Утверждаю
Главный врач
ГБУЗ «Ленинская «ЦРБ»
_____ Е.А. Крайнов
15.11.2013

Приложение №1
к приказу от 15.11.2013 №515-О

Положение об обработке и обеспечению защиты персональных данных в ГБУЗ «Ленинская ЦРБ»

1. Общие положения

1.1. Настоящее Положение «Об обработке и обеспечению защиты персональных данных» (далее по тексту «Положение») ГБУЗ «Ленинская ЦРБ» (далее по тексту «Учреждение») разработано в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных в информационных системах персональных данных (далее по тексту «ИСПДн»).

1.2. Целью Положения является формирование общих правил для обеспечения защиты Учреждением персональных данных (далее по тексту «ПДн») от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (далее по тексту «УБПДн»).

1.3. Положение разработано в соответствии с Конституцией РФ, Трудовым кодексом РФ, Федеральным законом Российской Федерации от 27 июля 2006 г. N 152-ФЗ «О персональных данных», Федеральным законом Российской Федерации от 25 июля 2011 г. N 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных», Постановлением Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012 г. № 1119, Постановлением Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и иными нормативными актами, действующими на территории Российской Федерации.

1.4. В Положении используются следующие термины:

– **Безопасность персональных данных** – состояние защищенности ПДн, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность ПДн при их обработке в ИСПДн.

– **Блокирование персональных данных** – временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

– **Информационная система персональных данных** – совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.

– **Контролируемая зона** – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

– **Конфиденциальность персональных данных** – обязательное для соблюдения оператором (в данном случае Учреждением) или иным лицом, получившим доступ к персональным данным, требование не допускать их распространения без согласия субъекта ПДн или наличия иного законного основания.

– **Неавтоматизированная обработка персональных данных** – обработка ПДн субъекта без использования средств вычислительной техники.

– **Обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

– **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 ПДн.

– **Оператор (персональных данных)** – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с персональными данными.

– **Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн).

– **Предоставление персональных данных** – действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.

– **Распространение персональных данных** – действия, направленные на раскрытие ПДн неопределенному кругу лиц.

– **Технические средства информационной системы персональных данных** – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

– **Трансграничная передача персональных данных** – передача ПДн на территорию иностранного государства, органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

– **Уничтожение персональных данных** – действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и (или) в результате которых уничтожаются материальные носители ПДн.

2. Область действия

2.1. Положение является обязательным для исполнения всеми работниками Учреждения, имеющими доступ к персональным данным.

3. Рекомендации по защите

3.1. Рекомендации содержат описание системы мер и принципов организации защиты ПДн в Обществе.

3.2. Рекомендуется устанавливать в технических заданиях на создание (модернизацию) конкретных ИСПДн и элементов информационно-телекоммуникационной инфраструктуры такой уровень требований по защите информации, который бы соответствовал или был строже рекомендаций, предложенных в настоящем разделе.

3.3. Работы по защите информации проводятся на основе реализации комплекса организационных и технических мероприятий.

3.4. Не допускается осуществление работниками Учреждения любых мероприятий и работ с использованием ПДн без принятия необходимых мер по защите информации.

3.5. Организация работ по обработке и защите информации в Обществе возлагается на работника, ответственного за организацию обработки и обеспечение безопасности ПДн, назначенного приказом Руководителя Учреждения, или на стороннюю организацию (далее – «Уполномоченное лицо») по договору.

3.6. Методическое руководство, координация работ в области защиты информации и контроль эффективности мер защиты информации возлагаются на работника Учреждения, ответственного за организацию обработки и обеспечение безопасности ПДн.

3.7. Техническая защита конфиденциальной информации является лицензируемым видом деятельности и должна осуществляться на основе лицензий, выданных уполномоченными федеральными органами исполнительной власти. Для обеспечения технической защиты ПДн должны привлекаться организации, имеющие лицензии на указанный вид деятельности.

