УТВЕРЖДАЮ

Главный врач
ГБУЗ «Кузнецкая межрайонная больница»

_____ А.В. Потапов

/____ /_____/ 2016 г.

Государственное бюджетное учреждение здравоохранения «Кузнецкая межрайонная больница»

Защита персональных данных

ПОЛОЖЕНИЕ ОБ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

_____ №_____

Листов 53

2016

Оглавление

1 УСЛОВНЫЕ ОБОЗНАЧЕНИЯ, СОКРАЩЕНИЯ И ПОНЯТИЯ

Автоматизированная обработка персональных данных	**Автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники.
Информационная система персональных данных	**Информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
Обезличивание персональных данных	**Обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.
Обработка персональных данных	**Обработка персональных данных** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.
Оператор	**Оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.
ПДн	**Персональные данные** - Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
Распространение персональных данных	**Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.
РФ	Российская Федерация
Уничтожение персональных данных	**Уничтожение персональных данных** – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.
ФЗ	Федеральный закон

2 КОНТРОЛЬ ВЕРСИЙ ДОКУМЕНТА

Версия	Описание изменений	Дата

3 ВВЕДЕНИЕ

Настоящее Положение разработано в соответствии с законодательством Российской Федерации о персональных данных (далее – ПДн) и нормативно-методическими документами исполнительных органов государственной власти по вопросам безопасности ПДн, в том числе при их обработке в информационных системах персональных данных (далее – ИСПДн), а также внутренними документами по информационной безопасности Государственного бюджетного учреждения здравоохранения «Кузнецкая межрайонная больница» (далее – Учреждение).

3.1 Основными нормативно-правовыми и методическими документами, на которых базируется настоящее Положение, являются:

- Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»), устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн.
- Требования к защите персональных данных при их обработке в информационных системах персональных данных. Утверждены Постановлением Правительства Российской Федерации от 01.10.2012 г. №1119.
- Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России 18.02.2013 г. №21.
- «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденное Постановлением Правительства РФ от 15.09.2008 г. № 687.

3.2 Для осуществления мероприятий по обеспечению и контролю безопасности персональных данных приказом главного врача Учреждения назначается сотрудник, ответственный за организацию обработки персональных данных.

3.3 Для осуществления обработки обращений субъектов ПДн и запросов уполномоченного органа по защите прав субъектов ПДн приказом главного врача Учреждения назначается ответственный по обращениям и запросам (ответственный за организацию обработки персональных данных).

4 НАЗНАЧЕНИЕ И ОБЛАСТЬ ДЕЙСТВИЯ

4.1 Настоящее Положение предназначено для организации в Учреждении процесса обеспечения безопасности ПДн согласно требованиям действующего федерального законодательства.

4.2 Действие настоящего Положения распространяется на все процессы по сбору, записи, систематизации, накоплению, хранению, уточнению, извлечению, использованию, передаче (распространению, предоставлению, доступу), обезличиванию, блокированию, удалению, уничтожению ПДн, осуществляемые с использованием средств автоматизации и без их использования.

4.3 Положение обязательно для ознакомления и исполнения Администраторами ИСПДн, Ответственным за организацию обработки персональных данных, Координатором по обращениям и запросам, и остальными работниками Учреждения, которые участвуют в процессах обработки персональных данных.

4.4 Работники Учреждения должны быть ознакомлены с настоящим Положением под росписью в «Листе ознакомления».

4.5 В случае нарушения норм настоящего Положения, или иных норм, закрепленных в законодательстве Российской Федерации и регулирующих обработку и защиту персональных данных, лица, допустившие такие нарушения, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

5 МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ

5.1 Учреждение обязано при обработке персональных данных принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

5.2 Обеспечение безопасности персональных данных достигается, в частности:

- предоставлением доступа к персональным данным, обрабатываемым в информационных системах персональных данных, для работников Учреждения, которым такой доступ необходим для выполнения их должностных обязанностей;
- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных, формирование на их основе модели угроз;
- определением требуемого уровня защищённости информационной системы персональных данных;
- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- проверкой готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации (Приложение 7.);
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- установкой и вводом в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учетом машинных носителей персональных данных (Приложение 4., Приложение 5.);
- учетом лиц, допущенных к работе с персональными данными в информационной системе (Приложение 3.);
- учетом применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных (Приложение 6.);
- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;
- проведением разбирательств и составление заключений по фактам несоблюдения условий хранения материальных носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
- обучением лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
- установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- контролем за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

5.3 Доступ к персональным данным должен предоставляться работникам Учреждения исключительно в пределах и объеме, необходимых для выполнения ими своих должностных обязанностей. Работнику запрещается работать с персональными данными, обработка которых не входит в его должностные обязанности.

5.4 В Учреждении ведется список работников, допущенных к обработке персональных данных (Приложение 3.Список работников, допущенных к обработке персональных данных (типовая форма)).

6 ОБЯЗАТЕЛЬНЫЕ МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИСПДН

6.1 Общие требования

6.1.1. В целях обеспечения безопасности персональных данных, обрабатываемых в информационных системах Учреждения, создается система защиты персональных данных, включающая в себя правовые, организационные и технические меры.

6.1.2. Система защиты персональных данных должна создаваться на основании следующих основных принципов:

- *Принцип правовой защищенности*. Обеспечение безопасности персональных данных должно осуществляться в соответствии с требованиями нормативно-правовых актов Российской Федерации в области защиты персональных данных;
- *Принцип достаточности*. Система защиты персональных данных должна обеспечивать необходимый уровень безопасности персональных данных, без её чрезмерного усложнения;
- *Принцип эффективности*. Применяемые средства защиты информации не должны существенно ухудшать основные функциональные характеристики и производительность информационных систем Учреждения. Необходимо найти баланс между обеспечением безопасности персональных данных и удобством использования информационных систем;
- *Принцип своевременности*. Принимаемые меры по обеспечению безопасности персональных данных должны носить в первую очередь упреждающий характер и должны быть приняты до начала обработки персональных данных в информационных системах.

6.1.3. В ходе проведения работ по обеспечению безопасности персональных данных предварительно должна быть проведена инвентаризация ИСПДн.

