

**ГЛАВА КАМЫШЛОВСКОГО ГОРОДСКОГО ОКРУГА**

**ПОСТАНОВЛЕНИЕ**

От \_\_\_. \_\_\_.2017 г. № \_\_\_\_

город Камышлов

***О контроле использования средств криптографической защиты информации в администрации Камышловского городского округа***

Для осуществления мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием средств криптографической информации (далее – СКЗИ) информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, с целью реализации системы допуска работников администрации Камышловского городского округа к работе с СКЗИ, в целях исполнения следующих нормативных правовых актов:

1. Федерального Закона от 27.07.2006 №152-ФЗ «О персональных данных».
2. Постановления Правительства Российской Федерации от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
3. Приказа ФСБ России от 10 июля 2014 года №378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности 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».
4. Приказа ФСБ России от 9 февраля 2005 г. №66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005).
5. Приказа ФАПСИ от 13 июня 2001 г. №152 «Об утверждении Инструкции об организации и обеспечении хранения обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»

**ПОСТАНОВЛЯЮ:**

1. Утвердить:

* Положение о контроле использования криптосредств (прилагается).
* Порядок разрешительного доступа пользователей и эксплуатирующего персонала к АРМ с установленным СКЗИ (прилагается).
* Перечень работников администрации Камышловского городского округа, допущенных к самостоятельной работе с СКЗИ (прилагается).

1. Утвердить формы журналов:

* Журнал учета средств криптографической защиты информации, эксплуатационной и технической документации к ним (прилагается).
* Технический (аппаратный) журнал (прилагается).
* Журнал инструктажа персонала (прилагается).
* Журнал учета хранилищ (прилагается).
* Журнал учета мероприятий по контролю организации работ с СКЗИ (прилагается).

1. Возложить функции по организации работ с СКЗИ, выработки соответствующих инструкций для пользователей, а также контролю за соблюдением требований по безопасности на администратора безопасности информации Ульянова Виталия Евгеньевича, ведущего специалиста по информационным технологиям и связи администрации Камышловского городского округа.
2. Администратору безопасности информации в своей деятельности по организации работ с СКЗИ руководствоваться Инструкцией администратора информационной безопасности, Положением о контроле использования криптосредств, Порядком разрешительного доступа пользователей и эксплуатирующего персонала к АРМ с установленным СКЗИ.
3. Администратору безопасности провести инструктаж и обучение пользователя(-ей) СКЗИ и ознакомить под роспись с правилами эксплуатации СКЗИ, Положением о контроле использования криптосредств, Порядком разрешительного доступа пользователей и эксплуатирующего персонала к АРМ с установленным СКЗИ, и с вышеперечисленными нормативными правовыми актами, регулирующими и регламентирующими использование криптосредств.
4. Администратору безопасности своевременно вносить изменения в Перечень работников администрации Камышловского городского округа, допущенных к самостоятельной работе с СКЗИ и представлять Перечень на утверждение.
5. Утвердить перечень автоматизированных рабочих мест для обработки персональных данных с использованием средств криптографической защиты информации (СКЗИ). Ввести в эксплуатацию АРМ с установленными СКЗИ для обработки ПДн согласно утвержденному Перечню (прилагается).
6. Контроль за исполнением постановления оставляю за собой.

И.о. главы

Камышловского городского округа А.В. Половников

СОГЛАСОВАНИЕ

постановления главы Камышловского городского округа

от «\_\_\_» \_\_\_\_\_\_ 2017 г. № \_\_\_\_

О контроле использования средств криптографической защиты информации в администрации Камышловского городского округа

|  |  |  |  |
| --- | --- | --- | --- |
| Должность Ф.И.О. | Дата поступления на согласование | Дата согласования | Замечания и подпись |
| Заместитель главы администрации  Бессонов Е.А. |  |  |  |
| Заместитель главы администрации  Власова Е.Н. |  |  |  |
| Начальник организационного отдела  Власова А.Е. |  |  |  |
| И.о. начальника отдела экономики  Акимова Н.В. |  |  |  |
| Начальник отдела архитектуры и градостроительства  Романов А.В. |  |  |  |
| Начальник отдела жилищно-коммунального и городского хозяйства администрации  Семенова Л.А. |  |  |  |
| Начальник юридического отдела  Усова О.А. |  |  |  |
| Начальник отдела учета и отчетности  Гиндер С.Н. |  |  |  |
| Ведущий специалист по гражданской обороны и пожарной безопасности  Гуляев В.Ж. |  |  |  |
| Главный специалист по учету и распределению жилья администрации  Клементьева И.В. |  |  |  |
| Ведущий специалист по муниципальному контролю  Лихачёв Е.Э. |  |  |  |
| Главный специалист по мобилизационной работе  Панова Е.А. |  |  |  |

Ульянов В.Е., ведущий специалист по информационным технологиям и связи Администрации КГО \_\_\_\_\_\_\_\_ 8 (34375) 2-45-55

Поступило на согласование «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_2017 г.