4. Обработка персональных данных субъектов персональных данных
Порядок получения персональных данных

4.1. Все ПДн субъекта ПДн следует получать работникам Учреждения, допущенным к обработке ПДн, у него самого. Если ПДн субъекта возможно получить только у третьей стороны, за исключением случаев, предусмотренных законодательством Российской Федерации, субъект должен быть уведомлен об этом заранее в письменном виде по почте работником, ответственным за организацию обработки и обеспечение безопасности ПДн, или другим сотрудником Учреждения по его поручению. Работник Учреждения, принимающий ПДн субъекта, должен сообщить субъекту ПДн следующую информацию:

- наименование, либо фамилия, имя, отчество и адрес Учреждения или его представителя;
- цель обработки ПДн и ее правовое основание;
- предполагаемые пользователи ПДн;
- установленные действующим законодательством РФ права субъекта ПДн.

4.2. Работники Учреждения не имеют права получать и обрабатывать ПДн субъектов, не соответствующие целям их обработки.

4.3. Обработка специальных категорий ПДн субъектов, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, возможна только с их согласия либо без их согласия в случаях, установленных законодательством РФ.

4.4. Субъект ПДн принимает решение о предоставлении его ПДн и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку ПДн должно быть конкретным, информированным и сознательным. Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем в письменной форме, если иное не установлено Федеральным законом. В случае получения согласия на обработку ПДн от представителя субъекта ПДн, полномочия данного представителя на дачу согласия от имени субъекта ПДн проверяются работником, ответственным за организацию обработки и обеспечение безопасности ПДн, на основе нотариально заверенных доверенностей либо других документов, подтверждающих полномочия представителей, копии которых должны быть приложены к согласию.

4.5. Передавать ПДн субъектов для обработки третьим лицам можно только после получения Учреждением от субъекта ПДн письменного согласия на передачу конкретному лицу (организации), кроме случаев, установленных действующим законодательством РФ. Передача ПДн на материальном носителе информации фиксируется в соответствующих журналах сотрудниками, ответственными за документооборот в Обществе. Передача ПДн в электронном виде по защищенным каналам связи фиксируется в электронных журналах средств защиты информации.

4.6. Письменное согласие субъекта ПДн на обработку его ПДн должно включать в себя:

- фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- фамилию, имя, отчество, адрес представителя субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты и приложенная нотариальная копия (или оригинал) доверенности или иного надлежащего документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта ПДн);
- наименование и адрес Учреждения, получающего согласие субъекта ПДн;
- цель обработки ПДн;
- перечень ПДн, на обработку которых дается согласие субъекта ПДн;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Учреждения, если обработка будет поручена такому лицу;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Учреждением способов обработки ПДн;
- срок, в течение которого действует согласие субъекта ПДн, а также способ его отзыва, если иное не установлено действующим законодательством РФ;
- подпись субъекта ПДн.

4.7. Согласие на обработку ПДн может быть отозвано субъектом ПДн. В случае отзыва субъектом ПДн согласия на обработку ПДн или в случае достижения целей обработки ПДн, Работник, ответственный за организацию обработки и обеспечение безопасности ПДн, инициирует сбор, блокировку обработки с последующим уничтожением ПДн субъекта, кроме случаев, установленных законодательством РФ.
4.8. Письменные согласия субъектов передаются Работнику, ответственному за организацию обработки и обеспечение безопасности ПДн, и хранятся в специально предназначенном месте.
4.9. При обработке ПДн субъекта, по его запросу могут быть предоставлены следующие данные:

- подтверждение факта обработки ПДн в Обществе;
- правовые основания и цели обработки ПДн;
- цели и применяемые в Обществе способы обработки ПДн;
- наименование и место нахождения Учреждения, сведения о лицах (за исключением работников Учреждения), которые имеют доступ к персональным данным или которым могут быть раскрыты ПДн на основании договора с Учреждением или на основании Федерального закона;
- обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом;
- сроки обработки ПДн, в том числе сроки их хранения;
- порядок осуществления субъектом ПДн прав, предусмотренных настоящим Федеральным законом;
- наименование или фамилия, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Учреждения, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими Федеральными законами.

4.10. В случае получения запросов от уполномоченного органа по защите прав субъектов ПДн работник, ответственный за организацию обработки и обеспечение безопасности ПДн, обязан представить документы и локальные акты, по обеспечению безопасности обработки ПДн субъектов и (или) иным образом подтвердить принятие необходимых мер в течение тридцати дней с даты получения такого запроса.

