**ПРАВИТЕЛЬСТВО КУРГАНСКОЙ ОБЛАСТИ**

**УПРАВЛЕНИЕ ЗАПИСИ АКТОВ ГРАЖДАНСКОГО СОСТОЯНИЯ КУРГАНСКОЙ ОБЛАСТИ**

# ПРИКАЗ

06.12.2013 г. № 124

г.Курган

**Об утверждении «Положения об организации и проведении работ в Управлении записи актов гражданского состояния Курганской области по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных»**

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, а также прочих нормативных документов по защите информации

П Р И К А З Ы В А Ю:

1. Утвердить «Положение об организации и проведении работ в Управлении записи актов гражданского состояния Курганской области по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных» согласно приложению 1 к настоящему приказу.
2. Утвердить типовые формы журналов:
- для учета криптосредств, ключевых носителей согласно приложению 2 к настоящему приказу;
- средств защиты информации согласно приложению 3 к настоящему приказу;
- носителей защищаемой информации согласно приложению 4 к настоящему приказу;
- хранилищ согласно приложению 5 к настоящему приказу;
- периодического тестирования средств защиты согласно приложению 6 к настоящему приказу;
- учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн согласно приложению 7 к настоящему приказу;
- учета пользователей, допущенных к информационным системам персональных данных согласно приложению 8 к настоящему приказу;
- проверок электронных журналов согласно приложению 9 к настоящему приказу;
- технического (аппаратного) журнала согласно приложению 10 к настоящему приказу.
3. Утвердить «Матрицу доступа пользователей к техническим, программным средствам и ресурсам информационной системы «Управление ЗАГС Курганской области» согласно приложению 11 к настоящему приказу.
4. Утвердить «Перечень защищаемых информационных ресурсов

информационной системы персональных данных «Управление ЗАГС Курганской области» согласно приложению 12 к настоящему приказу.

5. Утвердить «Модель угроз информационной системы персональных данных «Управление ЗАГС Курганской области».

6. Завести журналы согласно типовых форм и ведение журналов возложить на должностных лиц согласно их обязанностей.

7. Контроль за исполнением настоящего приказа оставляю за собой.

Начальник Управления записи актов
гражданского состояния Курганской области Л.А. Кудимова

Приложение 1 к приказу
Управления записи актов
гражданского состояния
Курганской области
от 06.12.2013 г. № 124

**ПОЛОЖЕНИЕ**
**об организации и проведении работ в Управлении записи актов гражданского состояния Курганской области по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных.**

## 1. Общие положения.

1.1. Данное «Положение об организации и проведению работ в Управлении записи актов гражданского состояния Курганской области по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных» (далее – Положение) разработано в соответствии с Законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», методическими рекомендациями ФСТЭК России и ФСБ России в целях обеспечения безопасности персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных (далее – ИСПДн).

1.2. Положение определяет порядок работы персонала ИСПДн в части обеспечения безопасности ПДн при их обработке, порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений, порядок приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления, порядок обучения персонала практике работы в ИСПДн, порядок проверки электронного журнала обращений к ИСПДн, порядок контроля соблюдения условий использования средств защиты информации, предусмотренные эксплуатационной и технической документацией, правила обновления общесистемного и прикладного программного обеспечения, правила организации антивирусной защиты и парольной защиты ИСПДн, порядок охраны и допуска посторонних лиц в защищаемые помещения.

1.3. При обеспечении безопасности персональных данных в ИСПДн с использованием криптографических средств защиты информации все сотрудники Управления записи актов гражданского состояния Курганской области обязаны выполнять требования, изложенные в документе «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)».

## 2. Порядок контроля защиты информации в ИСПДн и приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления. Порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации и принятие мер по предотвращению возможных опасных последствий.

2.1. Контроль защиты информации в ИСПДн - комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях предупреждения и пресечения возможности получения посторонними лицами охраняемых сведений, выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение характеристик безопасности информации или работоспособности систем информатизации.

2.2. Основными задачами контроля являются:

- проверка организации выполнения мероприятий по защите информации в подразделениях Управления записи актов гражданского состояния Курганской области, учета требований по защите информации в разрабатываемых плановых и распорядительных документах;
- выявление демаскирующих признаков объектов ИСПДн;
- уточнение зон перехвата обрабатываемой на объектах информации, возможных каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;
- проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите информации;
- проверка выполнения требований по защите ИСПДн от несанкционированного доступа;
- проверка выполнения требований по антивирусной защите автоматизированных систем и автоматизированных рабочих мест;
- проверка знаний работников по вопросам защиты информации и их соответствия требованиям уровня подготовки для конкретного рабочего места;
- оперативное принятие мер по пресечению нарушений требований (норм) защиты информации в ИСПДн;
- разработка предложений по устранению (ослаблению) демаскирующих признаков и технических каналов утечки информации.