Отправлено эксперту «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_2017 г.

Отправлено на сайт «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_2017 г.

Данное постановление разослать всем сотрудникам по списку согласования.

И.о. главы

Камышловского городского округа \_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.В. Половников

|  |
| --- |
| Приложение 1  к постановлению главы  Камышловского городского округа  от \_\_\_\_\_\_\_\_\_\_\_\_№\_\_\_\_\_\_  «О контроле использования средств криптографической защиты информации в  администрации Камышловского городского округа» |

**Положение**

**о контроле использования криптосредств**

1. **Общие положения**
   1. Положение о контроле использования криптосредств (далее – Положение) разработано в целях определения порядка применения средств криптографической защиты информации (далее – СКЗИ) в администрации Камышловского городского округа.
   2. К СКЗИ относятся:

* средства шифрования – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации от несанкционированного доступа при ее передаче по каналам связи и (или) при ее обработке и хранении;
* средства имитозащиты – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;
* средства электронной цифровой подписи – аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи;
* средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций;
* средства для изготовления ключевых документов (независимо от вида носителя ключевой информации);
* ключевые документы (независимо от вида носителя ключевой информации).
  1. Действие Положения распространяется на все СКЗИ, используемые в администрации Камышловского городского округа для защиты персональных данных (далее – ПДн), эксплуатационную и техническую документацию к ним.
  2. Для защиты персональных данных, обрабатываемых в информационных системах персональных данных администрации Камышловского городского округа, разрешается использование только сертифицированных в системе сертификации ФСБ России СКЗИ.
  3. Все работники администрации Камышловского городского округа, допущенные к работе с СКЗИ, должны быть ознакомлены с Положением.

1. **Порядок учета средств криптографической защиты информации**
   1. СКЗИ, техническая и эксплуатационная документация к ним подлежат обязательному поэкземплярному учету.
   2. Учет СКЗИ и эксплуатационной и технической документации к ним, учет приема-выдачи СКЗИ технической и эксплуатационной документации к ним работникам администрации Камышловского городского округа осуществляется в Журнале учета средств криптографической защиты информации, эксплуатационной и технической документации к ним(прилагается).
   3. Ответственным за учет СКЗИ и ведение журналов учета является администратор информационной безопасности.
2. **Порядок хранения и использования средств криптографической защиты информации**
   1. Хранение в нерабочее время установочных носителей СКЗИ, эксплуатационной и технической документации к СКЗИ, ключевых документов должно осуществляться в местах, исключающих возможность несанкционированного доступа к ним (в сейфах, в специальных пеналах, в опечатываемых и запираемых шкафах).
   2. Допускается хранение ключевой информации на специальных защищенных устройствах, предназначенных для безопасного хранения данных (USB-ключи eToken) вне специальных мест, обеспечивающих защиту от несанкционированного доступа.
   3. В случае необходимости хранения ключевых документов различных пользователей в одном месте, носители ключевых документов должны храниться в отдельных запечатанных конвертах.
   4. СКЗИ должны использоваться в полном соответствии с эксплуатационной и технической документацией к ним.
   5. Работники администрации Камышловского городского округа допускаются к работе с СКЗИ только после проведения администратором информационной безопасности обучения по вопросам использования СКЗИ.
   6. Администратор информационной безопасности должен вести список обученных пользователей СКЗИ.
   7. При использовании СКЗИ запрещается:

* разглашать информацию о составе СКЗИ, содержании эксплуатационной и технической документации к ним, ключевых документов;
* передавать выданные ключевые документы другим работникам администрации Камышловского городского округа и посторонним лицам;
* устанавливать СКЗИ на технические средства без учета в Журнале учета СКЗИ;
* снимать неучтенные копии с ключевых документов;
* выводить на печать закрытую ключевую информацию;
* допускать вывод ключевых документов на дисплей (монитор) электронно-вычислительных машин, если не обеспечена защита от утечки видовой информации;
* записывать на ключевой носитель постороннюю информацию;
* использовать СКЗИ в целях несоответствующих назначению СКЗИ.