6.1.4. Процедура инвентаризации информационных систем, посредством которых осуществляется обработка персональных данных, производится при помощи интервьюирования (опроса) или анкетирования владельцев данных информационных систем.

6.1.5. Перечень обнаруженных информационных систем, посредством которых осуществляется обработка персональных данных, должен быть документально зафиксирован и согласован (Приложение 1.)Приложение 1..

6.1.6. Периодически необходимо производить актуализацию данного перечня информационных систем, посредством которых осуществляется обработка персональных данных.

6.1.7. Информационные системы, посредством которых осуществляется обработка персональных данных, подлежат обязательной процедуре определения необходимого уровня защищённости, с целью установления организационных и технических, необходимых для обеспечения безопасности персональных данных. Определение уровня защищённости информационной системы производится на этапе их создания, или в ходе эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем).

6.1.8. Определение требуемого уровня защищённости информационной системы производится в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными Постановлением Правительства Российской Федерации от 01.10.2012 г. №1119. Определение уровня защищённости ИСПДн производится в следующей последовательности:

- создается Комиссия по проведению определения требуемого уровня защищённости ИСПДн;
- комиссия устанавливает требуемый уровень защищённости ИСПДн, а также определяет наличие в ИСПДн специальных категорий персональных данных, биометрических персональных данных, общедоступных персональных данных, принятия решений, порождающих юридические последствия, на основании исключительно автоматизированной обработки ПДн;
- комиссия формирует акты определения необходимого уровня защищенности для каждой ИСПДн, в которых указывается перечень обрабатываемых ПДн (Приложение 2.).

6.1.9. В Учреждении должны быть разработаны Модели угроз для всех ИСПДн.

6.1.10. Модель угроз разрабатывается на основании требований п.7 «Требований к защите персональных данных при их обработке в информационных системах персональных

данных», утвержденных Постановлением Правительства Российской Федерации от 01.10.2012 г. №1119.

6.1.11. Модель угроз разрабатывается в соответствии с требованиями РД «Методика определения актуальных угроз персональных данных при их обработке в информационных системах персональных данных» (утвержден руководством ФСТЭК России 14 февраля 2008 года) и РД «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утвержден руководством ФСТЭК России 15 февраля 2008 года).

6.1.12. Выбор и реализация мер защиты информации в ИСПДн осуществляются на основе Модели угроз и в зависимости от требуемого уровня защищённости ИСПДн.

6.1.13. Выбранные и реализованные меры защиты ПДн в ИСПДн должны обеспечивать нейтрализацию предполагаемых угроз безопасности ПДн при их обработке в ИСПДн в составе создаваемой системы защиты ПДн.

6.1.14. Модель угроз и требуемый уровень защищённости информационной системы могут быть пересмотрены по решению комиссии на основе проведенного анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной информационной системы.

6.1.15. Для проведения работ по выбору и реализации мер защиты ПДн (включая техническое проектирование системы защиты ПДн, внедрение средств защиты ПДн, сопровождение средств защиты ПДн и т. д.) могут привлекаться подрядные организации, имеющие лицензию на осуществление деятельности по технической защите конфиденциальной информации.

6.1.16. Работы, проводимые третьими лицами (организациями) должны проводиться в присутствии работников Учреждения. При этом доступ к персональным данным, обрабатываемым в информационных системах персональных данных, для третьих лиц должен быть органичен.

6.1.17. Технические требования по защите ПДн в ИСПДн приведены в разделе 7.

6.2 Требования к разрабатываемым и вводимым в эксплуатацию ИСПДн

6.1.18. Разработка ИСПДн должна включать следующие стадии:

- предпроектная стадия (включает предварительный анализ целей и условий функционирования ИСПДн, а также обрабатываемых в ней ПДн, на основании которого определяется предварительный уровень защищённости ИСПДн, степень участия должностных лиц, актуализируются угрозы безопасности);
- стадия проектирования системы защиты ПДн для ИСПДн;
- стадия ввода в действие ИСПДн.

6.1.19. По результатам проведенного анализа и с учетом действующих требований федерального законодательства и регуляторов должны быть разработаны:

- модель угроз безопасности персональных данных при их обработке в ИСПДн;
- требования к защите персональных данных при их обработке в ИСПДн;
- акт определения необходимого уровня защищенности ИСПДн;
- частное техническое задание на создание системы защиты ПДн для ИСПДн.

6.1.20. Проектирование системы защиты ПДн для вводимой в эксплуатацию ИСПДн должно производиться с учетом уже построенной в Учреждении системы защиты ПДн, включающей комплекс организационных и технических мер.

6.1.21. На стадии ввода в эксплуатацию ИСПДн должны быть проведены, как минимум, следующие мероприятия:

- установка пакета прикладных программ ИСПДн совместно со средствами защиты информации (встроенными и наложенными);
- опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн;
- приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации.

6.1.22. В случае внедрения дополнительных средств защиты должны быть составлены Акты внедрения средств защиты информации по результатам их приемо-сдаточных испытаний.

6.1.23. Перед вводом новой ИСПДн в опытную эксплуатацию должен быть составлен Акт о вводе в опытную эксплуатацию ИСПДн, а также Акт определения необходимого уровня защищенности ИСПДн.

6.1.24. В случае успешного функционирования ИСПДн на стадии опытной эксплуатации и принятия решения о переводе ее в промышленную эксплуатацию должен быть составлен Акт о вводе в промышленную эксплуатацию новой ИСПДн.

6.3 Требования к выводу ИСПДн из эксплуатации

6.1.25. В случае принятия решения о выводе ИСПДн из промышленной эксплуатации должен быть подписан Акт о выводе ИСПДн из промышленной эксплуатации.

6.1.26. При выводе ИСПДн из промышленной эксплуатации с целью обеспечения справочной поддержки Администрации доступ к ней должен быть ограничен только определенным составом лиц с правами только на чтение.