2.3. Контроль защиты информации проводится с учетом реальных условий по всем физическим полям, по которым возможен перехват информации, циркулирующей в ИСПДн Управления записи актов гражданского состояния Курганской области и осуществляется по объектовому принципу, при котором на объекте одновременно проверяются все вопросы защиты информации. Перечень каналов утечки устанавливается в соответствии с моделью угроз.

2.4. В ходе контроля проверяются:

- соответствие принятых мер по обеспечению безопасности персональных данных (далее – ОБ ПДн);
- своевременность и полнота выполнения требований настоящего Положения и других руководящих документов ОБ ПДн;
- полнота выявления демаскирующих признаков охраняемых сведений об объектах защиты и возможных технических каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на

информацию;

- эффективность применения организационных и технических мероприятий по защите информации;
- устранение ранее выявленных недостатков.

Кроме того, могут проводятся необходимые измерения и расчеты, приглашенными для этих целей специалистами организации, имеющей соответствующие лицензии ФСТЭК России.

2.5. Основными видами технического контроля являются визуально-оптический контроль, контроль эффективности защиты информации от утечки по техническим каналам, контроль несанкционированного доступа к информации и программно-технических воздействий на информацию.

2.6. Полученные в ходе ведения контроля результаты обрабатываются и анализируются в целях определения достаточности и эффективности предписанных мер защиты информации и выявления нарушений. При обнаружении нарушений норм и требований по защите информации администратор безопасности докладывает руководителю для принятия ими решения о прекращении обработки информации и проведения соответствующих организационных и технических мер по устранению нарушения. Результаты контроля защиты информации оформляются актами либо в соответствующих журналах учета результатов контроля.

2.7.Невыполнение предписанных мероприятий по защите ПДн, считается предпосылкой к утечке информации (далее - предпосылка).

По каждой предпосылке для выяснения обстоятельств и причин невыполнения установленных требований по указанию руководителя или ответственного за защиту информации проводится расследование.

Для проведения расследования назначается комиссия с привлечением администратора безопасности. Комиссия обязана установить, имела ли место утечка сведений, и обстоятельства ей сопутствующие, установить лиц, виновных в нарушении предписанных мероприятий по защите информации, установить причины и условия, способствовавшие нарушению, и выработать рекомендации по их устранению. После окончания расследования руководитель принимает решение о наказании виновных лиц и необходимых мероприятиях по устранению недостатков.

2.8.Ведение контроля защиты информации осуществляется путем проведения периодических, плановых и внезапных проверок объектов защиты. Периодические, плановые и внезапные проверки объектов организации проводятся, как правило, силами администратора безопасности и(или) ответственного за защиту информации, в соответствии с утвержденным планом или по согласованию с руководителем.

2.9.Одной из форм контроля защиты информации является обследование объектов ИСПДн. Оно проводится не реже одного раза в год рабочей группой в составе администратора безопасности, ответственного за защиту информации, ответственного за эксплуатацию объекта. Для обследования ИСПДн может привлекаться организация, имеющая лицензию ФСТЭК России на деятельность по технической защите информации. Аттестация ИСПДн проводится с привлечением организации, имеющей лицензию ФСТЭК России на деятельность по технической защите информации, один раз в три года.

2.10. Обследование ИСПДн проводится с целью определения соответствия помещений, технических и программных средств требованиям по защите информации, установленным в "Аттестате соответствия" (если проводилась аттестация) и(или) требованиям по безопасности персональных данных.

2.11. В ходе обследования проверяется:

- соответствие текущих условий функционирования обследуемого объекта ИСПДн условиям, сложившимся на момент проверки;
- соблюдение организационно-технических требований помещений, в

которых располагается ИСПДн;

- сохранность печатей, пломб на технических средствах передачи и обработки информации, а также на устройствах их защиты, отсутствие повреждений экранов корпусов аппаратуры, оболочек кабелей и их соединений с шинами заземления;
- соответствие выполняемых на объекте ИСПДн мероприятий по защите информации данным, изложенным в настоящем положении;
- выполнение требований по защите информационных систем от несанкционированного доступа;
- выполнение требований по антивирусной защите.

2.12. Для выявления радиоэлектронных устройств и проводов неизвестного назначения, преднамеренного нарушения защитных свойств оборудования, а также не предусмотренных правилами эксплуатации отводов от оборудования и соединительных линий, проложенных в выделенных и защищаемых помещениях, а также других нарушений и способов возникновения каналов утечки информации необходимо:

- тщательно осмотреть мебель, сувениры (особенно иностранного производства), оборудование, установленное в этом помещении, осветительную аппаратуру, ниши отопительных батарей, шторы, оконные проемы и т.д.;
- вскрыть и осмотреть розетки, выключатели осветительной сети, люки вентиляции и каналы скрытой проводки;
- проверить качество установки стеклопакетов оконных приемов;
- провести аппаратурную проверку помещения на отсутствие возможно внедренных электронных устройств перехвата информации (при наличии соответствующей аппаратуры), при необходимости для проведения данных видов работ могут привлекаться организации, имеющие соответствующие лицензии ФСБ России.

