам;
- устанавливаемое ПО должно быть лицензионным;
- устанавливаемое ПО должно предусматривать организацию разрешительной системы доступа, при которой Администратор и Пользователи имеют свои атрибуты (учетную запись) для входа в систему и доступа к ресурсам;
- устанавливаемое ПО и СКЗИ, а также диски для их инсталляции должны подвергаться периодическому контролю целостности в соответствии с ЭТД;
- устанавливаемое ПО должно устанавливаться совместно с антивирусным ПО, базы которого должны своевременно и регулярно обновляться;
- устанавливаемое ПО не должно содержать возможностей, позволяющих модифицировать системные ресурсы (области памяти, программный код), передавать управление несанкционированным подпрограммам, повышать предоставленные привилегии, использовать недокументированные разработчиками возможности ОС).

7. Конфигурирование системного и прикладного программного обеспечения на ПЭВМ с СКЗИ

К ОС, в среде, которой планируется использовать СКЗИ, предъявляются следующие общие требования:

- на ПЭВМ должна быть установлена только одна лицензионная ОС, удовлетворяющая системным требованиям СКЗИ (запрещается использовать нестандартные, измененные или отладочные версии ОС);
- удаленное управление ОС должно быть запрещено или ограничено путем отключения всех служб, реализующих данные механизмы, или путем настроек, запрещающих фильтров для протоколов и портов удаленного управления ОС для всех узлов, кроме специально выделенных для этих целей;
- каждый пользователь должен иметь для входа в ОС свою учетную запись, длина пароля которой должна быть не менее 6 символов (см. п.8 Инструкции);
- учетная запись для гостевого входа (Guest) должна быть отключена;
- правом установки и настройки ОС и СКЗИ должен обладать только Администратор;
- все неиспользуемые ресурсы ОС должны быть отключены (протоколы, сервисы и т.п.);

- режимы безопасности, реализованные в ОС, должны быть настроены на максимальный уровень;
- всем пользователям и группам, зарегистрированным в ОС, права доступа к ресурсам должны быть назначены в объеме, необходимом для выполнения ими своих обязанностей;
- доступ должен быть максимально ограничен к следующим ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части):

  - системный реестр;
  - файлы и каталоги;
  - временные файлы;
  - журналы системы;
  - файлы подкачки;
  - кэшируемая информация (пароли и т.п.);
  - отладочная информация.

- регулярно должны устанавливаться пакеты обновления безопасности ОС (Service Packs, Hot fix и т.п.), антивирусных баз;
- периодически должны исследоваться информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС;
- должна быть исключена возможность открытия и исполнения файлов и скриптовых объектов (например, JavaScript, VBScript, ActiveX), полученных из сети Internet, без проведения соответствующих проверок на предмет содержания в них программных закладок и сетевых вирусов (при подключении к сети Internet);
- на ПЭВМ с СКЗИ должны использоваться дополнительные методы и средства защиты (например: установка межсетевых экранов, организация VPN сетей и т.п.) при подключению к сети Internet. При этом предпочтение должно отдаваться сертифицированным средствам защиты;
- должна быть реализована система аудита событий безопасности ОС, проводиться регулярный анализ результатов аудита;

Администратор СКЗИ должен осуществлять периодический контроль выполнения указанных требований, а также требований, приведенных в ЭТД.

Не допускается:

- обрабатывать на ПЭВМ, оснащенной СКЗИ, информацию, содержащую государственную тайну;

- осуществлять несанкционированное изменение аппаратной и программной конфигурации ПЭВМ (в том числе несанкционированное вскрытие), СКЗИ, ПО.

8. Защита СКЗИ от несанкционированного доступа

Защита СКЗИ от НСД включают в себя выполнение следующих мероприятий:

- на административном уровне (предпринимаемые руководством Администрации действия по обеспечению процессов ИБ (в частности по вопросам применения СКЗИ) ресурсами, управлением и контролем со стороны руководства);
- на организационном уровне (регламентация процессов охраны и режима допуска в отношении СКЗИ, ТС с СКЗИ, помещений, процессов обеспечения информационной безопасности (в частности при эксплуатации СКЗИ) и контроля эффективности, процессов обеспечения и поддержания компетентности персонала при работе с СКЗИ, распределение обязанностей и ответственности);
- на техническом уровне (обеспечение соблюдения правил эксплуатации и работоспособности СКЗИ).