1. **Порядок уничтожения средств криптографической защиты информации**
   1. Решение об уничтожении неиспользованных или выведенных из действия ключевых документов принимает комиссия по уничтожению ключевых документов, назначаемая постановлением главы администрации Камышловского городского округа.
   2. Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ. Если срок уничтожения в эксплуатационной и технической документацией не установлен, то ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из действия.
   3. Уничтожение закрытой ключевой информации производится путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания без повреждения ключевого носителя, в случае возможности его многократного использования.
   4. Уничтожение ключевого носителя осуществляется путем сжигания или измельчения.
   5. Уничтожение ключевой информации с ключевого носителя осуществляется с использованием специального программного обеспечения, гарантирующего уничтожение данных.
   6. В случае прекращения использования программного СКЗИ, установленного на электронно-вычислительной машине, СКЗИ удаляется штатными средствами операционной системы.
   7. Факт уничтожения СКЗИ, технической и эксплуатационной документации к ним должен быть зафиксирован в Журнале учета СКЗИ.
2. **Порядок действий при компрометации закрытых**

**криптографических ключей**

* 1. Криптографические ключи, в отношении которых возникло подозрение в компрометации, а также работающие совместно с ними другие криптографические ключи, необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ.
  2. Скомпрометированные криптографические ключи подлежат уничтожению в соответствии с порядком уничтожения СКЗИ.
  3. По факту компрометации криптографических ключей ответственным за обеспечение безопасности ПДн проводится разбирательство.

1. **Обязанности пользователей средств криптографической защиты информации**
   1. Пользователи СКЗИ обязаны:

* соблюдать требования к обеспечению безопасности СКЗИ;
* сообщать о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ;
* немедленно уведомлять администратора информационной безопасности о фактах утраты ключевых документов;
* сдать СКЗИ, эксплуатационную и техническую документацию к ним при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ.

1. **Ответственность**
   1. Ответственность за соблюдение требований Положения и эксплуатационной и технической документации к СКЗИ несут ответственные пользователи СКЗИ.
   2. Ответственность за контроль выполнения Положения и эксплуатационной и технической документации к СКЗИ несет администратор информационной безопасности.

|  |
| --- |
| Приложение 2  к постановлению главы  Камышловского городского округа  от \_\_\_\_\_\_\_\_\_\_\_\_№\_\_\_\_\_\_  «О контроле использования средств криптографической защиты информации в  администрации Камышловского городского округа» |

**Порядок разрешительного доступа пользователей и эксплуатирующего персонала к АРМ с установленным СКЗИ**

1. **Общие положения**
   1. Настоящий документ описывает порядок разрешительного доступа эксплуатирующего персонала и пользователей к автоматизированным рабочим местам (АРМ) с установленными средствами криптографической защиты (СКЗИ).
2. **Требования к размещению технических средств с установленными СКЗИ** 
   1. При размещении технических средств с установленными СКЗИ необходимо выполнять следующие требования:

* должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены технические средства с установленными СКЗИ, посторонних лиц, по роду своей деятельности, не являющихся персоналом, допущенным к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями и обеспечена невозможность негативных действий с их стороны на СКЗИ, технические средства, на которых эксплуатируется СКЗИ и защищаемую информацию;
* внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию;
* помещения должны быть оснащены входными дверьми с замками, должно быть обеспечено постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода, а также осуществляться опечатывание помещений по окончанию рабочего дня или оборудования помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений;
* ключи от входных дверей должны быть пронумерованы, учтены и выдаваться работникам под расписку в журнале учета хранилищ. Дубликаты ключей от входных дверей следует хранить в сейфе ответственного работника. Хранение дубликатов ключей в других помещениях не допускается;
* для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей должно быть оборудовано необходимое число надежных металлических хранилищ, оснащенных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин. Один экземпляр ключа от хранилища должен находиться у работника, ответственного за хранилище. Дубликаты ключей от хранилищ работники хранят в сейфе администратора информационной безопасности.

