

# АДМИНИСТРАЦИЯ

**БЕРДНИКОВСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ**

**ГЛИНКОВСКОГО районА Смоленской области**

**П О С Т А Н О В Л Е Н И Е**

от 05.06. 2015 г. № 14

|  |  |
| --- | --- |
| Об утверждении инструкции по обеспечению безопасности эксплуатации сертифицированных средств криптографической защиты информации (СКЗИ). |  |

В соответствии с Приказом ФСБ РФ от 9 февраля 2005 года № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005) и требованиями «Инструкции по 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 года № 152

Администрация п о с т а н о в л я е т:

1. Утвердить прилагаемую инструкцию по обеспечению безопасности эксплуатации сертифицированных средств криптографической защиты информации (СКЗИ) в Администрации Бердниковского сельского поселения Глинковского района Смоленской области.

1. Контроль за исполнением настоящего постановления оставляю за собой.

Глава муниципального образования

Бердниковского сельского поселения

Глинковского района Смоленской области Г.Н.Рябенкова

|  |  |
| --- | --- |
|  | Утверждена постановлением Администрации Берднковскогосельского поселения Глинковского района Смоленской области  от 05.16.015 г. № 14 |

**Инструкция**

**по обеспечению безопасности эксплуатации сертифицированных средств криптографической защиты информации (СКЗИ).**

1. **Общие положения.**

1.1. Настоящая Инструкция определяет порядок учета, хранения и использования сертифицированных средств криптографической защиты информации (далее – СКЗИ) и криптографических ключей в целях обеспечения безопасности эксплуатации СКЗИ в Администрации Бердниковского сельского поселения Глинковского района Смоленской области (далее – Администрация), а также в системах электронного документооборота, подключение к которым осуществляется через Администрацию.

1.2. Администрация предоставляет услуги по подключению к системам защищенного электронного документооборота с использованием ЭЦП, таких как система сдача налоговой и бухгалтерской отчетности в ФНС РФ, система сдачи отчетности в ПФР РФ, система сдачи отчетности в Росстат и другие.

* 1. В системах электронного документооборота (СЭД), подключение к которым выполняет Администрация, используются сертифицированные СКЗИ, предназначенные для защиты информации, не содержащей сведений, составляющих государственную тайну.
  2. Для организации и обеспечения работ по техническому обслуживанию СКЗИ и управления криптографическими ключами распоряжением Главы Администрации Участника СЭД назначается Ответственный за эксплуатацию СКЗИ.
  3. Ответственный за эксплуатацию СКЗИ осуществляет:

- поэкземплярный учет предоставленных Участнику СЭД СКЗИ, эксплуатационной и технической документации к ним;

- поэкземплярный учет предоставленных Участнику СЭД СКЗИ, эксплуатационной и технической документации к ним;

- учет Пользователей СКЗИ Участника СЭД;

- контроль за соблюдением условий использования СКЗИ;

- расследования и составления заключения по фактам нарушения условий использования СКЗИ;

* 1. Пользователь СКЗИ обязан:

- не разглашать конфиденциальную информацию, к которой допущен, в том числе сведения о криптографических ключах;

- соблюдать требования по обеспечению безопасности конфиденциальной информации при использовании СКЗИ;

- незамедлительно уведомлять Ответственного за эксплуатацию СКЗИ 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.

* 1. Непосредственно к работе с СКЗИ Пользователи допускаются только после соответствующего обучения.
  2. Обучение Пользователей правилам работы с СКЗИ осуществляет Ответственный за эксплуатацию СКЗИ.
  3. Текущий контроль, обеспечение безопасного функционирования СКЗИ возлагается на Ответственного за эксплуатацию СКЗИ.
  4. Ответственный за эксплуатацию СКЗИ и Пользователи СКЗИ должны быть ознакомлены с настоящей Инструкцией под роспись.