2.13. Государственный контроль состояния защиты информации осуществляется Федеральной службы по техническому и экспортному контролю России и Федеральной службой безопасности России в рамках их полномочий в соответствии с действующим законодательством Российской Федерации. Доступ представителей указанных федеральных органов исполнительной власти на объекты для проведения проверки, а также к работам и документам в объеме, необходимом для осуществления контроля, обеспечивается в установленном порядке по предъявлении служебного удостоверения сотрудника, а также документа установленной формы на право проведения проверки.

## 3. Порядок обучения персонала практике работы в ИСПДн в части обеспечения безопасности персональных данных.

3.1. Перед началом работы в ИСПДн пользователи должны ознакомиться с инструкциями по использованию программных и технических средств, по использованию средств защиты информации под роспись.

3.2. Пользователи должны продемонстрировать администратору безопасности и(или) ответственному за защиту информации наличие необходимых знаний и умений для выполнения требований настоящего Положения. Администратор безопасности должен вести журнал учета проверок знаний и навыков пользователей.

3.3. Пользователи, демонстрирующие недостаточные знания и умения для обеспечения безопасности персональных данных в соответствии с требованиями настоящего положения, к работе в ИСПДн не допускаются.

3.4. Ответственным за организацию обучения и оказание методической помощи в Управлении записи актов гражданского состояния Курганской области является

администратор безопасности.

3.5. Для проведения занятий, семинаров и совещаний могут привлекаться специалисты по программному и техническому обеспечению, а также специалисты органов по аттестации объектов ИСПДн, организаций-лицензиатов ФСТЭК России и ФСБ России.

3.6. К работе в ИСПДн допускаются только сотрудники прошедшие первичный инструктаж ОБ в ИСПДн и показавшие твердые теоретические знания и практические навыки, о чём делается соответствующая запись в Журнале учёта допуска к работе в ИСПДн.

3.7. Администратор безопасности должен иметь профильное образование (либо дипломы о повышении квалификации) в области защиты информации. Рекомендуется прохождение администратором специализированных курсов по администрированию средств защиты информации, используемых в ИСПДн.

## 4. Порядок проверки электронного журнала обращений к ИСПДн.

4.1. Настоящий раздел Положения определяет порядок проверки электронных журналов обращений к ресурсам ИСПДн.

4.2. Проверка электронного журнала обращений проводится с целью выявления несанкционированного доступа к защищаемой информации в ИСПДн.

4.3. Право проверки электронного журнала обращений имеют:

- администратор безопасности;
- ответственный за защиту информации;
- руководитель.

4.4. На технических средствах ИСПДн, на которых установлены специализированные средства защиты информации (далее – СЗИ) типа «ViPNet», «Secret Net» и другие, проверка электронного журнала производится в соответствии с прилагаемым к указанным СЗИ Руководством.

4.5. Проверке подлежат все электронные журналы ИСПДн.

4.6. Проверка должна проводиться не реже чем один раз в неделю с целью своевременного выявления фактов нарушения требований настоящего Положения.

4.7. Факты проверок электронных журналов отражаются в специальном журнале проверок. После каждой проверки Администратор безопасности делает соответствующую отметку в журнале и ставит свою роспись.

## 5. Правила обновления общесистемного и прикладного программного обеспечения, технического обслуживания ИСПДн, внесения изменений в конфигурацию средств защиты информации.

5.1. Настоящие правила регламентируют обеспечение безопасности информации при проведении обновлении, модификации общесистемного и прикладного программного обеспечения, технического обслуживания и при возникновении нештатных ситуаций в работе ИСПДн.

5.2. Все изменения конфигураций технических и программных средств ИСПДн должны производиться только на основании заявок ответственного за эксплуатацию конкретной ИСПДн.

5.3. Право внесения изменений в конфигурацию аппаратно-программных средств защищенных ИСПДн предоставляется:

- в отношении системных и прикладных программных средств – администратору защиты по согласованию (в случае, если проводилась аттестация) с органом по аттестации, проводившим аттестацию данной ИСПДн;
- в отношении аппаратных средств, а также в отношении программно-

аппаратных средств защиты – администратору защиты по согласованию (в случае, если проводилась аттестация) с органом по аттестации, проводившим аттестацию данной ИСПДн.

5.4. Изменение конфигурации аппаратно-программных средств ИСПДн кем-либо, кроме вышеперечисленных уполномоченных сотрудников и подразделений, **запрещено**.