1. **Требования к программному и аппаратному обеспечению** 
   1. Технические средства с установленными СКЗИ должны отвечать следующим требованиям:

* На технических средствах, оснащенных СКЗИ должно использоваться только лицензионное программное обеспечение фирм-производителей, либо ПО, сертифицированное ФСБ. Указанное ПО не должно содержать средств разработки или отладки приложений, а также содержать в себе возможностей, позволяющих оказывать воздействие на функционирование СКЗИ. В случае технологических потребностей организации, эксплуатирующей СКЗИ, в использовании иного программного обеспечения, его применения должно быть санкционировано администратором безопасности. В любом случае ПО не должно содержать в себе 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;
* несанкционированное модифицировать файлы, содержащие исполняемые кода при их хранении на жестком диске;
* использовать недокументированные фирмами-разработчиками функции.
* На ПЭВМ одновременно может быть установлена только одна разрешенная ОС.
* В BIOC ПЭВМ должны быть определены установки, исключающие возможность загрузки ОС, отличной от установленной на жестком диске: отключается возможность загрузки с гибкого диска, привода CD-ROM и прочие нестандартные виды загрузки ОС, включая сетевую загрузку. Не применяются ПЭВМ с BIOS, исключающим возможность отключения сетевой загрузки ОС.
* Средствами BIOS должна быть отключена возможность отключения пользователями PCI устройств при использовании ПАК защиты от НСД, устанавливаемых в PCI разъем.
* Вход в BIOS должен быть защищен паролем. Пароль для входа в BIOS должен быть известен только администратору и быть отличным от пароля администратора для входа в ОС.
* Средствами BIOS должна быть исключена возможность работы на ПЭВМ, если во время его начальной загрузки не проходят встроенные тесты.
* Программные модули СКЗИ (прикладного ПО со встроенным СКЗИ) должны быть доступны только по чтению/запуску (в атрибутах файлов запрещена запись и модификация).
* Администратором безопасности должно быть проведено опечатывание системного блока с установленным СКЗИ, исключающее возможность несанкционированного изменения аппаратной части рабочей станции.

1. **Защита информации от НСД** 
   1. При использовании СКЗИ необходимо принять следующие организационные меры:

* Предоставить права доступа к рабочим местам с установленным СКЗИ только лицам, ознакомленным с правилами пользования и изучившим эксплуатационную документацию на СКЗИ.
* Запретить осуществление несанкционированного администратором безопасности копирования ключевых носителей.
* Запретить передачу ключевых носителей лицам, к ним недопущенным.
* Запретить использование ключевых носителей в режимах, не предусмотренных правилами пользования СКЗИ.
* Запретить запись на ключевые носители посторонней информации.
* Запретить оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ после ввода ключевой информации. При уходе пользователя с рабочего места должно использоваться автоматическое включение парольной заставки.
* Хранить ключевые носители в опечатываемых пеналах, которые в свою очередь должны хранить в запираемых и опечатываемых сейфах. Пользователь несет персональную ответственность за хранение личных ключевых носителей.
* Сдать ключевые носители в соответствии с порядком, установленным при увольнении или отстранении от исполнения обязанностей.
* Немедленно уведомлять Удостоверяющий центр о фактах утраты или недостачи ключевых носителей, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению конфиденциальной информации.
* Запрещается разглашать содержимое носителей ключевой информации и передавать носители лицам к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п., иные средства отображения информации.
* Перед началом процесса установки ПО со встроенными модулями СКЗИ, либо автономных программных модулей СКЗИ должен осуществляться контроль целостности устанавливаемого ПО.
* При каждом запуске ПЭВМ с установленным СКЗИ должен осуществляться контроль целостности программного обеспечения, входящего в состав СКЗИ, самой ОС и всех исполняемых файлов, функционирующих совместно с СКЗИ.
* Администратор безопасности должен периодически (не реже 1 раза в год) менять пароль на вход в BIOS.
* В случае обнаружения «посторонних» (незарегистрированных) программ или нарушения целостности программного обеспечения работа должна быть прекращена.
* Пользователь должен запускать только те приложения, которые разрешены администратором.
* Администратор безопасности должен сконфигурировать ОС, в среде которой планируется использовать СКЗИ, и осуществлять периодический контроль сделанных настроек в соответствии со следующими требованиями:
* Не использовать нестандартные, измененные или отладочные ОС.
* Исключить возможность загрузки и использования ОС, отличной от предусмотренной штатной работой.
* Исключить возможность удаленного управления, администрирования и модификации ОС и ее настроек.
* Правом установки и настройки ОС и СКЗИ должен обладать только администратор безопасности.
* ОС должна быть настроена только для работы с СКЗИ. Все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т.п.).
* Всем пользователям и группам, зарегистрированным в ОС, необходимо назначить минимально возможные для нормальной работы права.
* Необходимо предусмотреть меры, максимально ограничивающие доступ к следующим ресурсам системы (в соответствующих условиях возможно полное удаление/ограничение доступа к ресурсу или к его неиспользуемой части):
* системный реестр;
* файлы и каталоги;
* временные файлы;
* журналы системы;
* файлы подкачки;
* кэшируемая информация (пароли и т.п.);
* отладочная информация.
* Кроме того, 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 ОС должна использоваться в однопользовательском режиме и на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям.
* Должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибками ОС, повышать предоставленные привилегии.
* Необходимо регулярно устанавливать пакеты обновления безопасности ОС, обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС.
* В случае подключения ПЭВМ с установленным СКЗИ к общедоступным сетям передачи данных, необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов (JavaScript, VBScript, ActiveX), полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети.
* При использовании СКЗИ на ПЭВМ, подключенных к общедоступным сетям связи, с целью исключения возможности несанкционированного доступа к системным ресурсам используемых ОС, к программному обеспечению, в окружении которого функционируют СКЗИ, и к компонентам СКЗИ со стороны указанных сетей, должны использоваться дополнительные методы и средства защиты.
* Организовать и использовать систему аудита, организовать регулярный анализ результатов аудита.
* Организовать и использовать комплекс антивирусной защиты.
* Исключить одновременную работу в ОС с работающим СКЗИ и загружаемой ключевой информацией нескольких пользователей.

