Утверждено приказом
Главного врача
Республиканского Центра СПИД
_____/Санчы И.Д./
От «10» января 2023 г. № ___

Инструкция

по обращению с сертифицированными средствами криптографической защиты информации в Государственном бюджетном учреждении здравоохранения Республики Тыва «Республиканский Центр по профилактике и борьбе со СПИД и инфекционными заболеваниями» (Республиканский Центр СПИД)

г. Кызыл
2023 год

Утверждено приказом
Главного врача
Республиканского Центра СПИД
_____/Санчы И.Д./
От «10» января 2023 г. № ___

Инструкция

по обращению с сертифицированными средствами криптографической защиты информации в Государственном бюджетном учреждении здравоохранения Республики Тыва «Республиканский Центр по профилактике и борьбе со СПИД и инфекционными заболеваниями» (Республиканский Центр СПИД)

г. Кызыл
2023 год

1. Общие положения

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 информационных системах.

СКЗИ эксплуатируются в соответствии с правилами пользования ими, указанными в эксплуатационно-технической документации. 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. Термины и сокращения

Лицензиат	Организация, обладающая лицензиями ФСБ России на осуществление деятельности
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 Республиканском Центре СПИД, эксплуатирующей сертифицированные СКЗИ, назначены и закреплены распоряжением следующие лица:

Ответственный за обеспечение безопасности информации (далее - 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.

Обучение Администратора СКЗИ правилам работы с СКЗИ осуществляют сотрудники соответствующего органа криптографической защиты - Лицензиата. Документом, подтверждающим должную специальную подготовку Администратора СКЗИ и возможность его допуска к самостоятельной работе с СКЗИ, является заключение, составленное комиссией соответствующего органа криптографической защиты на основании принятых от этих лиц зачетов по программе обучения.

Пользователей инструктирует и обучает Администратор СКЗИ.

Пользователи СКЗИ обязаны:

1. не разглашать конфиденциальную информацию, к которой они допущены, рубежи ее защиты, в том числе сведения о криптоключах;
2. соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;
3. сообщать в орган криптографической защиты о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;
4. сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным настоящей Инструкцией, при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;
5. немедленно уведомлять орган криптографической защиты о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

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 Республиканского Центра СПИД 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).

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 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.

Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ. На время отсутствия пользователей СКЗИ указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища.

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.), с пометкой в Журнале учета хранилищ. За их

сохранность Администратор и Пользователей СКЗИ несут персональную ответственность.

6. Установка СКЗИ и программного обеспечения на ПЭВМ

Установка и настройка общесистемного, прикладного ПО и дополнительных средств защиты на ПЭВМ с СКЗИ производится Лицензиатом 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 Республиканского Центра СПИД 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, закреплен распоряжением Республиканского Центра СПИД. 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 осуществлении шифрования на пароле и т.д. Администратор СКЗИ основывается на Инструкции по организации парольной защиты в информационных системах Республиканского Центра СПИД.

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 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.

Неиспользованные или выведенные из действия ключевые документы подлежат возвращению в орган криптографической защиты или по его указанию должны быть уничтожены на месте.

Уничтожение криптоключей (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

10. Учет СКЗИ

Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету по установленным формам в соответствии с требованиями Положения ПКЗ-2005.

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 поэкземплярного учета средств криптографической защиты информации (СКЗИ), эксплуатационной и технической документации к ним, ключевых документов.

Данный журнал 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

Контроль за соблюдением правил пользования СКЗИ и условий их использования, указанных в правилах пользования на них, осуществляется:

1. обладателем, пользователем (потребителем) защищаемой информации, установившим режим защиты информации с применением СКЗИ;
2. собственником (владельцем) информационных ресурсов (информационных систем), в составе которых применяются СКЗИ;
3. ФСБ России в рамках контроля за организацией и функционированием криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, систем шифрованной, засекреченной и иных видов специальной связи.

Перечень нормативных правовых документов, связанных с работой со средствами криптографической защиты информации (СКЗИ):

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ.
2. Федеральный закон «О персональных данных» от 27 июля 2006 г. № 152-ФЗ.
3. Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ.
4. «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» (утверждена Приказом ФАПСИ от 13.06.2001 № 152).
5. «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» (Положение «ПКЗ-2005») (утверждено Приказом ФСБ от 9 февраля 2005г. № 66).
6. «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» (утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/6/6-622).
7. «Кодекс РФ об административных правонарушениях (КоАП РФ)» от 30.12.2001 № 195-ФЗ (Глава 13. Административные правонарушения в области связи и информации).
8. «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ (Глава 28. Преступления в сфере компьютерной информации).
9. «Трудовой кодекс Российской Федерации» от 30.12.2001 № 197-ФЗ (Глава 14. Защита персональных данных работника).
10. Эксплуатационная и техническая документация к СКЗИ.