6.1.27. После подписания Акта о выводе ИСПДн из промышленной эксплуатации ИСПДн должна быть переведена в архивный фонд Учреждения (в соответствии с ч. 2 ст. 13 ФЗ «Об архивном деле»), при этом должны быть выполнены следующие требования:

- Доступ к архивной ИСПДн и хранимым в ней документам должен обеспечиваться на основании соответствующей заявки на имя директора Учреждения, по согласованию с отделом информационных технологий и владельцем ИСПДн.
- ПДн, хранящиеся в архиве, могут быть использованы и переданы третьим лицам только в целях исполнения законодательства Российской Федерации.
- Должны быть обеспечены финансовые, материально-технические и иные условия, необходимые для комплектования, хранения, учета и использования ИСПДн, включая специальное помещение, отвечающее нормативным условиям труда сотрудников архива.
- Доступ в помещения, где предполагается хранение выводимой из эксплуатации ИСПДн, должен быть ограничен.
- Должен быть регламентирован перечень лиц, допущенных к работе с ИСПДн, переданной в архив.
- Все внешние запоминающие устройства (ленты с резервными копиями, дискеты, CD-диски, флеш-накопители и т. п.), относящиеся к архивной ИСПДн, должны храниться в сейфах.
- Должно быть разработано описание ИСПДн, переведенной в архивный фонд.

7 ОБЕСПЕЧЕНИЕ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ПДН

7.1 Общие требования

7.1.1. Обеспечение безопасности ПДн при их обработке в ИСПДн должно осуществляться на всех стадиях жизненного цикла ИСПДн и состоять из согласованных мероприятий, направленных на предотвращение (нейтрализацию) и устранение угроз безопасности ПДн в ИСПДн, минимизацию возможного ущерба, а также мероприятий по восстановлению данных и нормального функционирования ИСПДн в случае реализации угроз.

7.1.2. В целях защиты ПДн от несанкционированного доступа и иных неправомерных действий мероприятия по организации и техническому обеспечению безопасности ПДн для каждой ИСПДн должны включать:

- Определение требуемого уровня защищённости информационной системы производится в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными Постановлением Правительства Российской Федерации от 01.10.2012 г. №1119;
- выявление и закрытие технических каналов утечки ПДн на основе анализа и актуализации модели угроз безопасности ПДн;
- выбор и реализацию мер защиты информации в информационной системе на основе модели угроз безопасности ПДн и в зависимости от уровня защищённости информационной системы;
- установку, настройку и применение соответствующих программных, аппаратных и программно-аппаратных средств защиты информации;
- разработку дополнений к трудовым договорам (или должностных инструкций) по обеспечению безопасности ПДн при их обработке в ИСПДн для персонала, задействованного в эксплуатации данной ИСПДн.

7.1.3. Используемые средства вычислительной техники, удовлетворяют требованиям национальных стандартов по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным

нормам, предъявляемым к видеодисплейным терминалам средств вычислительной техники.

7.1.4. Защита ПДн при их обработке в ИСПДн от несанкционированного доступа и иных неправомерных действий должна осуществляться в Учреждении следующими мерами:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

7.1.5. В случае определения в соответствии с Требованиями к защите персональных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119, в качестве актуальных угроз безопасности персональных данных 1-го и 2-го типов

дополнительно к мерам по обеспечению безопасности персональных данных могут применяться следующие меры:

- проверка системного и (или) прикладного программного обеспечения, включая программный код, на отсутствие недекларированных возможностей с использованием автоматизированных средств и (или) без использования таковых;
- тестирование информационной системы на проникновения;
- использование в информационной системе системного и (или) прикладного программного обеспечения, разработанного с использованием методов защищенного программирования.

7.1.6. В Учреждении также могут разрабатываться и применяться другие меры защиты информации от несанкционированного доступа, обеспечивающие нейтрализацию угроз безопасности ПДн.

7.1.7. Конкретные методы и средства защиты ПДн в ИСПДн должны определяться на основании нормативно-методических документов ФСТЭК России и ФСБ России исходя из требуемого уровня защищённости и актуальных угроз безопасности ПДн.

7.1.8. Выполнение функций обеспечения безопасности персональных данных в ИСПДн обеспечивается средствами защиты информации, прошедшими в установленном порядке процедуру оценки соответствия, а также комплексом встроенных механизмов защиты электронных вычислительных машин, операционных систем, систем управления базами данных, прикладного программного обеспечения.

7.1.9. Все технические средства защиты информации должны быть снабжены инструкциями по эксплуатации (рекомендациями по использованию).

7.1.10. Должен вестись учет технических средств защиты информации.

7.1.11. Форма Журнала учета технических средств защиты информации приведена в Приложение 6..

7.1.12. Ответственность за ведение учета технических средств защиты информации возлагается на ответственного за организацию обработки ПДн.

7.2 Тестирование функций системы защиты ПДн

7.1.13. В соответствии с «Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» должно проводиться периодическое тестирование функций системы защиты ПДн.

7.1.14. Тестирование функций системы защиты производится на основании Положения (Плана) о порядке контроля защищенности персональных данных.

7.1.15. Ответственность за тестирование функций системы защиты ПДн возлагается на ответственного за организацию обработки ПДн.

7.3 Учет отчуждаемых электронных носителей ПДн

7.1.16. В Учреждении должен проводиться учет отчуждаемых защищаемых носителей ПДн. К защищаемым носителям ПДн относятся следующие:

- съемные носители информации серверов;
- съемные носители информации АРМ;
- ленты с резервными копиями;
- внешние запоминающие устройства (дискеты, флеш-накопители и т. п.), содержащие ПДн.

7.1.17. Форма учета отчуждаемых защищаемых электронных носителей приведена в Приложение 4..

7.1.18. Ответственность за учет отчуждаемых защищаемых электронных носителей ПДн возлагается на ответственного за организацию обработки ПДн.

8 ОБЯЗАННОСТИ АДМИНИСТРАТОРОВ ИСПДН, ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПДН, КООРДИНАТОРА ПО ОБРАЩЕНИЯМ И ЗАПРОСАМ

8.1 Ответственность за обеспечение безопасности персональных данных при их автоматизированной обработке, соблюдение установленных в Учреждении требований к защите персональных данных при их автоматизированной обработке, в том числе требований настоящего Положения, в структурных подразделениях Учреждения возлагается на их руководителей.

8.2 Каждый работник Учреждения, имеющий доступ к информационным системам персональных данных, необходимый ему для выполнения своих должностных обязанностей, несет персональную ответственность за свои действия.