5.5. Процедура внесения изменений в конфигурацию системных и прикладных программных средств ИСПДн, а также средств защиты информации инициируется заявкой ответственного за эксплуатацию ИСПДн.

5.6. В заявке могут указываться следующие виды необходимых изменений в составе аппаратных и программных средств ИСПДн:

- установка (развертывание) на компьютер(ы) программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи в данной ИСПДн;
- обновление (замена) на компьютере(ах) программных средств, необходимых для решения определенной задачи (обновление версий используемых для решения определенной задачи программ);
- изменение настроек средств защиты информации;
- удаление с компьютера программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на данном компьютере).

5.7. Также в заявке указывается условное наименование ИСПДн. Наименования задач указываются в соответствии с перечнем задач архива дистрибутивов установленного программного обеспечения, которые можно решать с использованием указанного компьютера.

5.8. Заявку ответственного за эксплуатацию ИСПДн, в которой требуется произвести изменения конфигурации, рассматривает руководитель, визирует ее, утверждая тем самым производственную необходимость проведения указанных в заявке изменений.

После чего заявка передается администратору защиты для непосредственного исполнения работ по внесению изменений в конфигурацию компьютера указанного в заявке ИСПДн.

5.9. Подготовка обновления, модификации общесистемного и прикладного программного обеспечения ИСПДн тестирование, стендовые испытания (при необходимости) и передача исходных текстов, документации и дистрибутивных носителей программ в архив дистрибутивов установленного программного обеспечения, внесение необходимых изменений в настройки средств защиты от НСД и средств контроля целостности файлов на компьютерах, (обновление) и удаление системных и прикладных программных средств производится администратором безопасности по согласованию с органом по аттестации (в случае, если проводилась аттестация), проводившим аттестацию данной ИСПДн. Работы производятся в присутствии ответственного за эксплуатацию данной ИСПДн.

5.10. Установка или обновление подсистем ИСПДн должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

5.11. Установка и обновление ПО (системного, тестового и т.п.) на компьютерах производится только с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.), полученных установленным порядком, прикладного ПО – с эталонных копий программных средств, полученных из архива дистрибутивов установленного программного обеспечения.

5.12. Все добавляемые программные и аппаратные компоненты должны быть предварительно установленным порядком проверены на работоспособность, а также

отсутствие опасных функций.

5.13. После установки (обновления) ПО, администратор защиты должен произвести требуемые настройки средств управления доступом к компонентам компьютера и проверить работоспособность ПО и правильность их настройки и произвести соответствующую запись в «Журнале учета нештатных ситуаций в ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн», делает отметку о выполнении (на обратной стороне заявки) и в «Техническом паспорте».

5.14. Формат записей «Журнала учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн» устанавливается приказом руководителя Организации.

5.15. При возникновении ситуаций, требующих передачи технических средств в сервисный центр с целью ремонта, ответственный за ее эксплуатацию докладывает об этом ответственному за защиту информации, который в свою очередь связывается с сотрудниками органа по аттестации (в случае, если проводилась аттестация) и в дальнейшем действует согласно их инструкций. В данном случае администратор защиты обязан предпринять необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера. Оригиналы заявок (документов), на основании которых производились изменения в составе программных средств компьютеров с отметками о внесении изменений в состав программных средств, должны храниться вместе с техническим паспортом на ИСПДн и «Журналом учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн» у ответственного за защиту информации.

5.16. Копии заявок могут храниться у администратора защиты:

- для восстановления конфигурации ИСПДн после аварий;
- для контроля правомерности установки на ИСПДн средств для решения соответствующих задач при разборе конфликтных ситуаций;

для проверки правильности установки и настройки средств защиты ИСПДн

5.17. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом за подписью администратора защиты и сотрудника ответственного за эксплуатацию данной ИСПДн.

## 6. Порядок контроля соблюдения условий использования средств защиты информации, в том числе криптографических.

6.1. Данный раздел Положения определяет порядок контроля соблюдения условий использования средств защиты информации (далее - СЗИ).

6.2. Технические средства защиты информации являются важным компонентом ОБ ПДн.

6.3. Порядок работы с техническими СЗИ определен в соответствующих руководствах по настройке и использованию СЗИ обязательных для исполнения, как сотрудниками обрабатывающими конфиденциальную информацию, так и администратором безопасности ИСПДн.

6.4. Право проверки соблюдения условий использования средств защиты информации имеют:

- руководитель;
- ответственный за защиту информации;
- администратор безопасности.

6.5. Пользователю ИСПДн категорически запрещается:

- обрабатывать конфиденциальную информацию с отключенными СЗИ;
- менять настройки СЗИ.