# Учет и хранение СКЗИ и криптографических ключей.

* 1. СКЗИ, эксплуатационная и техническая документация к ним, криптографические ключи подлежат поэкземплярному учету.
  2. Поэкземплярный учет ведет Ответственный за эксплуатацию СКЗИ Участника СЭД в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (Приложение № 1).
  3. Единицей поэкземплярного учета криптографических ключей считается отчуждаемый ключевой носитель.
  4. Все полученные экземпляры СКЗИ, эксплуатационной и технической документации к ним, криптографические ключи должны быть выданы под роспись в Журнале Пользователям СКЗИ. Пользователи СКЗИ несут персональную ответственность за сохранность полученных СКЗИ.
  5. Криптографические ключи хранятся у Пользователей СКЗИ. Хранение осуществляется в сейфах (шкафах, ящиках) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.
  6. Ключевые носители с неработоспособными криптографическими ключами Ответственный за эксплуатацию СКЗИ принимает от Пользователя СКЗИ под роспись в Описи криптографических ключей Пользователя СКЗИ (Приложение 2) и в Журнале поэкземплярного учета (Приложение 1). Неработоспособные ключевые носители подлежат уничтожению.

# Использование СКЗИ и криптографических ключей.

* 1. Во всех СЭД, подключаемых через Администрацию СКЗИ используются для обеспечения конфиденциальности, авторства и целостности электронных документов.
  2. Конфиденциальность электронных документов обеспечивается путем их шифрования. Авторство и целостность электронных документов обеспечивается путем создания ЭЦП Пользователя.
  3. Выполнение криптографических операций построено на использовании двуключевых алгоритмов. Каждый Пользователь является владельцем персонального закрытого и открытого ключей. Открытый ключ используется в составе сертификата X.509 v.3.
  4. Пользователь может выполнять криптографические операции, используя только действующие криптографические ключи.
  5. Реализованные в СКЗИ алгоритмы гарантируют невозможность восстановления закрытого криптографического ключа по открытому ключу.
  6. В случае обнаружения не зарегистрированных программ работа с СКЗИ на данной ПЭВМ должна быть прекращена. По данному факту проводится служебное расследование, и осуществляются работы по анализу и ликвидации последствий данного нарушения.
  7. Правом доступа к рабочим местам с установленными СКЗИ должны обладать только определенные для эксплуатации лица, прошедшие соответствующую подготовку.
  8. Защита информации от несанкционированного доступа (далее - НСД) должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе, при проведении ремонтных и регламентных работ.
  9. К установке общесистемного и специального программного обеспечения, а также СКЗИ, допускаются лица, прошедшие соответствующую подготовку и изучившие документацию на соответствующее программное обеспечение (далее – ПО) и на СКЗИ.
  10. При установке ПО СКЗИ следует:

- на технических средствах, предназначенных для работы с СКЗИ, использовать только лицензионное программное обеспечение фирм — изготовителей;

- при установке ПО СКЗИ на ПЭВМ должен быть обеспечен контроль целостности и достоверность дистрибутива СКЗИ;

- на ПЭВМ не должны устанавливаться средства разработки ПО и отладчики;

- после завершения процесса установки должны быть выполнены действия, необходимые для осуществления периодического контроля целостности установленного ПО СКЗИ, а также его окружения в соответствии с документацией;

* 1. Программное обеспечение, устанавливаемое на ПЭВМ с СКЗИ не должно содержать возможностей, позволяющих:

- модифицировать содержимое произвольных областей памяти;

- модифицировать собственный код и код других подпрограмм;

- модифицировать память, выделенную для других подпрограмм;

- передавать управление в область собственных данных и данных других подпрограмм;

- несанкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;

- повышать предоставленные привилегии;

- модифицировать настройки операционной системы (далее – ОС).

* 1. Средствами BIOS должна быть исключена возможность работы на ПЭВМ с СКЗИ, если во время её начальной загрузки не проходят встроенные тесты.
  2. Администратор безопасности должен сконфигурировать операционную систему, в среде которой планируется использовать СКЗИ, и осуществлять периодический контроль сделанных настроек в соответствии со следующими требованиями:

- не использовать нестандартные, измененные или отладочные версии ОС;

- исключить возможность загрузки и использования ОС, отличной от предусмотренной штатной работой;

- исключить возможность удаленного управления, администрирования и модификации ОС и её настроек;

- на ПЭВМ должна быть установлена только одна операционная система;

- правом установки и настройки ОС и СКЗИ должен обладать только администратор безопасности;

- все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т. п.);

- режимы безопасности, реализованные в ОС, должны быть настроены на максимальный уровень;

- всем пользователям и группам, зарегистрированным в ОС, необходимо назначить минимально возможные для нормальной работы права.