8.3 Должностные инструкции администраторов ИСПДн, ответственного за организацию обработки ПДн и координатора по обращениям и запросам должны быть расширены с учетом специфики обработки и защиты ПДн. Работники, назначенные на данные роли, должны быть ознакомлены под подпись со своими должностными инструкциями.

8.4 В обязанности администраторов ИСПДн входит:

- управление учетными записями пользователей комплекса ИСПДн;
- поддержание штатной работы комплекса ИСПДн;
- предоставление и прекращение доступа пользователей к ПДн в ИСПДн в соответствии с утвержденным Перечнем должностей сотрудников, допущенных к работе с ПДн или с утвержденными заявками на доступ к ПДн;
- установка и конфигурирование аппаратного и программного обеспечения комплекса ИСПДн, не связанного с обеспечением безопасности ПДн в ИСПДн;
- уточнение ПДн в случаях, определенных настоящим Положением и Положением о порядке обработки обращений субъектов персональных данных;
- блокирование ПДн в случаях, определенных настоящим Положением и Положением о порядке обработки обращений субъектов персональных данных;
- уничтожение ПДн в случаях, определенных настоящим Положением и Положением о порядке обработки обращений субъектов персональных данных;

8.5 В обязанности ответственного за организацию обработки ПДн входит:

- осуществление внутреннего контроля за соблюдением Учреждения и ее работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доведение до сведения работников Учреждения положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- осуществлять контроль за приемом и обработкой обращений и запросов субъектов ПДн или их представителей;
- тестирование системы защиты ПДн;
- предоставление сведений о ПДн в рамках проведения учета защищаемых носителей и проведения инвентаризации;
- установка, конфигурирование и администрирование аппаратных и программных СЗИ комплекса ИСПДн;
- учет и хранение отчуждаемых носителей ПДн;
- учет технических средств защиты информации;
- периодические проверки журналов безопасности;
- анализ защищенности ИСПДн;
- организация процесса обучения работников по направлению обеспечения безопасности ПДн;
- мониторинг порядка обработки ПДн;
- участие в проведении внутреннего контроля и служебных расследований фактов нарушения установленного порядка обработки и обеспечения безопасности ПДн.

8.6 Ответственный за организацию обработки ПДн обладает следующими полномочиями:

- проводить плановые и внеплановые контрольные мероприятия в целях контроля, изучения и оценки фактического состояния защищенности ПДн;
- запрашивать необходимую информацию у очевидцев и подозреваемых лиц при проведении разбирательств по фактам нарушения установленного порядка обработки и обеспечения безопасности ПДн;

- запрашивать необходимую информацию у администраторов ИСПДн;
- давать администраторам ИСПДн распоряжения касательно блокирования, уточнения, уничтожения ПДн;
- оценивать правомерность полученных запросов уполномоченного органа по защите прав субъектов ПДн;
- созывать комиссию для решения вопросов по возражениям субъектов ПДн против принятия решений на основании исключительно автоматизированной обработки персональных данных.

8.7 В обязанности Координатора по обращениям и запросам входит:

- обработка обращений субъектов ПДн;
- ведение Журнала учета обращений субъектов ПДн;
- взаимодействие с уполномоченным органом по защите прав субъектов ПДн;
- обработка запросов уполномоченного органа по защите прав субъектов ПДн;
- ведение Журнала учета запросов уполномоченного органа по защите прав субъектов ПДн;
- ведение и хранение Журнала учета проверок уполномоченным органом по защите прав субъектов ПДн.

8.8 Координатор по обращениям и запросам обладает следующими полномочиями:

- запрашивать необходимую информацию у администраторов ИСПДн;
- давать администраторам ИСПДн распоряжения касательно блокирования, уточнения, уничтожения ПДн;
- оценивать правомерность полученных запросов уполномоченного органа по защите прав субъектов ПДн;
- созывать комиссию для решения вопросов по возражениям субъектов ПДн против принятия решений на основании исключительно автоматизированной обработки персональных данных.

8.9 В целях обеспечения распределения полномочий, реализации взаимного контроля и недопущения сосредоточения критичных для безопасности ПДн полномочий у одного лица запрещается совмещать роли администратора ИСПДн и роль ответственного за организацию обработки ПДн в лице одного сотрудника.

9 ГОСУДАРСТВЕННЫЙ КОНТРОЛЬ И НАДЗОР ЗА ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1 Государственный контроль и надзор за соблюдением требований законодательства Российской Федерации в области персональных данных осуществляет федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности (ФСБ России), а также федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации (ФСТЭК России).

9.2 Государственный контроль и надзор за соблюдением требований законодательства Российской Федерации в области персональных данных осуществляется в соответствии с требованиями Федерального закона от 26.12.2008 г. № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля».

9.3 Организацию работ по прохождению государственного контроля и надзора осуществляет Ответственный за организацию обработки ПДн.

10 ОРГАНИЗАЦИЯ ВНУТРЕННЕГО КОНТРОЛЯ ОБРАБОТКИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1 Цели организации внутреннего контроля

10.1.1. Организация внутреннего контроля процесса обработки ПДн в Учреждении осуществляется в целях изучения и оценки фактического состояния защищенности ПДн, своевременного реагирования на нарушения установленного порядка их обработки, а также в целях совершенствования этого порядка и обеспечения его соблюдения.

10.1.2. Мероприятия по осуществлению внутреннего контроля обработки и обеспечения безопасности ПДн направлены на решение следующих задач:

- обеспечение соблюдения сотрудниками Учреждения требований настоящего Положения и нормативных правовых актов, регулирующих защиту персональных данных;
- оценка компетентности персонала, задействованного в обработке ПДн;
- обеспечение работоспособности и эффективности технических средств ИСПДн и средств защиты ПДн, их соответствия требованиям уполномоченных органов исполнительной власти по вопросам безопасности ПДн;
- выявление нарушений установленного порядка обработки ПДн и своевременное предотвращение негативных последствий таких нарушений;
- принятие корректирующих мер, направленных на устранение выявленных нарушений, как в порядке обработки ПДн, так и в работе технических средств ИСПДн;
- разработка рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ПДн по результатам контрольных мероприятий;
- осуществление контроля за исполнением рекомендаций и указаний по устранению нарушений.