6.6. Администратору безопасности запрещается менять настройки программно-аппаратных СЗИ предустановленные специалистом организации, имеющей лицензию на деятельность по технической защите информации, без согласования с этой организацией.

6.7. Криптографические средства защиты информации должны использоваться в соответствии с технической и эксплутационной документацией на них, а также в соответствии с правилами пользования ими.

## 7. Порядок управления учетными записями.

7.1. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику, допущенному к работе на компьютерах конкретной ИСПДн, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать на данном компьютере.

7.2. Использование несколькими сотрудниками при работе в ИСПДн одного и того же имени пользователя («группового имени») **запрещено**.

7.3. Процедура регистрации (создания учетной записи) пользователя и предоставления ему (или изменения его) прав доступа к ресурсам ИСПДн инициируется заявкой ответственного за эксплуатацию данной ИСПДн. Форма заявки приведена ниже.

В заявке указывается:

- содержание запрашиваемых изменений (регистрация нового пользователя ИСПДн, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам ИСПДн ранее зарегистрированного пользователя);
- должность (с полным наименованием отдела), фамилия, имя и отчество сотрудника;
- имя пользователя (учетной записи) данного сотрудника;
- полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач в ИСПДн).

7.4. Заявку рассматривает руководитель, визируя её, утверждая тем самым производственную необходимость допуска (изменения прав доступа) данного сотрудника к необходимым для решения им указанных в заявке задач ресурсам ИСПДн. Затем подписывает задание администратору защиты на внесение необходимых изменений в списки пользователей соответствующих подсистем ИСПДн.

7.5. На основании задания, в соответствии с документацией на средства защиты от несанкционированного доступа, администратор защиты производит необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля (возможно также регистрацию персонального идентификатора), заявленных прав доступа к ресурсам ИСПДн и другие необходимые действия, указанные в задании. Для всех пользователей должен быть установлен режим принудительного запроса смены пароля не реже одного раза в течение 360 дней.

7.6. После внесения изменений в списки пользователей администратор защиты должен обеспечить настройки средств защиты соответствующие требованиям безопасности указанной ИСПДн. По окончании внесения изменений в списки пользователей в заявке делается отметка о выполнении задания за подписью исполнителя – администратор защиты.

7.7. Сотруднику, зарегистрированному в качестве нового пользователя ИСПДн, сообщается имя соответствующего ему пользователя и может выдаваться персональный идентификатор (для работы в режиме усиленной аутентификации) и

начальное (-ые) значение (-ия) пароля (-ей), которое (-ые) он обязан сменить при первом же входе в систему.

7.8. Исполненные заявка и задание (за подписью администратора защиты) передаются руководителю на хранение.

Они могут впоследствии использоваться:

- для восстановления полномочий пользователей после аварий ИСПДн;
- для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам ИСПДн при разборе конфликтных ситуаций;
- для проверки сотрудниками контролирующих органов правильности настройки средств разграничения доступа к ресурсам ИСПДн.

## 8. Порядок управления машинными носителями информации.

8.1. Общие положения

8.1.1. Настоящий порядок устанавливает основные требования к организации учета и использования машинных носителей данных, предназначенных для обработки и хранения персональных данных в ИСПДн.

8.1.2. Ответственность за организацию учета и использования машинных носителей данных, предназначенных для обработки и хранения персональных данных, возлагается на администратора защиты.

8.1.3. Учет машинных носителей информации осуществляется в соответствии с формой учетной документации.

8.1.4. Все машинные носители данных, используемые при работе со средствами вычислительной техники (СВТ) для обработки и хранения персональных данных, должны обязательно регистрироваться и учитываться. Допускается автоматизированный учет машинных носителей информации.

8.1.5. Проверка наличия машинных носителей данных, предназначенных для обработки и хранения персональных данных, проводится в сроки, установленные настоящим порядком.

8.1.6. Вынос съемных носителей за пределы контролируемой зоны запрещен. Периодические проверки (не реже одного раза в месяц) наличия всех учтенных носителей в пределах контролируемой зоны проводятся администратором защиты и(или) руководителем подразделения. В случае выявления факта выноса съемного носителя за пределы контролируемой зоны инициируется служебная проверка. Факт фиксируется в журнале учета нештатных ситуаций ИСПДн.

8.1.7. Запрещено использование в служебных целях личных, неучтенных носителей информации. Периодические проверки (не реже одного раза в месяц) использования личных, неучтенных носителей в пределах контролируемой зоны проводятся администратором защиты и(или) руководителем подразделения. В случае выявления факта использования личных, неучтенных носителей в пределах контролируемой зоны инициируется служебная проверка. Факт фиксируется в журнале учета нештатных ситуаций ИСПДн, носитель изымается по акту для проведения процедуры принудительного стирания информации, после которой возвращается владельцу полностью отформатированным.