|  |
| --- |
| Приложение 3  к постановлению главы  Камышловского городского округа  от \_\_\_\_\_\_\_\_\_\_\_\_№\_\_\_\_\_\_  «О контроле использования средств криптографической защиты информации в  администрации Камышловского городского округа» |

**Перечень лиц, допускаемых к самостоятельной работе с СКЗИ**

|  |  |  |  |
| --- | --- | --- | --- |
| №  п/п | ФИО работника | Структурное подразделение | Должность |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |
| 6 |  |  |  |
| 7 |  |  |  |

И.о. главы

Камышловского городского округа А.В. Половников

|  |
| --- |
| Приложение 4  к постановлению главы  Камышловского городского округа  от \_\_\_\_\_\_\_\_\_\_\_\_№\_\_\_\_\_\_  «О контроле использования средств криптографической защиты информации в  администрации Камышловского городского округа» |

**Журнал учета средств криптографической защиты информации, эксплуатационной и технической документации к ним**

ИНВ. № \_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| Журнал начат «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. | Журнал завершен «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. |
| Должность | Должность |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / ФИО должностного лица / | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / ФИО должностного лица / |

На \_\_\_\_\_ листах

| № п.п. | Наименование криптосредства, эксплуатационной и технической документации к ним, ключевых документов | Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых докумен-тов | Номера экземпляров (криптографические номера) ключевых документов | Отметка о получении | | Отметка о выдаче | | Отметка о подключении (установке) СКЗИ | | | Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов | | | Примечание |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| От кого получены | Дата и номер сопроводительного письма | Ф.И.О. пользователя криптосредств, производившего подключение (установку) | Дата подключения (установки) и подписи лиц, произведших подключение (установку) | 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 подклю-чены крипто-средства | Дата изъятия (уничто-жения) | Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение) | Номер акта или расписка об уничтожении |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |
| --- |
| Приложение 5  к постановлению главы  Камышловского городского округа  от \_\_\_\_\_\_\_\_\_\_\_\_№\_\_\_\_\_\_  «О контроле использования средств криптографической защиты информации в  администрации Камышловского городского округа» |

**Технический (аппаратный) журнал**

ИНВ. № \_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| Журнал начат «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. | Журнал завершен «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. |
| Должность | Должность |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / ФИО должностного лица / | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / ФИО должностного лица / |

На \_\_\_\_\_ листах

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № п.п | Дата | Тип и серийные номера используемых СКЗИ | Записи по обслуживанию СКЗИ | Используемые криптоключи | | | Отметка об уничтожении (стирании) | | Примечание |
| Тип ключевого документа | Серийный, криптографческий номер и номер экземпляра ключевого документа | Номер разового ключевого носителя или зоны СКЗИ, в которую введены криптоключи | Дата | Подпись пользователя СКЗИ |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

|  |
| --- |
| Приложение 6  к постановлению главы  Камышловского городского округа  от \_\_\_\_\_\_\_\_\_\_\_\_№\_\_\_\_\_\_  «О контроле использования средств криптографической защиты информации в  администрации Камышловского городского округа» |