10.2 Проведение контрольных мероприятий

10.2.1. Ответственный за организацию обработки ПДн на периодической основе организует проведение внутреннего контроля соблюдения порядка обработки и обеспечения безопасности ПДн.

10.2.2. Проведение контрольных мероприятий по обеспечению безопасности ПДн должно включать:

- проведение проверок деятельности работников Учреждения, допущенных к работе с ПДн в ИСПДн, на соответствие порядку обработки и обеспечения безопасности ПДн, установленному настоящим Положением, ФЗ «О персональных данных» и другими нормативными правовыми актами;
- проведение проверок состояния защищенности ПДн, обрабатываемых в ИСПДн, включая проверку доступов пользователей к ПДн, выполнение требований по защите каждой конкретной ИСПДн, корректности работы системы защиты ПДн и т. д.

10.2.3. Все результаты проверок должны быть предоставлены в виде Актов для проведения анализов результатов и подготовки соответствующего Отчета о проведении внутреннего контроля обработки и обеспечения безопасности персональных данных.

10.2.4. При необходимости должны быть предложены меры по минимизации последствий выявленных угроз ИБ.

ЛИСТ ОЗНАКОМЛЕНИЯ

с «Положением об обеспечении безопасности персональных данных при их обработке»

Ознакомлены:

№ п/п	Фамилия и инициалы	Должность	Подразделение	Ознакомлен(а)		С изменениями №__ Ознакомлен(а)		С изменениями №__ Ознакомлен(а)	
				Дата	Подпись	Дата	Подпись	Дата	Подпись

Приложение 1. **Перечень информационных систем персональных данных**

(типовая форма)

ПЕРЕЧЕНЬ

ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

№ п/п	Наименование информационной системы	Пользователи информационной системы
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		

Приложение 2. Акт определения необходимого уровня защищенности информационной системы персональных данных (типовая форма)

АКТ

ОПРЕДЕЛЕНИЯ УРОВНЯ ЗАЩИЩЁННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫПЕРСОНАЛЬНЫХ ДАННЫХ

_____

(наименование информационной системы)

В соответствии с постановлением Правительства Российской Федерации от 01.11.2012 № 1119 , комиссия в составе:

Председатель Комиссии:

– *Фамилия Имя Отчество, должность;*

Члены Комиссии:

– *Фамилия Имя Отчество, должность;*

– *Фамилия Имя Отчество, должность,*

рассмотрев «Модель угроз безопасности персональных данных …», а также учитывая следующие исходные данные на информационную систему персональных данных:

1) в ИСПДн (не) обрабатываются специальные категории персональных данных, биометрические персональные данные, общедоступные персональные данные. (В ИСПДн обрабатываются иные категории персональных данных).

2) Объем обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе):_____.

3) для ИСПДн актуальны угрозы N-го типа.

4) Наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена:_____.

5) Режим обработки персональных данных:_____.

6) Режим разграничения прав доступа пользователей:_____.

7) Местонахождение технических средств информационной системы:_____.

РЕШИЛА: *Решение комиссии об определении необходимого уровня защищенности информационной системы*

Председатель комиссии: _____ _____

личная подпись *инициалы, фамилия*

Члены комиссии: _____ _____

личная подпись *инициалы, фамилия*

Приложение 3. Список работников, допущенных к обработке персональных данных (типовая форма)

СПИСОК

РАБОТНИКОВ, ДОПУЩЕННЫХ К ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

№ п/п	Ф.И.О.	Структурное подразделение	Должность	Наименование информационных систем, к которым предоставлен доступ
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				

Приложение 4. Журнал учета машинных носителей персональных данных (типовая форма)

ЖУРНАЛ
УЧЕТА МАШИННЫХ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

Журнал начат «____» _____ 20__ г.

Должность

_____ / Ф.И.О. должностного лица /

Журнал завершен «____» _____ 20__ г.

Должность

_____ / Ф.И.О. должностного лица /

На _____ листах

№ п/п	Регистрационный номер носителя	Дата регистрации носителя	Тип / емкость носителя	Серийный номер носителя	Отметка о постановке на учет (Ф.И.О., подпись, дата)	Отметка о снятии с учета (Ф.И.О., подпись, дата)	Местонахождение носителя	Сведения об уничтожении носителя
1.								
2.								
3.								
4.								
5.								
6.								
7.								
8.								
9.								
10.								

Приложение 5. Акт на списание и (или) уничтожение машинных носителей персональных данных (типовая форма)

АКТ

НА СПИСАНИЕ / УНИЧТОЖЕНИЕ МАШИННЫХ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

Комиссия в составе:

Председатель Комиссии:

– *Фамилия Имя Отчество, должность;*

Члены Комиссии:

– *Фамилия Имя Отчество, должность;*

– *Фамилия Имя Отчество, должность,*

провела отбор машинных носителей персональных данных и установила, что в соответствии с требованиями документов:

_____

_____

_____

Персональные данные, записанные на них в процессе эксплуатации, подлежит уничтожению:

№ п/п	Регистрационный номер носителя	Дата регистрации носителя	Тип / емкость носителя	Серийный номер носителя	Примечание
1.					
2.					
3.					
4.					

Всего подлежит уничтожению _____ носителей

(цифрами и прописью)

Машинные носители персональных данных уничтожены путем:

_____

_____

_____

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

Уничтоженные носители с «Журнала учета машинных носителей персональных данных» списаны.

Председатель комиссии: _____ _____

личная подпись *инициалы, фамилия*

Члены комиссии: _____ _____

личная подпись *инициалы, фамилия*

_____ _____

личная подпись *инициалы, фамилия*

Приложение 6. Журнал учета средств защиты информации, эксплуатационной и технической документации (типовая форма)

ЖУРНАЛ
УЧЕТА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ, ЭКСПЛУАТАЦИОННОЙ И ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ

Журнал начат «____» _____ 20__ г.

Должность

_____ / Ф.И.О. должностного лица /

Журнал завершен «____» _____ 20__ г.