8.2. Учет машинных носителей информации

8.2.1. К машинным носителям информации относятся:

- магнитные ленты в кассетах;
- съемные носителя информации всех видов и способов подключения;
- несъемные жесткие магнитные диски.

8.2.2. Каждый машинный носитель данных, применяемый при обработке персональных данных в ИСПДн, должен иметь гриф – «конфиденциально».

8.2.3. Персональную ответственность за сохранность полученных машинных

носителей данных и предотвращении несанкционированного доступа к записанной на них информации несет сотрудник, получивший эти носители.

8.2.4. При обработке персональных данных на СВТ должен соблюдаться следующий общий порядок учета, хранения и уничтожения машинных носителей данных.

8.2.4.1. Учет машинных носителей данных, предназначенных для записи персональных данных производится в Журнале учета машинных носителей информации.

8.2.4.2. Каждому носителю информации присваивается учетный номер, который состоит из кода машинного носителя, номера объекта и порядкового номера по журналу учета машинных носителей информации.

8.2.4.3. Учетный номер и гриф «конфиденциально» наносятся на носитель информации или его корпус. Если невозможно маркировать непосредственно машинный носитель данных, то маркируется упаковка, в которой хранится носитель. В этом случае учетный номер записывается также на носитель машинным способом.

8.2.4.4. Хранение их должно осуществляться в условиях, исключающих возможность хищения, приведения в негодность или уничтожения содержащейся на них информации.

8.2.4.5. Машинные носители данных после стирания с них персональных данных, с учета не снимаются, а хранятся наравне с другими машинными носителями.

8.2.4.6. В последующем эти носители используются для записи персональных данных. Если носители не пригодны для дальнейшего использования, они подлежат уничтожению по соответствующему акту.

8.2.4.7. О фактах утраты машинных носителей с грифом «конфиденциально» незамедлительно докладывается руководству и администратору защиты, проводится служебное расследование.

8.2.4.8. Машинные носители данных должны пересылаться, по возможности, в металлических коробках, помещаемых в пакет, в упаковках, конвертах тем же порядком, что и конфиденциальные документы. На пакетах, упаковках, конвертах с носителями делается надпись: «Осторожно, машинные носители информации. Не прошивать».

8.2.4.9. Машинные носители данных выдаются операторам или другим лицам, участвующим в обработке информации, для работы под расписку в Журнале учета машинных носителей информации. По завершению работы машинные носители данных сдаются ответственному (руководителю подразделения за их хранение.

8.2.4.10. Копирование информации, содержащей персональные данные, с машинных носителей производится с разрешения руководства Управления записи актов гражданского состояния Курганской области по заявке руководителя отдела.

8.2.4.11. Машинные носители с персональными данными, утратившими практическое значение или пришедшие в негодность, уничтожаются по соответствующему акту.

8.2.5. При подготовке документов должны соблюдаться следующие особенности учета, хранения и уничтожения машинных носителей данных.

8.2.5.1. Машинные носители данных, предназначенные для записи персональных данных, выдаются сотрудникам по письменному разрешению руководства Управления записи актов гражданского состояния Курганской области в необходимом для работы количестве под расписку в Журнале учета машинных носителей информации.

8.2.5.2. Несъемные жесткие магнитные диски закрепляются за сотрудником, ответственным за СВТ, в котором они установлены.

8.2.5.3. В случае повреждения машинных носителей данных, содержащих персональные данные, сотрудник, в пользовании которого они находятся, обязан

сообщить о случившемся администратору защиты.

8.2.5.4. В случае необходимости (командировка, отпуск и т. д.) машинные носители с персональными данными, сдаются сотрудником ответственному лицу на постоянное или временное хранение в опечатанном виде. При этом на упаковке указывается срок их хранения, заверенный личной подписью сотрудника. По истечению указанного срока информация может быть уничтожена, а носители могут повторно использоваться.

8.2.5.5. Копирование персональных данных, с машинных носителей с целью передачи другим сотрудникам производится с разрешения начальника отдела.

8.2.5.6. Копирование осуществляется только на тех СВТ, на которых разрешена обработка персональных данных, и только на те носители, которые соответствуют грифу «конфиденциально».

8.2.5.7. Передача скопированной информации третьим лицам производится по письменному разрешению руководства Управления записи актов гражданского состояния Курганской области.

8.2.5.8. Хранящиеся на магнитных носителях и потерявшие актуальность персональные данные должны своевременно стираться (уничтожаться). Ответственность за это несет владелец информации.

8.2.6. Начальник отдела не реже одного раза в год создает комиссию по проверке наличия и условий хранения персональных данных.