Защита СКЗИ от НСД должна удовлетворять следующим общим требованиям:

- должна обеспечиваться на всех технологических этапах и во всех режимах функционирования СКЗИ, в том числе при проведении ремонтных и регламентных работ;
- должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль должен периодически выполняться Администратором СКЗИ на основе требований документации на средства защиты от НСД;
- должна исключать возможность несанкционированного не обнаруживаемого доступа к СКЗИ, ТС с СКЗИ, инсталлирующих и ключевых носителей изменения аппаратной части ТС с СКЗИ (путем опечатывания (опломбирования) системного блока и разъемов ПЭВМ, опечатывания замочных скважин мест сейфов, шкафов, ящиков для хранения).

Перечень сотрудников, допущенных к работе в помещениях, на ТС с СКЗИ и непосредственно СКЗИ, должен быть закреплен распоряжением по Администрации. Все они должны иметь соответствующий уровень компетентности и допускаться к работе только после инструктажа по обеспечению информационной безопасности с использованием СКЗИ и обучения эксплуатации СКЗИ.

Для регламентации входа в ОС, BIOS, при осуществления шифрования на пароле и т.д. Администратором СКЗИ разрабатывается и применяется политика назначения и смены паролей. Пароли должны формироваться в соответствии со следующими правилами:

- длина пароля должна быть не менее 6 символов;

- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ, числа, сочетания цифр и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях.

Администратор СКЗИ, а также Пользователи СКЗИ несут персональную ответственность за обеспечение режима конфиденциальности в отношении паролей доступа. Запрещается записывать пароли на материальные носители и хранить их в легкодоступных местах, в том числе на мониторе, рабочем столе или ящиках стола.

Периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 1 год. Пароль должен быть изменен раньше плановой замены в случае его компрометации. Ответственность за своевременную смену пароля несет Администратор СКЗИ.

Указанная политика обязательна для всех учетных записей, зарегистрированных в ОС. Средствами BIOS должна быть исключена возможность работы на ПЭВМ СКЗИ, если во время её начальной загрузки не проходят встроенные тесты.

9. Криптографическая защита

Порядок хранения и использования носителей ключевой информации с ключами электронной подписи должен исключать возможность несанкционированного доступа к ним.

Пользователи и Администратор СКЗИ, имеющие доступ к носителям ключевой информации, несут персональную ответственность за безопасность ключевой информации на них и обязаны обеспечивать её сохранность, неразглашение и нераспространение.

Во время работы с носителями ключевой информации доступ к ним посторонних лиц должен быть исключен.

При хранении ключевой информации СКЗИ в реестре Windows и на HDD ПЭВМ требования по хранению ключевых носителей распространяются на ПЭВМ.

В случае невозможности отчуждения ключевого носителя с ключевой информацией от ПЭВМ организационно-техническими мероприятиями должен быть исключен доступ нарушителей к ПЭВМ с ключами.

При хранении ключей на HDD ПЭВМ необходимо использовать парольную защиту.

Ключи должны обновляться с периодичностью, указанной в Правилах работы с СКЗИ.

Ключи на ключевых носителях (включая Touch Memory и смарт-карты), срок действия которых истек, уничтожаются путем переформатирования ключевых

носителей средствами ПО СКЗИ, после чего ключевые носители могут использоваться для записи на них новой ключевой информации.

Запрещается:

- осуществлять несанкционированное копирование ключевых носителей;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным
- вставлять ключевой носитель в считывающее устройство в режимах, не предусмотренных штатным режимом использования ключевого носителя;
- оставлять без контроля ТС, на которых эксплуатируется СКЗИ, после ввода ключевой информации;
- использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами СКЗИ.

10. Учет СКЗИ

Администратор безопасности ведет учет поставки, установки и обслуживания в отношении следующих материалов:

- СКЗИ (СКЗИ);
- ЭТД (Э);
- ключевые документы - физические носители определенной структуры, содержащие ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию (КД);
- ключевые носители или аппаратные средства, к которым подключаются или в которые устанавливаются СКЗИ (А);
- эталонные CD диски (Д).