Должность

_____ / Ф.И.О. должностного лица /

На _____ листах

№ п/п	Наименование СЗИ	Серийный номер СЗИ	Наименование и номер документации к СЗИ	Отметка о вводе в эксплуатацию СЗИ			Отметка об изъятии СЗИ из аппаратных средств			Примечание
				Ф.И.О. пользователя СЗИ, производившего подключение (установку)	Дата ввода в эксплуатацию и подписи лиц, производивших ввод в эксплуатацию	Номера аппаратных средств на которые установлены СЗИ	Дата снятия с эксплуатации	Ф.И.О. пользователя СЗИ, производившего снятие с эксплуатации СЗИ	Номер акта о снятии с эксплуатации СЗИ	
1.										
2.										
3.										
4.										
5.										
6.										
7.										
8.										

Приложение 7. Заключение о возможности эксплуатации средств зашиты информации (типовая форма)

ЗАКЛЮЧЕНИЕ

О ВОЗМОЖНОСТИ ЭКСПЛУАТАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

_____

(наименование средства зашиты информации)

_____

_____

(наименования информационных систем персональных данных, в которых применяется средство защиты)

Комиссия в составе:

Председатель Комиссии:

– *Фамилия Имя Отчество, должность;*

Члены Комиссии:

– *Фамилия Имя Отчество, должность;*

– *Фамилия Имя Отчество, должность,*

УСТАНОВИЛА:

_____

_____

(назначение средства защиты информации)

_____

_____

(сведения о технической и эксплуатационной документации на средство защиты информации)

_____

_____

(сведения о сертификации средства защиты информации)

_____

_____

(сведения об обучении работников правилам работы со средством защиты информации)

ВЫВОДЫ О ВОЗМОЖНОСТИ ЭКСПЛУАТАЦИИ:

_____

_____

_____

Председатель комиссии: _____ _____

личная подпись *инициалы, фамилия*

Члены комиссии: _____ _____

личная подпись *инициалы, фамилия*

_____ _____

личная подпись *инициалы, фамилия*

Приложение 8. **Инструкция по обращению с сертифицированными ФСБ шифровальными средствами (средствами криптографической защиты информации)**

ИНСТРУКЦИЯ

ПО ОБРАЩЕНИЮ С СЕРТИФИЦИРОВАННЫМИ ФСБ ШИФРОВАЛЬНЫМИ СРЕДСТВАМИ (СРЕДСТВАМИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ)

1. В составе средств защиты информации системы защиты персональных данных применяются средства криптографической защиты информации (далее по тексту – СКЗИ).

2. Работы по обеспечению безопасности информации при помощи СКЗИ должны проводиться в соответствии с действующими в настоящее время нормативными документами, регламентирующими вопросы эксплуатации СКЗИ, технической документацией на СКЗИ и лицензионными требованиями ФСБ России.

3. Процесс установки и ввод в эксплуатацию средств криптографической защиты информации должен осуществляться в соответствии с эксплуатационной и технической документацией к ним.

4. При применении СКЗИ должна поддерживаться непрерывность процессов протоколирования работы СКЗИ и обеспечения целостности программного обеспечения для среды функционирования СКЗИ.

5. Проверка готовности СКЗИ к эксплуатации должна осуществляться экспертной группой из числа сотрудников Компании с составлением и подписанием заключения о возможности эксплуатации средств криптографической защиты информации.

6. Эксплуатация средства криптографической защиты информации должна быть организована в соответствии с правилами пользования ими. Все изменения условий использования СКЗИ, указанных в правилах пользования ими, должны согласовываться с ФСБ России и специализированной организацией, проводившей тематические исследования СКЗИ.

6.1. При эксплуатации СКЗИ должны выполняться следующие требования по криптографической защите:

- использовать только лицензионное системное программное обеспечения;
- при инсталляции СКЗИ обеспечить организационно-технические меры по исключению подмены дистрибутива и внесения изменений в СКЗИ после установки;
- исключить средства отладки из программного обеспечения ПЭВМ с установленным СКЗИ;
- использовать СКЗИ на рабочих станциях и серверах с установленными лицензионными средствами антивирусной защиты;
- для аутентификации пользователей использовать пароль, содержащий не менее 6 символов алфавита мощности не менее 10;
- смену паролей проводить не реже одного раза в течение 6 месяцев.

6.2. Для исключения возможности вскрытия и подключения к СКЗИ в нештатном режиме и/или внесения в него несанкционированных изменений должно применяться:

- ограничение доступа к настройкам BIOS паролем администратора;
- запрещение в настройках BIOS загрузки с устройств, отличных от штатного накопителя;
- физическое отключение после установки и настройки комплекса устройств ввода/вывода (клавиатура, мышь, монитор, принтер и т.д.);
- ограничение доступа к консоли операционной системы с помощью пароля административной учетной записи;
- ограничение доступа к web-интерфейсу администрирования паролем администратора;
- ограничение доступа к средствам централизованного управления паролем администратора;
- все пароли администраторов должны быть различны;
- отсутствие возможности доступа к консоли операционной системы пользователей кроме администратора;
- обеспечение использования для доступа к консоли операционной системы и web - администрирования только с заданного сетевого порта;
- опечатывание корпуса устройства (например, голографическими метками);
- опечатывание имеющихся разъемов RS232/PS/2/LPT (например, голографическими метками);
- опечатывание разъемов USB (например, голографическими метками);
- опечатывание дисководов и приводов чтения оптических носителей, неиспользуемых внутренних отсеков корпуса (например, голографическими метками);
- опечатывание неиспользуемых сетевых портов (например, голографическими метками);
- опечатывание подключенных коммуникационных кабелей (например, голографическими метками).

7. Эксплуатация СКЗИ должна производиться сотрудниками, назначенными приказом руководителя.

7.1. Сотрудники, ответственные за эксплуатацию СКЗИ должны проходить обучение (на специализированных курсах) по порядку работы с ними.

7.2. Сотрудники, ответственные за эксплуатацию СКЗИ должны осуществлять:

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

- учет пользователей СКЗИ и закрепленных за ними криптографических ключей;
- контроль за соблюдением условий функционирования СКЗИ;
- принятие мер по предотвращению возможных негативных последствий нарушения нормального функционирования СКЗИ.