8.3.Порядок уничтожения машинных носителей, содержащих персональные данные

8.3.1. В обязательном порядке уничтожению подлежат поврежденные, выводимые из эксплуатации носители, содержащие защищаемую информацию, использование которых не предполагается в дальнейшем. Стиранию подлежат носители, содержащие защищаемую информацию, которые выводятся из эксплуатации в составе ИСПДн. Не допускается стирание неисправных носителей и передача их в сервисный центр для ремонта. Такие носители должны уничтожаться в соответствии с настоящим порядком.

8.3.2. Стирание должно производиться по технологии, предусмотренной для данного типа носителя, с применением сертифицированных средств гарантированного уничтожения информации (допускается задействовать механизмы затирания встроенные в сертифицированные средства защиты информации).

8.3.3. Уничтожение носителей производится путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления информации (перед уничтожением, если носитель исправен, должно быть произведено гарантирование стирание информации на носителе). Непосредственные действия по уничтожению конкретного типа носителя должны быть достаточны для исключения возможности восстановления информации.

8.3.4. Бумажные и прочие сгораемые носители (конверты с неиспользуемыми более паролями) уничтожают путем сжигания или с помощью любых бумагорезательных машин.

8.3.5. По факту уничтожения или стирания носителей составляется акт, в журналах учета делаются соответствующие записи.

8.3.6. Процедуры стирания и уничтожения осуществляются комиссией, в которую входят: ответственный за эксплуатацию ИСПДн, ответственный за защиту информации, администратор безопасности.

## 9. Порядок использования мобильных технических средств и беспроводной сети передачи данных.

9.1.В ИСПДн разрешается применение мобильного технического средства -

ноутбука для проведения торжественных регистраций брака. Ноутбук подключается к ИСПДн с помощью технологии беспроводной сети.

9.2. Применение прочих мобильных технических средств в ИСПДн запрещено.

9.3. Использование беспроводной сети для прочих подключений запрещено.

9.4. Беспроводная сеть должны быть скрытой (не обнаруживаемой) с применением стойкого шифрования.

9.5. Для подключения ноутбука к ИСПДн через беспроводную сеть передачи данных должно в обязательном порядке дополнительно применяться сертифицированное СКЗИ.

9.6. Для ноутбука должны быть определено одно постоянное место, на которое он устанавливается при работе через беспроводную сеть передачи данных.

9.7. После окончания торжественной регистрации, необходимо обеспечить хранение ноутбука как съемного носителя персональных данных.

9.8. После окончания торжественной регистрации необходимо физически отключить беспроводную сеть.

## 10. Порядок управления взаимодействием с информационными системами сторонних организаций.

10.1. Информационное взаимодействие с системами сторонних организаций допускается только при условии заключения соглашения о взаимодействии.

10.2. Соглашение должно предусматривать технические способы взаимодействия, соответствующие требованиям безопасности информации.

10.3. Соглашение должно предусматривать формат запросов и способов обмена информацией.

10.4. В сторонней организации должны быть назначены лица, ответственные за информационное взаимодействие. Со стороны Управления записи актов гражданского состояния Курганской области ответственным является администратор защиты.

10.5. Меры защиты информации, принятые в сторонней организации, должны обеспечивать уровень защищенности персональных данных и безопасности информации не ниже, чем в Управлении записи актов гражданского состояния Курганской области. В противном случае информационное взаимодействие не допускается.

10.6. Информационное взаимодействие с использованием сетей передачи данных, выходящих за пределы контролируемой зоны допускается только с применением средств криптографической защиты информации.

10.7. Администратор защиты имеет право прекратить информационное взаимодействие техническими мерами, в случае обнаружения фактов несоблюдения сторонней организацией требований по защите персональных данных.

## 11. Порядок управления виртуальными машинами и обрабатываемыми на них данными.

11.1. При эксплуатации виртуальных машинных следует рассматривать их как приложения, обрабатывающие персональные данные и выполнять соответствующие требования безопасности информации.

## 12. Заключительные положения.

12.1. Требования настоящего Положения обязательны для всех сотрудников обрабатывающих конфиденциальную информацию (персональные данные).

12.2. Нарушение требований настоящего Положения влечет за собой

дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение 2 к приказу
Управления записи актов
гражданского состояния
Курганской области
от 06.12.2013 г. № 124

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 (криптографичес-кие номера) ключевых документов | Отметка о получении | | Отметка о выдаче | |
|---|---|---|---|---|---|---|---|
| | | | | От кого получены | Дата и номер сопроводи-тельного 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 кото-рым подклю-чены крипто-средства | Дата изъятия (уничто-жения) | Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение) | Номер акта или расписка об уничтожении | |
| 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| | | | | | | |

Приложение 3 к приказу
Управления записи актов
гражданского состояния
Курганской области
от 06.12.2013 г. № 124