**Журнал инструктажа персонала**

ИНВ. № \_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| Журнал начат «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. | Журнал завершен «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. |
| Должность | Должность |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / ФИО должностного лица / | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / ФИО должностного лица / |

На \_\_\_\_\_ листах

**Инструктаж по самостоятельной работе с СКЗИ прошел, с нижеперечисленными документами ознакомлен:**

* Федеральный Закон от 27.07.2006 №152-ФЗ «О персональных данных»;
* Постановление Правительства Российской Федерации от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
* Приказ ФСБ России от 10 июля 2014 года №378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных с использованием средств криптографической защиты информации, необходимых для выполнений, установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
* Приказ ФСБ России от 9 февраля 2005 г. №66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005);
* Приказ ФАПСИ от 13 июня 2001 г. №152 «Об утверждении Инструкции об организации и обеспечении хранения обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
* Положение о контроле использования криптосредств;
* Порядок разрешительного доступа пользователей и эксплуатирующего персонала к АРМ с установленным СКЗИ.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Дата | Фамилия, имя, отчество | Должность | Подпись |
| 1 | 2 | 3 | 4 | 5 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |
| --- |
| Приложение 7  к постановлению главы  Камышловского городского округа  от \_\_\_\_\_\_\_\_\_\_\_\_№\_\_\_\_\_\_  «О контроле использования средств криптографической защиты информации в  администрации Камышловского городского округа» |

**Журнал учета хранилищ**

|  |  |
| --- | --- |
| Журнал начат «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. | Журнал завершен «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. |
| Должность | Должность |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / ФИО должностного лица / | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / ФИО должностного лица / |

На \_\_\_\_\_ листах

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Наименование хранилища (помещение, сейф, металлический шкаф) | Инвентарный номер | Местонахождение (подразделение, номер комнаты) | Что находится (документы, изделия) | Ф.И.О. ответственного за сейф (шкаф/помещение) | Кол-во комплектов ключей и их номера | Подпись ответственного за хранилище о выдаче ключа и дата | ФИО и подпись, подтверждающая получение ключа, и дата |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

|  |
| --- |
| Приложение 8  к постановлению главы  Камышловского городского округа  от \_\_\_\_\_\_\_\_\_\_\_\_№\_\_\_\_\_\_  «О контроле использования средств криптографической защиты информации в  администрации Камышловского городского округа» |

**Журнал учета мероприятий по контролю организации работ с СКЗИ**

ИНВ. № \_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| Журнал начат «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. | Журнал завершен «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. |
| Должность | Должность |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / ФИО должностного лица / | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / ФИО должностного лица / |

На \_\_\_\_\_ листах

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Наименование проводимого мероприятия | Дата провидения мероприятия | Исполнитель мероприятия | | Результат (отчет, действия) мероприятия | Подпись и расшифровка подписи |
| ФИО | Должность |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

|  |
| --- |
| Приложение 9  к постановлению главы  Камышловского городского округа  от \_\_\_\_\_\_\_\_\_\_\_\_№\_\_\_\_\_\_  «О контроле использования средств криптографической защиты информации в  администрации Камышловского городского округа» |

**Перечень автоматизированных рабочих мест для обработки персональных данных с использованием средств криптографической защиты информации (СКЗИ).**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № | Тип ОТСС | Модель | Серийный (инв.) номер | Место расположения (этаж, кабинет) | Используемое СКЗИ  (наименование/ серийный номер) | Системный блок опечатан.  Печать № |
| ПЭВМ № 1 (Имя компьютера) – ФИО пользователя | | | | | | |
| 1 | Системный блок |  |  |  |  |  |
| 2 | Монитор |  |  |
| 3 | Клавиатура |  |  |
| 4 | Манипулятор «мышь» |  |  |
| 5 | Принтер |  |  |
| ПЭВМ № 2 (Имя компьютера) – ФИО пользователя | | | | | | |
| 1 | Системный блок |  |  |  |  |  |
| 2 | Монитор |  |  |
| 3 | Клавиатура |  |  |
| 4 | Манипулятор «мышь» |  |  |
| 5 | Принтер |  |  |

И.о. главы

Камышловского городского округа А.В. Половников