7.3. Пользователи, допущенные к работе с СКЗИ, обязаны:

- не разглашать информацию, к которой они допущены, сведений об используемых криптосредствах, ключевых документах к ним и применяемых защитных мерах;
- соблюдать требования по обеспечению безопасности криптосредств и ключевых документов к ним;
- докладывать Ответственному за эксплуатацию СКЗИ о ставших им известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним;
- немедленно уведомлять Ответственного за эксплуатацию СКЗИ о фактах утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей, о других фактах, которые могут привести к несанкционированному доступу к компонентам СКЗИ;
- сдать криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств.

7.4. Пользователям СКЗИ запрещается:

- осуществлять копирование криптографических ключей;
- использовать ключевые носители вне информационной системы;
- записывать на ключевые носители постороннюю информацию;
- вносить какие-либо изменения в программное обеспечение СКЗИ;
- оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ, после ввода ключевой информации либо иной конфиденциальной информации;
- осуществлять администрирование (конфигурирование) СКЗИ с рабочих мест, не проверенных на наличие вредоносного программного (руткиты, вирусы, кейлоггеры и т.д.) или аппаратного обеспечения;
- вносить какие-либо изменения в программное обеспечение СКЗИ;

- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и иные подобные средства отображения информации;
- использовать ключевые носители в режимах, не предусмотренных функционированием СКЗИ.

8. СКЗИ подлежат поэкземплярному учету в «Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов» (Приложение 9.) с использованием индексов или условных наименований и регистрационных номеров. Перечень индексов (условных наименований) и регистрационных номеров поэкземплярного учета СКЗИ определяет ФСБ России.

8.1. Поэкземплярный учет производится Ответственным за эксплуатацию средств криптографической защиты информации.

8.2. Экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевые документы должны выдаваться под расписку в Журнале поэкземплярного учета.

9. Ответственный за эксплуатацию должен вести на каждого пользователя СКЗИ Лицевой счет (Приложение 10.), в котором регистрируются СКЗИ закрепленные за пользователем, эксплуатационная и техническая документация к ним, ключевые документы.

10. Средства криптографической защиты информации, эксплуатационная и техническая документация к ним, ключевые носители и документы должны размещаться, и храниться в специальных (режимных) помещениях, исключающих несанкционированный доступ к ним. Все режимные помещения подлежат учету в «Журнале учета хранилищ (сейфов)» (Приложение 12.).

10.1. Режимные 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, оборудуются металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими несанкционированному проникновению в режимные помещения.

10.2. Порядок охраны режимных помещений, правила допуска сотрудников, должны устанавливаться Ответственным за эксплуатацию СКЗИ и утверждается руководителем. Порядок охраны должен предусматривать периодический контроль за состоянием технических средств охраны (исправностью сигнализации). Исправность сигнализации периодически проверяется Ответственным за эксплуатацию СКЗИ. Результаты проверок должны регистрироваться в «Журнале проверок исправности сигнализации» (Приложение 13.).

10.3. Ключи от входных дверей режимных помещений должны быть пронумерованы, учтены в «Журнале учета ключей от хранилищ» (Приложение 14.) и выдаваться сотрудникам, имеющим право допуска в режимные помещения, под роспись в этом Журнале. Дубликаты ключей от входных дверей таких помещений должны храниться в опечатанном пенале (конверте) в сейфе у руководителя.

10.4. По окончании рабочего дня режимные помещения должны закрываться, и опечатываются пользователями СКЗИ. Ключи от этих помещений должны сдаваться Ответственному за эксплуатацию под роспись в Журнале учета хранилищ (сейфов)» (Приложение 12.).

10.5. Аппаратные средства, с установленными СКЗИ, должны быть оборудованы средствами контроля за их вскрытием (опечатаны). Вскрытие аппаратных средств СКЗИ должно осуществляться в присутствии Ответственного за эксплуатацию СКЗИ.

11. Для предотвращения просмотра извне режимных помещений на окнах должны быть установлены жалюзи.

12. Ключевые документы, носители с СКЗИ, эталонные CD диски с ПО СКЗИ, носители с конфиденциальной информацией, касающейся СКЗИ, эксплуатационная и техническая документация на СКЗИ, хранятся в сейфе Ответственного за эксплуатацию СКЗИ. Ключи от сейфа должны быть пронумерованы, учтены в «Журнале учета ключей от хранилищ» (рекомендованная форма приведена в Приложение 14.) и выдаваться сотрудникам, имеющим право использования содержимого сейфа, под роспись в этом Журнале. Дубликаты ключей от сейфа должны храниться в опечатанном пенале (конверте) в сейфе у руководителя.

12.1. Все действия с криптографическими ключами регистрируются в «Техническом (аппаратном) журнале» (Приложение 11.).

12.2. Неиспользуемые СКЗИ, ключевые документы подлежат сдаче Ответственного за эксплуатацию СКЗИ.

12.3. Выведенные из действия криптоключи подлежат уничтожению. Применяемые способы уничтожения исключают возможность повторного использования или восстановления криптоключей.

12.4. Уничтожение магнитных и оптических носителей информации производится путем:

- физического уничтожения ключевого носителя, т.е. нанесения неустранимого физического повреждения;
- программного уничтожения без уничтожения носителя (стирания) по технологии, принятой для соответствующих носителей информации, что обеспечивает его многократное использования.

12.5. Уничтожение бумажных и прочих сгораемые носители информации, а также эксплуатационная и техническая документация к СКЗИ производится путем:

- сжигания;
- измельчения в бумагорезательных машинах (шрёдерах).

12.6. Факт уничтожения ключевых данных, документов и носителей регистрируется в Акте уничтожения (рекомендованная форма приведена в Приложение 15.).

13. В случае выявления недостачи СКЗИ, ключевых документов, ключевых носителей, эксплуатационной и технической документации; обнаружении признаков, указывающих на возможное несанкционированное проникновение в режимные помещения немедленно докладывается Ответственному за эксплуатацию СКЗИ.

14. При возникновении пожара, аварии или стихийного бедствия, в соответствии с порядком, утвержденным руководителем производится эвакуация документов, СКЗИ, криптоключей.