ТИПОВАЯ ФОРМА
журнала поэкземплярного учета средств защиты информации, эксплуатационной и технической документации к ним

| № п.п. | Наименование средства защиты информации, эксплуатационной и технической документации к ним, ключевых документов | Регистрационные номера СЗИ, эксплуатационной и технической документации к ним | Отметка о получении | | Отметка о выдаче | |
|---|---|---|---|---|---|---|
| | | | От кого получены | Дата и номер сопроводи-тельного письма | Ф.И.О. пользователя | Дата и расписка в получении |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| | | | | | | |

| Отметка о подключении (установке) СЗИ | | | Отметка об изъятии СЗИ из аппаратных средств | | | Примечание |
|---|---|---|---|---|---|---|
| Ф.И.О. пользователя, производившего подключение (установку) | Дата подключения (установки) и подписи лиц, произведших подключение (установку) | Номера аппаратных средств, в которые установлены или к кото-рым подклю-чены СЗИ | Дата изъятия (уничто-жения) | Ф.И.О. пользователя СЗИ, производившего изъятие (уничтожение) | Номер акта или расписка об уничтожении | |
| 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| | | | | | | |

Приложение 4 к приказу
Управления записи актов
гражданского состояния
Курганской области
от 06.12.2013 г. № 124

ТИПОВАЯ ФОРМА
журнала учета машинных носителей информации

| № п/п | Регистрационный (учетный) номер носителя | Вид носителя | Тип носителя и его емкость | Дата поступления |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| | | | | |

| Расписка в получении (ФИО, подпись, дата) | Расписка в обратном приеме (ФИО, подпись, дата) | Место хранения | Дата и номер акта об уничтожении | Примечание |
|---|---|---|---|---|
| 6 | 7 | 8 | 9 | 10 |
| | | | | |

Приложение 5 к приказу
Управления записи актов
гражданского состояния
Курганской области
от 06.12.2013 г. № 124

ТИПОВАЯ ФОРМА
журнала учета хранилищ

| № п/п | Регистрационный (учетный) номер хранилища | Вид хранилища | Дата постановки на учет | Фамилия и подпись принявшего (ответственного), дата |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| | | | | |

| Место расположения (номер помещения) | Дата и номер акта о выводе из эксплуатации | Примечание |
|---|---|---|
| 6 | 7 | 8 |
| | | |

Приложение 6 к приказу
Управления записи актов
гражданского состояния
Курганской области
от 06.12.2013 г. № 124

ТИПОВАЯ ФОРМА
журнала периодического тестирования средств защиты информации

| № п/п | Наименование средства защиты информации от НСД или криптосредства | Регистрационные номера СЗИ от НСД или криптосредства | Дата тестирования | Фамилия и подпись ответственного пользователя, проводившего тестирование |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| | | | | |

| Наименование теста, используемые средства для проведения теста | Результат тестирования (успешный/неуспешный), комментарий | Дата очередного тестирования |
|---|---|---|
| 6 | 7 | 8 |
| | | |

Приложение 7 к приказу
Управления записи актов
гражданского состояния
Курганской области
от 06.12.2013 г. № 124

ТИПОВАЯ ФОРМА
журнала учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн

| № п/п | Дата | Краткое описание выполненной работы (нештатной ситуации) | ФИО исполнителей и их подписи |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| | | | |

| ФИО ответственного за эксплуатацию ПЭВМ, подпись | Подпись специалиста по защите информации | Примечание (ссылка на заявку) |
|---|---|---|
| 5 | 6 | 7 |
| | | |

Приложение 8 к приказу
Управления записи актов
гражданского состояния
Курганской области
от 06.12.2013 г. № 124

ТИПОВАЯ ФОРМА
журнала учета пользователей, допущенных к информационным системам персональных данных

| № п/п | Дата | Фамилия, имя, отчество пользователя | Наименование ИСПДн |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| | | | |

| Подпись пользователя об ознакомлении с Положением и требованиями по безопасности | Подпись администратора безопасности о готовности пользователя к работе в ИСПДн | Примечание |
|---|---|---|
| 5 | 6 | 7 |
| | | |

Приложение 9 к приказу
Управления записи актов
гражданского состояния
Курганской области
от 06.12.2013 г. № 124

ТИПОВАЯ ФОРМА
Журнала проверок электронных журналов

| № п/п | Дата проверки | Наименование ИСПДн, компьютера, технического средства | Наименование проверяемого журнал |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| | | | |
| | | | |

| Выявленные нарушения требований безопасности, нештатные ситуации | Подпись администратора безопасности | Примечание |
|---|---|---|
| 5 | 6 | 7 |
| | | |

Приложение 10 к приказу
Управления записи актов
гражданского состояния
Курганской области
от 06.12.2013 г. № 124

ТИПОВАЯ ФОРМА
технического (аппаратного) журнала

| № 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 |
| | | | | | | | | | |