Учет ведется в Журнале учета (Приложение № 1).

Журнал учета СКЗИ должен храниться в месте, исключающем возможность несанкционированного доступа к нему (сейф, личный шкаф с замком и т.п.).

За ведение и хранение Журнала отвечает Администратор безопасности.

11. Контроль соблюдения условий эксплуатации и работоспособности СКЗИ

Лицензиат осуществляет контроль соблюдения Администрацией условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ, настоящей Инструкцией, а также иными нормативно-методическими документами по эксплуатации.

Лицензиат также осуществляет контроль выполнения Администрацией данных ей указаний по Администрации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации.

Контроль может быть плановым и внеплановым.

Плановый контроль осуществляется с установленной периодичностью, но не реже 1 раза в год.

Внеплановый контроль осуществляется в случае установления фактов нарушения Администрацией условий эксплуатации или работоспособности СКЗИ.

В ходе контроля оцениваются:

- организация безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации;
- достигнутый уровень криптографической защиты конфиденциальной информации;
- условия использования СКЗИ.

По результатам контроля Лицензиатом оформляется Протокол проверки в двух экземплярах (один для Администрации, другой для Лицензиата. С протоколом проверки должно быть ознакомлено руководство Администрации под расписку на экземпляре Администрации.

Сведения о контроле заносятся Администратором СКЗИ в Журнал контроля соблюдения условий эксплуатации и работоспособности СКЗИ (Приложение № 2).

Если при контроле обнаружены недостатки, то Лицензиат делает записи в Журнал замечаний по результатам контроля (Приложение № 3). На каждое замечание назначается лицо, ответственное за его устранение, а также срок устранения. По результатам работы над замечанием в Журнале замечаний по результатам контроля делается запись о статусе устранения замечания, которая заверяется подписью лица, ответственного за устранение замечания и Администратора СКЗИ.

Администрация обязана принять меры по устранению вскрытых недостатков и выполнению рекомендаций Лицензиата, изложенных в Журнале замечаний по результатам контроля.

Если в ходе контроля выявлены серьезные нарушения в эксплуатации СКЗИ, из-за чего становится реальной утечка конфиденциальной информации, Лицензиат вправе дать указание о прекращении использования СКЗИ до устранения причин выявленных нарушений.

Приложение № 1
к Инструкции по обращению с сертифицированными шифровальными средствами (средствами криптографической защиты информации) в БПОУ ВО «Белозерский индустриально-педагогический колледж им.А.А.Желобовского»

ТИПОВАЯ ФОРМА
журнала поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов

N п/п	Наименование криптосредства, эксплуатационной и технической документации к ним, ключевых документов	Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя криптосредств	Дата и расписка в получении
1	2	3	4	5	6	7	8

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф.И.О. пользователя криптосредств, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены криптосредства	Дата изъятия (уничтожения)	Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15

Приложение № 2
к Инструкции по обращению с сертифицированными шифровальными средствами (средствами криптографической защиты информации) в БПОУ ВО «Белозерский индустриально-педагогический колледж им.А.А.Желобовского»

Журнал контроля соблюдения условий эксплуатации и работоспособности СКЗИ

№ п/п	Вид контроля (плановый/ внеплановый - причина)	Дата контроля	ФИО контролирующего	Результат контроля (без замечаний/ с замечаниями – №№ замечаний по Журналу замечаний)	Подпись контролирующего	Подпись ответственного Организации	№ протокола	Примечания
1								
2								
3								

Приложение № 3
к Инструкции по обращению с сертифицированными шифровальными средствами (средствами криптографической защиты информации) в БПОУ ВО «Белозерский индустриально-педагогический колледж им.А.А.Желобовского»

Журнал замечаний по результатам контроля
(Лист 1)

№ замечания	Содержание замечания	Ответственный по замечанию	Дата замечания	Срок устранения замечания	Статус замечания	Подпись ответственного	Подпись Администратора	Примечание
1								
2								
3								
4								

ЛИСТ
регистрации изменений

(Лист 2)

№ п/п	Дата внесения изменений	Наименование документа, фиксирующего изменения	№№ замененных (исправленных) листов	Подпись лица, внесшего изменения
1. 1.				
1. 2.				
1. 3.				
1. 4.				