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

- Ответственным за эксплуатацию СКЗИ;
- Владельцем информационной системы, в составе которой применяется СКЗИ;
- Ответственным за организацию обработки персональных данных в рамках контрольных мероприятий;
- ФСБ России в рамках контроля за организацией и функционированием криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, систем шифрованной, засекреченной и иных видов специальной связи.

16. Контроль за соблюдением условий производства ключевых документов, указанных в технической, и эксплуатационной документации к системе изготовления ключей, осуществляется изготовителем ключевых документов, а также ФСБ России в рамках в рамках контрольных мероприятий.

17. С целью оценки обоснованности и достаточности мер, принятых для защиты персональных данных, Ответственный за организацию обработки ПДн, владелец информационной системы, в составе которой применяются СКЗИ, вправе обратиться в ФСБ России с просьбой о проведении контроля за соблюдением правил пользования СКЗИ и условий их использования, указанных в правилах пользования СКЗИ.

18. СКЗИ подвергаются контрольным тематическим исследованиям, конкретные сроки проведения которых, определяются заказчиком СКЗИ по согласованию с разработчиком СКЗИ, специализированной организацией и ФСБ России.

Приложение 9. **Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации, ключевых документов (типовая форма)**

ЖУРНАЛ

ПОЭКЗЕМПЛЯРНОГО УЧЕТА СКЗИ, ЭКСПЛУАТАЦИОННОЙ И ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ К НИМ,

КЛЮЧЕВЫХ ДОКУМЕНТОВ

Журнал начат «____» _____ 20__ г.

Должность

_____ / Ф.И.О. должностного лица /

Журнал завершен «____» _____ 20__ г.

Должность

_____ / Ф.И.О. должностного лица /

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и расписка в получении	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, произведших подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	

На _____ листах

Приложение 10. Лицевой счет пользователя средств криптографической защиты информации (типовая форма)

ЛИЦЕВОЙ СЧЕТ

ПОЛЬЗОВАТЕЛЯ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

_____

(Ф.И.О., должность, наименование структурного подразделения)

№ п/п	Дата получения криптографических ключей	Номера криптографических ключей	Наименование СКЗИ и статус криптографического ключа	Количество ключевых носителей	Инвентарные номера АРМ на которых используются криптографические ключи	Возвращено	
						Дата	Подпись
1	2	3	4	5	6	7	8

Приложение 11. Технический (аппаратный) журнал (типовая форма)

ТЕХНИЧЕСКИЙ (АППАРАТНЫЙ) ЖУРНАЛ

Журнал начат «____» _____ 20__ г.

Должность

_____ / Ф.И.О. должностного лица /

Журнал завершен «____» _____ 20__ г.

Должность

_____ / Ф.И.О. должностного лица /

На _____ листах

№ 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 12. Журнал учета хранилищ (типовая форма)

ЖУРНАЛ
УЧЕТА ХРАНИЛИЩ (СЕЙФОВ)

Журнал начат «____» _____ 20__ г.

Должность

_____ / Ф.И.О. должностного лица /

Журнал завершен «____» _____ 20__ г.

Должность

_____ / Ф.И.О. должностного лица /

На _____ листах

Учетный номер	Наименование хранилищ (сейф, металлический шкаф)	Инвентарный номер	Местонахождение (подразделение, номер комнаты)	Что находится (документы, изделия)	Фамилия ответственного за сейф (шкаф)	Кол-во комплектов ключей и их номера	Расписка ответственного за хранилище в получении ключа и дата	Расписка в приеме ключа и дата
1	2	3	4	5	6	7	8	9

Приложение 13. Журнал проверок исправности сигнализации (типовая форма)

ЖУРНАЛ

ПРОВЕРОК ИСПРАВНОСТИ СИГНАЛИЗАЦИИ

Журнал начат «____» _____ 20__ г.

Должность

_____ / Ф.И.О. должностного лица /

Журнал завершен «____» _____ 20__ г.

Должность

_____ / Ф.И.О. должностного лица /

На _____ листах

№ п/п	Ф.И.О. сотрудника ответственного за исправную работу сигнализации	Дата проверки	Состояние сигнализации, выявленные неисправности	Рекомендации к принятию мер для устранения неисправностей (в случае необходимости)	Подпись ответственного	Примечание
1	2	3	4	5	6	7

Приложение 14. Журнал учета ключей от хранилищ (типовая форма)

ЖУРНАЛ
УЧЕТА КЛЮЧЕЙ ОТ ХРАНИЛИЩ (СЕЙФОВ)

Журнал начат «____» _____ 20__ г.

Должность

_____ / Ф.И.О. должностного лица /

Журнал завершен «____» _____ 20__ г.

Должность

_____ / Ф.И.О. должностного лица /

На _____ листах

№ п/п	Адрес и наименование (номер) хранилища	Номер выданного ключа от хранилища	Ф.И.О. сотрудника, получившего ключ от хранилища	Выдача ключей			Сдача ключей	
				Дата выдачи ключа от хранилища	Подпись сотрудника, получившего ключ от хранилища	Подпись сотрудника, ответственного за хранилище	Дата сдачи ключа от хранилища	Подпись сотрудника, ответственного за хранилище
1	2	3	4	5	6	7	8	9

Приложение 15. Акт уничтожения криптографических ключей

АКТ

уничтожения криптографических ключей, ключевых носителей, эксплуатационной и технической документации

Комиссия, назначенная приказом директора Учреждения от «___»_____ 201__г. № ___ в составе:

председателя – _____.

и членов комиссии:

– _____;

произвела отбор криптографических ключей, ключевых носителей, документов утративших свою актуальность и подлежащих уничтожению:

№ п/п	Учетный номер ключевого носителя (документа)	Номер (идентификатор) криптографического ключа, наименование документа	Владелец ключа (документа)	Количество ключевых носителей (документов)	Номера экземпляров	Всего уничтожается ключей (документов)	При-мечание
1.							

Всего уничтожено _____ единиц учета

(цифрами и прописью)

Записи настоящего Акта сверены с записями документа «Журнал поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов».

Уничтожение криптографических ключей выполнено по технологии, регламентированной в эксплуатационной и технической документации на СКЗИ:

_____

_____

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

Акт составлен в соответствии с требованиями 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 обработке в информационных системах персональных данных». Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. №149/6/6-622.

Председатель комиссии: _____

Члены комиссии: _____