* 1. Необходимо предусмотреть меры, максимально ограничивающие доступ 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;

* 1. Необходимо организовать затирание (по окончании сеанса работы СКЗИ) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы СКЗИ. Если это не выполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям;
  2. Необходимо регулярно устанавливать пакеты обновления безопасности ОС (Service Packs, Hot fix и т.п.), обновлять антивирусные базы, а так же исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС.
  3. Организовать и использовать систему аудита, организовать регулярный анализ результатов аудита.
  4. Организовать и использовать комплекс мероприятий антивирусной защиты.
  5. ЗАПРЕЩАЕТСЯ:

- оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ, после ввода ключевой информации либо иной конфиденциальной информации;

- вносить какие-либо изменения в программное обеспечение СКЗИ;

- осуществлять несанкционированное администратором безопасности копирование ключевых носителей;

- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п. иные средства отображения информации;

- использовать ключевые носители в режимах, не предусмотренных функционированием СКЗИ;

- записывать на ключевые носители постороннюю информацию;

- осуществлять несанкционированное копирование ключевых носителей;

- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер (за исключением случаев, предусмотренных данными правилами);

- вставлять ключевой носитель в устройство считывания в режимах, не предусмотренных штатным режимом использования ключевого носителя;

- подключать к ПЭВМ дополнительные устройства и соединители, не предусмотренные штатной комплектацией;

- работать на компьютере, если во время его начальной загрузки не проходит встроенный тест ОЗУ, предусмотренный в ПЭВМ;

- вносить какие-либо изменения в программное обеспечение СКЗИ;

- изменять настройки, установленные программой установки СКЗИ или администратором;

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

- использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами СКЗИ;

- осуществлять несанкционированное вскрытие системных блоков ПЭВМ.

# 4. Действия при компрометации криптографических ключей.

4.1. К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь, следующие:

- потеря ключевых носителей;

- потеря ключевых носителей с их последующим обнаружением;

- увольнение сотрудников, имевших доступ к ключевой информации;

- нарушение правил хранения и уничтожения (после окончания срока действия) закрытого ключа;

- возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;

- случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника)

4.2. В случае возникновения обстоятельств, указанных в п. 4.1 настоящей Инструкции, Пользователь обязан немедленно прекратить обмен электронными документами с использованием скомпрометированных закрытых криптографических ключей и сообщить о факте компрометации Ответственному за эксплуатацию СКЗИ.

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

|  |  |
| --- | --- |
|  | Приложение №1  к Инструкции по обеспечению безопасности эксплуатации сертифицированных средств криптографической защиты информации (СКЗИ) |

Журнал

поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Наименование СКЗИ,  эксплуатационной и  технической документации  к ним, ключевых документов | Серийные номера СКЗИ  эксплуатационной и  технической документации  к ним, номера серий  ключевых документов | Номера экземпляров ключевых документов | Ф.И.О пользователя СКЗИ | Дата и расписка в получении |
| 1 | 2 | 3 | 4 | 5 | 6 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ф.И.О. сотрудника,  проводившего установку | Дата установки и  подписи лиц, произведших установку | Номера аппаратных  средств, в которые  установлены СКЗИ | Дата  изъятия | Ф.И.О. сотрудника, проводившего изъятие СКЗИ | Примечание |
| 7 | 8 | 9 | 10 | 11 | 12 |

|  |  |
| --- | --- |
|  | Приложение №2  к Инструкции по обеспечению безопасности эксплуатации сертифицированных средств криптографической защиты информации (СКЗИ) |

**ОПИСЬ**

**криптографических ключей Пользователя СКЗИ:**

(ФИО, подразделение, должность)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Дата получения | Номер криптографического ключа | Наименование СКЗИ | Количество ключевых носителей | Возвращено | |
| Дата | Роспись |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |