ПРАВИТЕЛЬСТВО КУРГАНСКОЙ ОБЛАСТИ

УПРАВЛЕНИЕ ЗАПИСИ АКТОВ ГРАЖДАНСКОГО СОСТОЯНИЯ КУРГАНСКОЙ ОБЛАСТИ

ПРИКАЗ

от 20 апреля 2022 года № 21

г. Курган

Об утверждении мер, направленных на выполнение требований законодательства Российской Федерации в области защиты информации с использованием средств криптографической защиты информации

Во исполнение требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119, приказа ФСБ России от 10.07.2014 N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», а также прочих нормативных документов по защите информации ПРИКАЗЫВАЮ:

1. Утвердить типовую форму журнала поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов (Приложение №1).

2. Утвердить инструкцию по обеспечению безопасности эксплуатации средств криптографической защиты информации в Управление записи актов гражданского состояния Курганской области (Приложение №2).

3. Утвердить список работников Управления записи актов гражданского состояния Курганской области, допущенных к работе с ключами средств криптографической защиты информации (Приложение №3).

4. Утвердить должностную инструкцию пользователей средств криптографической защиты информации (Приложение №4).

5. Утвердить должностную инструкцию ответственного за эксплуатацию криптографических средств защиты информации (приложение №5).

6. Утвердить типовую форму акта о комиссионном уничтожении криптографических ключей (Приложение №6).

7. Утвердить состав комиссии по обучению лиц, допущенных к работе с

средствами криптографической защиты информации (Приложение №7).

8. Утвердить типовую форму лицевого счета пользователя средства криптографической защиты информации (Приложение №8).

9. Утвердить перечень лиц, доступ которых в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и носители ключевой, аутентифицирующей и парольной информации СКЗИ, необходим для выполнения их служебных обязанностей (Приложение № 9).

10. Утвердить типовую форму технического (аппаратного) журнала. (приложение № 10).

11. Утвердить программу обучения пользователей средств криптографической защиты информации (приложение №11).

12. Утвердить форму акта установки СКЗИ, ввода в эксплуатацию и закрепления за ответственным лицом (приложение №12).

13. Контроль за исполнением настоящего приказа оставляю за собой.

Начальник Управления записи
актов гражданского состояния
Курганской области Е.М. Сибиряев

Алексеев В.А.
(3522) 65-00-57

Приложение №1 к приказу
Управления записи актов гражданского состояния Курганской области
от «20» апреля 2022 г. № 21
«Об утверждении мер, направленных на выполнение требований законодательства Российской Федерации в области защиты информации с использованием средств криптографической защиты информации»

Типовая форма журнала поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов

№ 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	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 приказу
Управления записи актов гражданского
состояния Курганской области
от «20» апреля 2022 г. № 21
«Об утверждении мер, направленных на
выполнение требований законодательства
Российской Федерации в области защиты
информации с использованием средств
криптографической защиты информации»

Инструкция по обеспечению безопасности эксплуатации средств криптографической защиты информации в Управлении ЗАГС Курганской области

1. Термины и определения

1.1. В настоящей инструкции по обеспечению безопасности эксплуатации средств криптографической защиты информации (далее - Инструкция) в Управлении записи актов гражданского состояния Курганской области (далее - Управление ЗАГС Курганской области) применяются следующие термины и определения:

Администратор безопасности - должностное лицо, обеспечивающее эксплуатацию средств криптографической защиты информации (далее – СКЗИ) и управление криптографическими ключами.

Безопасность эксплуатации СКЗИ - совокупность мер управления и контроля, защищающая СКЗИ и криптографические ключи от несанкционированного (умышленного или случайного) их раскрытия, модификации, разрушения или использования.

Ответственный за эксплуатацию СКЗИ – сотрудник, осуществляющий организацию и обеспечение работ по техническому обслуживанию СКЗИ и управление криптографическими ключами.

Пользователь - сотрудник, который использует СКЗИ

ПЭВМ - персональная электронно-вычислительная машина (персональный компьютер).

Средства криптографической защиты информации (СКЗИ) - совокупность программно-технических средств, обеспечивающих применение шифрования при осуществлении электронного документооборота, в том числе программное обеспечение с реализацией криптографических функций.

Электронный документ (ЭД) - документ, в котором информация представлена в электронно-цифровой форме.

Остальные термины и определения, используемые в настоящей Инструкции, должны пониматься в соответствии с законодательством Российской Федерации.

2. Общие положения

2.1. Настоящая Инструкция определяет порядок учета, хранения и

использования СКЗИ и криптографических ключей, а также порядок изготовления, смены, уничтожения и действий работников Управления ЗАГС Курганской области при компрометации криптографических ключей в целях обеспечения безопасности эксплуатации СКЗИ.

2.2. Все действия с СКЗИ осуществляются в соответствии с эксплуатационной документацией на СКЗИ.

2.3. Настоящая Инструкция разработана на основе законодательства Российской Федерации, иных правовых актов, а также:

- Приказа ФСБ РФ от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

- Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом ФАПСИ от 13 июня 2001 г. № 152;

- Приказа ФСБ России от 10.07.2014 N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

2.4. Управление ЗАГС Курганской области использует сертифицированные ФСБ России СКЗИ, предназначенные для защиты информации, не содержащей сведений, составляющих государственную тайну.

2.5. Для организации и обеспечения работ по техническому обслуживанию СКЗИ и управления криптографическими ключами приказом начальника Управления ЗАГС Курганской области назначается ответственный за эксплуатацию СКЗИ.

Ответственный за эксплуатацию СКЗИ осуществляет:

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

- учет пользователей СКЗИ;

- контроль за соблюдением условий использования СКЗИ в соответствии с эксплуатационной и технической документацией на СКЗИ и настоящей Инструкцией;

- расследование и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению требуемого уровня безопасности информации;

- разработку и принятие мер по предотвращению возможных негативных последствий подобных нарушений.

2.6. Пользователи СКЗИ назначаются приказом начальника Управления ЗАГС Курганской области.

Пользователь СКЗИ обязан:

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

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

- сдать СКЗИ, эксплуатационную и техническую документацию к ним, криптографические ключи в соответствии с порядком, установленным настоящей Инструкцией, при прекращении использования СКЗИ;

- незамедлительно уведомлять ответственного за эксплуатацию СКЗИ о фактах утраты или недостачи СКЗИ, криптографических ключей, 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.

2.7. Обучение пользователей правилам работы с СКЗИ осуществляет ответственный за эксплуатацию СКЗИ. Ответственный за эксплуатацию СКЗИ должен иметь соответствующий документ о квалификации в области эксплуатации СКЗИ. Непосредственно к работе с СКЗИ пользователи допускаются после обучения и выдачи соответствующего заключения по форме прилагаемой к настоящей инструкции (Приложение 1).

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

2.9. Ответственный за эксплуатацию СКЗИ и Пользователи должны быть ознакомлены с настоящей Инструкцией под роспись.

2.10. В случае, если вход в программное обеспечение СКЗИ осуществляется по паролю тогда организация работы с паролями осуществляется в соответствии с положением по обеспечению безопасности персональных данных при их обработке в Управлении ЗАГС Курганской области. За организацию парольной защиты при работе с СКЗИ несет ответственность ответственный за эксплуатацию СКЗИ.

3. Учет и хранение СКЗИ и криптографических ключей

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

3.2. Поэкземплярный учет СКЗИ ведет ответственный за эксплуатацию СКЗИ в журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним (далее – Журнал) согласно приложению к Инструкции (Приложение № 1). При этом программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатная эксплуатация. Если аппаратные или аппаратно-программные СКЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие СКЗИ учитываются также совместно с соответствующими аппаратными средствами.

3.3. Единицей поэкземплярного учета криптографических ключей считается отчуждаемый ключевой носитель многократного использования. Если один и тот же ключевой носитель многократно используют для записи

криптографических ключей, то его каждый раз следует регистрировать отдельно.

3.4. Все полученные экземпляры СКЗИ, криптографических ключей должны быть выданы под роспись в Журнале пользователям СКЗИ, несущим персональную ответственность за их сохранность.

3.5. При необходимости пользователю выдается документация по эксплуатации СКЗИ с последующим возвратом ответственному за эксплуатацию СКЗИ;

3.6. Дистрибутивы СКЗИ на носителях, эксплуатационная и техническая документация к СКЗИ, инструкции хранятся у ответственного за эксплуатацию СКЗИ. Криптографические ключи хранятся у пользователей СКЗИ. Хранение осуществляется в закрываемых на замок металлических хранилищах пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение или в опечатанном пенале (тубусе). Металлические шкафы должны быть оборудованы внутренними замками с двумя экземплярами ключей и кодовыми замками и приспособлениями для опечатывания. Один экземпляр ключа от хранилища должен находиться у ответственного за эксплуатацию СКЗИ, ответственного за хранилище. Дубликаты ключей от хранилищ сотрудники хранят в специальном сейфе.

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

3.8. На ключевые носители с изготовленными криптографическими ключами наклеиваются наклейки, содержащие надписи: на один ключевой носитель - «Рабочий»; на другой ключевой носитель - «Резервный».

3.9. Ключевой носитель с наклейкой «Резервный» помещается в конверт и опечатывается пользователем и ответственным за эксплуатацию СКЗИ.

3.10. Все полученные экземпляры криптографических ключей должны быть выданы под роспись в Журнале. Резервные криптографические ключи могут находиться на хранении у ответственного за эксплуатацию СКЗИ.

3.11. Ключевые носители с неработоспособными криптографическими ключами ответственный за эксплуатацию СКЗИ принимает от пользователя под роспись в Журнале. Неработоспособные ключевые носители подлежат уничтожению.

3.12. При необходимости замены наклейки на ключевом носителе (стирание надписи реквизитов) пользователь передает его ответственному за эксплуатацию СКЗИ, который в присутствии пользователя снимает старую наклейку и приклеивает новую наклейку с такими же учетными реквизитами.

3.13. Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно-программные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать.

3.14. СКЗИ и криптографические ключи могут доставляться специальной

(фельдъегерской) связью или курьером, имеющего доверенность, подписанную начальником, на право получения СКЗИ, при соблюдении мер, исключающих бесконтрольный доступ к СКЗИ и криптографическим ключам во время доставки.

3.15. Для пересылки СКЗИ и криптографические ключи помещаются в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия, в особенности на записанную ключевую информацию. Криптографические ключи пересылают в отдельном пакете с пометкой «Лично». Упаковки опечатывают таким образом, чтобы исключалась возможность извлечения из них содержимого без нарушения целостности упаковок и оттисков печати.

3.16. Для пересылки СКЗИ, эксплуатационной и технической документации к ним, криптографических ключей составляется Акт приема-передачи (Опись) документов, в котором указывается: что посылается и в каком количестве, учетные номера СКЗИ, криптографических ключей или документов, а также, при необходимости, назначение и порядок использования высылаемого отправления. Акт приема-передачи (Опись) документов вкладывается в упаковку.

3.17. Полученную упаковку вскрывает только лицо, для которого она предназначена. Если содержимое полученной упаковки не соответствует указанному в Акте приема-передачи (Описи) документов или сама упаковка и оттиск печати - их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к ее содержимому, то должен быть составлен акт о происшедшем нарушении. Полученные с такими отправлениями СКЗИ и криптографические ключи до получения указаний от начальника применять не разрешается.

3.18. При обнаружении бракованных криптографических ключей ключевой носитель с такими ключами следует возвратить для установления причин происшедшего и их устранения в дальнейшем. В этом случае необходимо получить новые криптографические ключи.

3.19. Ключевые носители совместно с Журналом должны храниться ответственным за эксплуатацию СКЗИ в сейфе (металлическом шкафу), как правило, в отдельной ячейке. В исключительных случаях допускается хранить ключевые носители и Журнал совместно с другими документами, при этом ключевые носители и Журнал должны быть помещены в отдельную папку.

3.20. На время отсутствия ответственного за эксплуатацию СКЗИ должен быть назначен сотрудник его замещающий.

3.21. При необходимости криптографические ключи сдаются на временное хранение ответственному за эксплуатацию СКЗИ.

4. Использование СКЗИ и криптографических ключей

4.1. Криптографические ключи используются для обеспечения конфиденциальности, авторства и целостности электронных документов.

4.2. Криптографический ключ невозможно использовать, если истек срок действия.

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

4.4. Пользователь должен периодически (ежедневно) проверять сохранность оборудования и целостность печатей на ПЭВМ. В случае обнаружения «посторонних» (не зарегистрированных) программ или выявления факта повреждения печати на системном блоке ПЭВМ работа должна быть прекращена. По данному факту проводится служебное расследование, и осуществляются работы по анализу и ликвидации последствий данного нарушения.

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

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

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

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

4.9. Пользователю ЗАПРЕЩАЕТСЯ:

- осуществлять несанкционированное копирование криптографических ключей; использовать ключевые носители для работы на других рабочих местах или для шифрования и подписи электронных документов;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер;
- вставлять носители криптографических ключей в устройства считывания в режимах, не предусмотренных штатным режимом работы СКЗИ, а также в устройства считывания других ПЭВМ;
- записывать на носители с криптографическими ключами постороннюю информацию;
- подключать к ПЭВМ дополнительные устройства и соединители, не предусмотренные в штатной комплектации;
- работать на ПЭВМ, если во время ее начальной загрузки не проходят

встроенные тесты, предусмотренные в ПЭВМ;

- вносить какие-либо изменения в программное обеспечение СКЗИ;
- для повышения надежности работоспособности криптографических ключей для записи новых криптографических ключей необходимо использовать новые носители информации.

5. Изготовление и плановая смена криптографических ключей

5.1. Изготовление криптографических ключей может производиться администратором безопасности в присутствии пользователя.

5.2. Криптографические ключи изготавливаются на отчуждаемый ключевой носитель (дискету, ruToken, EToken и др.) в соответствии с эксплуатационно-технической документацией на СКЗИ и требованиями безопасности, установленными настоящей Инструкцией.

5.3. В целях обеспечения непрерывности проведения работы плановую смену криптографических ключей следует производить заблаговременно (за 2 (два) месяца до окончания срока действия закрытых криптографических ключей).

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

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

6. Действия при компрометации криптографических ключей

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

- потеря ключевых носителей с рабочими и/или резервными криптографическими ключами;
- потеря ключевых носителей с рабочими и/или резервными криптографическими ключами с последующим их обнаружением;
- увольнение сотрудников, имевших доступ к рабочим и/или резервным криптографическим ключам;
- возникновение подозрений относительно утечки информации или ее искажения;
- нарушение целостности печатей на сейфах (металлических шкафах) с ключевыми носителями с рабочими и/или резервными криптографическими

ключами, если используется процедура опечатывания сейфов;

- утрата ключей от сейфов в момент нахождения в них ключевых носителей с рабочими и/или резервными криптографическими ключами;

- временный доступ посторонних лиц к ключевым носителям, а также другие события, при которых достоверно не известно, что произошло с ключевыми носителями.

6.2. В случае возникновения обстоятельств, указанных в п. 6.1 настоящей Инструкции, пользователь обязан незамедлительно прекратить обмен электронными документами с использованием скомпрометированных закрытых криптографических ключей, по телефону информировать администратора безопасности, ИО за эксплуатацию СКЗИ о факте компрометации используемых закрытых криптографических ключей.

6.3. Решение о компрометации криптографических ключей принимает начальник на основании письменного уведомления о компрометации, подписанного ответственным за эксплуатацию СКЗИ, с приложением, при необходимости, письменного объяснения пользователя по факту компрометации его криптографических ключей.

6.4. Уведомление должно содержать:

- идентификационные параметры скомпрометированного криптографического ключа;

- фамилию, имя, отчество пользователя СКЗИ, который владел скомпрометированным криптографическим ключом;

- сведения об обстоятельствах компрометации криптографического ключа;

- время и обстоятельства выявления факта компрометации криптографического ключа.

6.5. После принятия решения о компрометации ключа принимаются меры о его изъятии из обращения и замены его на новый администратор безопасности после получения информации о компрометации криптографического ключа, убеждается в достоверности полученной информации, выводит из действия ключ подписи, соответствующий скомпрометированному закрытому криптографическому ключу (прекращает обмен электронными документами с использованием сертификата ключа подписи, соответствующего скомпрометированному закрытому криптографическому ключу). Проводит работу по отзыву сертификата ключа подписи пользователя. Отозванный сертификат ключа подписи, соответствующий скомпрометированному закрытому криптографическому ключу пользователя, помещается в список отозванных сертификатов.

6.6. Дата, начиная с которой сертификат ключа подписи считается недействительны, устанавливается равной дате формирования списка отозванных сертификатов, в который был включен отзываемый сертификат ключа подписи.

6.7. Сертификат ключа подписи, соответствующий скомпрометированному закрытому криптографическому ключу, должен храниться ответственным за эксплуатацию СКЗИ в течение срока хранения электронных документов для проведения (в случае необходимости) разбора конфликтных ситуаций,

связанных с применением ЭЦП.

6.8. Пользователь может одновременно иметь несколько закрытых криптографических ключей и соответствующих им сертификатов ключей подписи, часть из которых использовать в качестве рабочих, а часть - в качестве резервных на случай компрометации рабочих закрытых криптографических ключей. Это обеспечивает осуществление непрерывного электронного документооборота за счет оперативного перехода на использование резервных криптографических ключей в случае компрометации рабочих криптографических ключей.

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

7. Уничтожение криптографических ключей

7.1. Неиспользованные или выведенные из действия криптографические ключи подлежат уничтожению.

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

7.3. Криптографические ключи, находящиеся на ключевых носителях, уничтожаются путем их стирания (разрушения) по технологии, принятой для ключевых носителей многократного использования в соответствии с требованиями эксплуатационной и технической документации на СКЗИ.

7.4. При уничтожении криптографических ключей, находящихся на ключевых носителях, необходимо:

- установить наличие оригинала и количество копий криптографических ключей;
- проверить внешним осмотром целостность каждого ключевого носителя;
- установить наличие на оригинале и всех копиях ключевых носителей реквизитов путем сверки с записями в Журнале поэкземплярного учета;
- убедиться, что криптографические ключи, находящиеся на ключевых носителях, действительно подлежат уничтожению;
- произвести уничтожение ключевой информации на оригинале и на всех копиях носителей.

7.5. В Журнале поэкземплярного учета ответственным за эксплуатацию СКЗИ производится отметка об уничтожении криптографических ключей.

8. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся криптографические ключи

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

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

функционирующего с СКЗИ.

8.3. Помещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в режимные помещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в режимные помещения.

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

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

8.6. Двери режимных помещений должны быть постоянно закрыты и могут открываться только для санкционированного прохода работников и посетителей. Ключи от входных дверей нумеруют, учитывают и выдают работникам, имеющим право допуска в режимные помещения, под расписку в журнале учета хранилищ. Дубликаты ключей от входных дверей таких помещений следует хранить в специальном сейфе.

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

8.8. Помещения, в которых используются при работе криптографические ключи, как правило, должны быть оснащены охранной сигнализацией, связанной со службой охраны здания. Сотрудникам, ответственным за охрану здания необходимо проверять периодически исправность сигнализации с отметкой в соответствующих журналах.

8.9. В обычных условиях помещения, находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями или ответственным за эксплуатацию СКЗИ или комиссионно сотрудниками с разрешения руководителя организации.

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

замене.

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

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

Приложение №4 к приказу
Управления записи актов гражданского
состояния Курганской области
от «20» апреля 2022 г. № 21
«Об утверждении мер, направленных на
выполнение требований законодательства
Российской Федерации в области защиты
информации с использованием средств
криптографической защиты информации»

Должностная инструкция пользователей средств криптографической защиты информации

1. Общие положения

Настоящая Инструкция разработана в целях регламентации действий пользователей, допущенных к работе со средствами криптографической защиты информации (СКЗИ) в Управлении ЗАГС Курганской области, которые осуществляют работы с применением СКЗИ (далее – Организация).

Под работами с применением СКЗИ в настоящей Инструкции понимаются защищенное подключение к информационным системам, подписание электронных документов электронной подписью и проверка подписи, шифрование файлов и т.д.

СКЗИ должны использоваться для защиты информации ограниченного доступа (включая персональные данные), не содержащей сведений, составляющих государственную тайну.

Настоящая Инструкция в своем составе, терминах и определениях основывается на положениях «Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденной приказом ФАПСИ от 13 июня 2001 г. №152 (далее – Инструкция ФАПСИ от 13 июня 2001 г. №152), «Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», утвержденного приказом ФСБ РФ от 9 февраля 2005 г. N 66, Приказа ФСБ России от 10.07.2014 N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

2. Термины и определения

Информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами;

Исходная ключевая информация - совокупность данных, предназначенных для выработки по определенным правилам криптоключей;

Ключевая информация - специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока;

Ключевой документ - физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию.

Ключевой носитель - физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации).

Компрометация – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, связанные с криптоключами и ключевыми носителями, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

Криптографический ключ (криптоключ) - совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе;

Орган криптографической защиты (ОКЗ) – структурное подразделение обладателя конфиденциальной информации, разрабатывающее и осуществляющее мероприятия по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ информации ограниченного доступа.

Персональный компьютер (ПК) - вычислительная машина, предназначенная для эксплуатации пользователем Организации в рамках исполнения должностных обязанностей.

Пользователи СКЗИ – работники Организации, непосредственно допущенные к работе с СКЗИ.

Средство криптографической защиты информации (СКЗИ) - совокупность аппаратных и(или) программных компонентов, предназначенных для подписания электронных документов и сообщений электронной подписью, шифрования этих документов при передаче по открытым каналам, защиты информации при передаче по каналам связи, защиты информации от несанкционированного доступа при ее обработке и хранении.

Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

3. Порядок получения допуска пользователей к работе с СКЗИ

3.1. Для работы с СКЗИ привлекаются физические лица, назначенные соответствующим приказом руководителя организации (включенные в перечень пользователей СКЗИ). Основанием для включения в перечень является Заключение о допуске к самостоятельной работе с СКЗИ.

3.2. Решение о готовности пользователя к самостоятельной работе с СКЗИ принимает комиссия на основании результатов принятого у пользователя зачета.

3.3. Для того чтобы получить Заключение о допуске к самостоятельной работе с СКЗИ, пользователю необходимо выполнить следующее:

1) Самостоятельно ознакомиться с положениями

- Федерального закона «Об электронной подписи» № 63-ФЗ от 06.04.2011;
- Приказа ФСБ РФ от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом ФАПСИ от 13 июня 2001 г. № 152;
- Приказа ФСБ России от 10.07.2014 N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
- Федерального закона «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. N 149-ФЗ;
- Федерального закона «О персональных данных» от 27 июля 2006 г. N 152-ФЗ;
- Федеральный закон «Об электронной подписи» от 06.04.2011 №63-ФЗ;
- Данной инструкции.

2) Пройти собеседование на знание правил работы с СКЗИ;

3) При успешном прохождении тестирования пользователь получит Заключение о допуске пользователя к самостоятельной работе с СКЗИ.

4. Обязанности пользователей СКЗИ

4.1. Пользователи СКЗИ обязаны

- не разглашать информацию ограниченного доступа, к которой они допущены, в том числе сведения о криптоключах;
- сохранять носители ключевой информации и другие документы о ключах, выдаваемых с ключевыми носителями;
- соблюдать требования к обеспечению с использованием СКЗИ

безопасности информации ограниченного доступа;

- сообщать в ОКЗ о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

- сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

- немедленно уведомлять ОКЗ 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.

4.2. Пользователь несет ответственность за то, чтобы на ПК, на котором установлены СКЗИ, не были установлены и не эксплуатировались программы (в том числе, программы-вирусы), которые могут нарушить функционирование СКЗИ. На ПК, оборудованном СКЗИ, программное обеспечение должно быть лицензионным.

4.3. При обнаружении на ПК, оборудованном СКЗИ, посторонних программ или вирусов, работа с СКЗИ на данном рабочем месте должна быть прекращена. Незамедлительно организуются мероприятия по анализу и ликвидации негативных последствий данного нарушения.

4.4. Все полученные обладателем информации ограниченного доступа экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем журнале поэкземплярного учета пользователям СКЗИ, несущим персональную ответственность за их сохранность.

4.5. Не допускается

- разглашать информацию ограниченного доступа, к которой был допущен Пользователь СКЗИ;

- разглашать содержимое ключевых носителей или передавать сами носители лицам, к ним не допущенным;

- выводить ключевую информацию на дисплей и(или) принтер;

- вставлять ключевой носитель в порт ПК при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровывание информации, проверка электронной цифровой подписи и т.д.), а также в порты других ПК;

- записывать на ключевом носителе постороннюю информацию;

- вносить какие-либо изменения в программное обеспечение СКЗИ;

- использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования (рекомендуется физическое уничтожение носителей).

4.6. О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием информации ограниченного доступа, пользователи СКЗИ обязаны сообщать Ответственному за организацию работ по криптографической

защите информации.

5. Ответственность пользователей СКЗИ

5.1. Пользователи СКЗИ отвечают за исполнение своих функциональных обязанностей и сохранность информации ограниченного доступа, которая стала ему известной вследствие исполнения им своих служебных обязанностей.

5.2. Ответственность лиц, допущенных к работе с СКЗИ, за неисполнение и/или ненадлежащее исполнение своих обязанностей, предусмотренных соответствующими инструкциями (Инструкция по обращению с СКЗИ, Инструкция пользователя СКЗИ), а также за разглашение информации ограниченного доступа, ставшей ему известной вследствие исполнения им своих служебных обязанностей, определяется действующим законодательством Российской Федерации и условиями трудового договора.

Приложение №1 к должностной инструкции
пользователя средств криптографической
защиты информации

ЗАКЛЮЧЕНИЕ
О ПОДГОТОВКЕ И ДОПУСКЕ К САМОСТОЯТЕЛЬНОЙ РАБОТЕ СО СРЕДСТВАМИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

_____

(должность, фамилия, имя, отчество сотрудника)

_____

(наименование криптосредства, по которому осуществлялась подготовка)

Подготовка начата _____, окончена _____

Пользователь СКЗИ – обязан не разглашать конфиденциальную информацию, к которой допущен, рубежи ее защиты, в том числе сведения о криптоключах;

- соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;
- сообщать сотруднику ответственному за эксплуатацию СКЗИ сведения о ставших ему известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;
- сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с установленным порядком при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;
- немедленно уведомлять орган криптографической защиты о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ (сейфов), 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.

Заключение: На основании принятого зачета указанный пользователь готов(а) к самостоятельной работе с СКЗИ.

С заключением
ознакомлен(а):

_____ _____

(фамилия, инициалы) (подпись)

Ответственный за
эксплуатацию СКЗИ:

_____ _____

(фамилия, инициалы) (подпись)

Приложение №5 к приказу
Управления записи актов гражданского состояния Курганской области
от «28» апреля 2022 г. № 21
«Об утверждении мер, направленных на выполнение требований законодательства Российской Федерации в области защиты информации с использованием средств криптографической защиты информации»

Инструкция ответственного за эксплуатацию криптографических средств защиты информации

1. Общие положения.

1.1. Настоящий документ разработан в соответствии с положениями документа «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 (ФСБ России, № 149/6/6-622, 2008)» (далее Типовые требования).

1.2. Настоящий документ определяет права и обязанности пользователей, ответственных за использование криптосредств в организации.

1.3. Ответственный пользователь криптосредства назначается приказом начальника Управления ЗАГС Курганской области.

2. Ответственный пользователь криптосредства обязан:

2.1. Вести поэкземплярный учет используемых криптосредств, эксплуатационной и технической документации к ним, носителей персональных данных в журнале.

2.2. Вести учет лиц, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности персональных данных в информационной системе (пользователи криптосредств) в журнале.

2.3. Вести и поддерживать в актуальном состоянии лицевые счета пользователей средств криптографической защиты информации.

2.4. Производить установку и ввод в эксплуатацию криптосредств в соответствии с эксплуатационной и технической документацией к этим средствам.

2.5. Проверять готовность криптосредств к использованию с составлением заключений о возможности их эксплуатации.

2.6. Не разглашать информацию, к которой он допущен, в том числе сведения о криптосредствах, ключевых документах к ним и других мерах защиты.

2.7. Соблюдать требования к обеспечению безопасности персональных данных, требования к обеспечению безопасности криптосредств и ключевых документов к ним.

2.8. Сообщать о ставших ему известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним ответственному за защиту информации.

2.9. Немедленно уведомлять ответственного за защиту информации о фактах утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых персональных данных.

2.10. Сдать криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы в соответствующем порядке, при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств.

2.11. Организовывать и проводить собеседования с пользователями криптосредств на знание требований по обращению с СКЗИ, а также знаний законодательства РФ в области эксплуатации криптографических средств.

2.12. Выполнять прочие положения, предусмотренные Типовыми требованиями, в полном объеме.

3. Ответственный пользователь криптосредства имеет право:

3.1. Инициировать разбирательство и составление заключений по фактам нарушения условий хранения носителей персональных данных, использования криптосредств, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений в соответствии с документом «Положение об организации и проведению работ по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных».

4. Ответственному пользователю запрещается:

4.1. Разглашать информацию, к которой он допущен, в том числе сведения о криптосредствах, ключевых документах к ним и других мерах защиты.

С функциональными обязанностями ознакомлен _____/_____

Приложение №6 к приказу
Управления записи актов гражданского состояния Курганской области
от «20» апреля 2022 г. №21
«Об утверждении мер, направленных на выполнение требований законодательства Российской Федерации в области защиты информации с использованием средств криптографической защиты информации»

Типовая форма
Акта о комиссионном уничтожении криптографических ключей

Комиссия в составе:

	ФИО	**Должность**
Председатель		
Секретарь		
Члены комиссии		

провела уничтожение криптографических ключей:

N п/п	**Дата**	**Тип носителя ключа**	**Регистрационный номер носителя ключа**	**Наименование СКЗИ**	**Примечание**

Всего носителей криптографических ключей

_____
(цифрами и прописью)

На указанных носителях криптографические ключи уничтожены путем

_____
(стирания на устройстве гарантированного уничтожения информации и т.п.)

Перечисленные носители криптографических ключей уничтожены путем

_____
(разрезания, сжигания, механического уничтожения, сдачи предприятию по утилизации вторичного сырья и т.п.)

Председатель комиссии: _____/_____

Секретарь комиссии _____/_____

Члены комиссии: _____/_____

_____/_____

_____/_____

Приложение №8 к приказу
Управления записи актов гражданского состояния Курганской области
от «20» апреля 2022 г. № 21
«Об утверждении мер, направленных на выполнение требований законодательства Российской Федерации в области защиты информации с использованием средств криптографической защиты информации»

Типовая форма
лицевого счета пользователя средства криптографической защиты информации

_____

(ФИО, подразделение, должность)

№ п/п	Наименование СКЗИ	Лицензионный номер СКЗИ	Номер дистрибутива СКЗИ	Получено		Возвращено
				Дата	Подпись	Дата
1	2	3	4	5	6	7

Отметка об установке			Отметка об удалении		Примечание
ФИО сотрудника, производившего установку	Дата установки	Учетный номер аппаратного средства	ФИО сотрудника, производившего удаление	Дата удаления	
9	10	11	12	13	14

№ п/п	Наименование носителя КД	Серийный номер носителя КД	Номер КД (номер контейнера, содержащего криптографические ключи)	Серийный номер сертификата ключа подписи в контейнере	Получено		Возвращено	
					Дата	Роспись	Дата	Роспись
1	2	3	4	5	6	7	8	9

Приложение №10 к приказу
Управления записи актов гражданского
состояния Курганской области
от «20» апреля 2022 г. № 21
«Об утверждении мер, направленных на
выполнение требований законодательства
Российской Федерации в области защиты
информации с использованием средств
криптографической защиты информации»

Типовая форма
технического (аппаратного) журнала

N п/п	Дата	Тип и регистрационные номера используемых криптосредств	Записи по обслуживанию криптосредств	Используемые криптоключи			Отметка об уничтожении (стирании)		Примечание
				Тип ключевого документа	Серийный, криптографический номер и номер экземпляра ключевого документа	Номер разового ключевого носителя или зоны криптосредств, в которую введены криптоключи	Дата	Подпись пользователя криптосредств	
1	2	3	4	5	6	7	8	9	10

Приложение №11 к приказу
Управления записи актов гражданского состояния Курганской области
от «20» апреля 2022 г. №21
«Об утверждении мер, направленных на выполнение требований законодательства Российской Федерации в области защиты информации с использованием средств криптографической защиты информации»

ПРОГРАММА
обучения пользователей средств криптографической защиты информации

Тема № 1: «Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».
Содержание:
- основные понятия Федерального закона;
- виды электронных подписей (далее — ЭП);
- обязанности пользователей ЭП;
- удостоверяющий центр и аккредитованный удостоверяющий центр;
- технологии PKI, сертификат ключа проверки ЭП.

Тема № 2: «Приказ ФАПСИ от 13 июня 2001 г. № 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».
Содержание:
- основные понятия Инструкции;
- обязанности пользователей СКЗИ;
- порядок обращения с СКЗИ;
- действия при компрометации.

Тема № 3: «Методические указания при работе с СКЗИ и ключевой информацией».
Содержание:
- действия работника при возникновении штатных и внештатных ситуаций, связанных с использованием СКЗИ и ключевой информации.

№ п/п	Изучаемые темы	Кол-во часов	Форма подготовки
1.	Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»	2	Самостоятельная работа
2.	Приказ ФАПСИ от 13 июня 2001 г. № 152 «Об	2	Самостоятельная

	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»		работа
3.	Методические указания при работе с СКЗИ и ключевой информацией	1	Самостоятельная работа

Приложение №12 к приказу
Управления записи актов гражданского
состояния Курганской области
от «20» апреля 2022 г. № 21
«Об утверждении мер, направленных на
выполнение требований законодательства
Российской Федерации в области защиты
информации с использованием средств
криптографической защиты информации»

Акт
установки средств криптографической защиты информации, ввода в эксплуатацию и закрепления их за ответственным лицом

Настоящий акт составлен о том, что _____ сотрудником
(дата)

_____

_____

_____
(наименование организации, должность, фамилия, имя, отчество, иные сведения (например, дата номер лицензии, в случаях установки средства ЭП с привлечением специализированной организации))

(далее –Уполномоченное лицо) была произведена установка и настройка средства криптографической защиты информации _____

_____
(наименование, версия)

регистрационный номер _____
(регистрационный номер СКЗИ)

(далее - СКЗИ) на ПЭВМ _____
(серийный или инвентарный номер)

расположенный _____
(адрес местонахождения, номер помещения)

ответственного пользователя СКЗИ _____

_____
(ФИО, должность ответственного пользователя СКЗИ)

(далее - пользователь СКЗИ).

Размещение ПЭВМ пользователя, хранение ключевых носителей, охрана помещений организованы установленным порядком.

Обучение правилам работы с СКЗИ и проверка знаний нормативно правовых актов и эксплуатационной и технической документации к нему проведены.

Условия для использования СКЗИ, установленные эксплуатационной и технической документацией к СКЗИ, созданы.

Установленное и настроенное СКЗИ находятся в работоспособном состоянии.

Пользователь СКЗИ обязуется:

- не разглашать конфиденциальную информацию, к которой он допущен, в том числе криптоключи и сведения о ключевой информации;
- соблюдать требования к обеспечению безопасности конфиденциальной

информации с использованием СКЗИ;

- сообщать исполнителю о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

- сдать СКЗИ, установочный комплект к нему, эксплуатационную и техническую документацию, ключевые документы при увольнении или отстранения от исполнения обязанностей, связанных с использованием СКЗИ;

- немедленно уведомлять исполнителя 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, а также о причинах и условиях возможной утечки таких сведений.

Акт составлен в двух экземплярах.

Уполномоченное лицо _____
(подпись) *(Фамилия И.О.)*

«____» _____ 20__ г.

Пользователь СКЗИ _____
(подпись) *(Фамилия И.О.)*

«____» _____ 20__ г.