Порядок обработки, передачи и хранения персональных данных

4.11. В соответствии с законодательством РФ в целях обеспечения прав и свобод человека и гражданина Учреждение и его представители при обработке ПДн субъекта должны соблюдать следующие общие требования:

- обработка ПДн может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов РФ;
- при определении объема и содержания, обрабатываемых ПДн Учреждение должно руководствоваться действующим законодательством РФ и локальными нормативными актами Учреждения;
- при принятии решений, затрагивающих интересы субъекта, Учреждение не имеет права основываться на ПДн субъекта, полученных исключительно в результате их автоматизированной обработки или электронного получения;
- защита ПДн субъекта от неправомерного их использования или утраты обеспечивается Учреждением в порядке, установленном действующим законодательством РФ;
- работники Учреждения должны быть ознакомлены под роспись с документами Учреждения, устанавливающими порядок обработки ПДн, а также об их правах и обязанностях в этой области;
- доступ Работников Учреждения к персональным данным субъектов ПДн в ИСПДн регламентируется только на основании локальных нормативных актов Учреждения с

указанием перечня допущенных лиц, прав доступа, необходимых для выполнения служебных обязанностей;

– обработка ПДн, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (материальных носителей) и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ;

– уничтожение или обезличивание части ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление);

– уточнение ПДн при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными;

– при хранении материальных носителей ПДн должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный доступ к ним.

4.12. При передаче ПДн субъекта Работниками должны соблюдаться следующие требования:

– не сообщать персональные данные субъекта третьей стороне без его письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных Федеральным законом;

– осуществлять передачу ПДн субъектов в пределах Учреждения в соответствии с нормативными документами внутреннего документооборота Учреждения.

4.13. Допускается передача ПДн субъектов сторонним организациям, если данная передача обусловлена Федеральным законом, либо соответствующим соглашением, и не нарушает прав субъекта ПДн.

Обязанности Учреждения по устранению нарушений законодательства, допущенных при обработке персональных данных, а также по уточнению, блокированию и уничтожению персональных данных

4.14. В случае выявления неправомерной обработки ПДн при обращении субъекта ПДн или его представителя, либо по запросу субъекта ПДн или его представителя или уполномоченного органа по защите прав субъектов ПДн должно быть осуществлено блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту ПДн, или обеспечено их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) с момента такого обращения или получения указанного запроса на период внутренней проверки в Обществе.

4.15. В случае выявления неточных ПДн при обращении субъекта ПДн или его представителя, либо по их запросу или по запросу уполномоченного органа по защите прав субъектов ПДн, должно быть осуществлено блокирование ПДн, относящихся к этому субъекту ПДн, или обеспечено их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) с момента такого обращения или получения указанного запроса на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта ПДн или третьих лиц.

4.16. В случае подтверждения факта неточности ПДн на основании сведений, представленных субъектом ПДн или его представителем либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов, должно быть проведено уточнение ПДн работником, ответственным за организацию обработки и обеспечение безопасности ПДн, либо обеспечено их уточнение (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) в течение семи рабочих дней со дня представления таких сведений и снято блокирование ПДн. Уточнение ПДн должно производиться на основании данных, полученных от субъекта ПДн.

4.17. В случае выявления неправомерной обработки ПДн, осуществляемой Учреждением или лицом, действующим по поручению Учреждения, Учреждение в срок, не превышающий трех рабочих дней с даты этого выявления, обязано прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению Учреждения. В случае, если обеспечить правомерность обработки ПДн невозможно, Учреждение в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн, обязано уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении ПДн Учреждение обязано уведомить субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.
4.18. В случае достижения цели обработки ПДн Учреждение обязано прекратить обработку ПДн или обеспечить ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) и уничтожить персональные данные или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Учреждением и субъектом ПДн, либо если Учреждение не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законодательством.
4.19. В случае отзыва субъектом ПДн согласия на обработку его ПДн Учреждение обязано прекратить их обработку или обеспечить прекращение такой обработки (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить персональные данные или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Учреждением и субъектом ПДн либо если Учреждение не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законодательством.
4.20. В случае невозможности уничтожения ПДн в течение срока, указанного в п. 4.17 – 4.19, Учреждение осуществляет блокирование таких ПДн или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) и обеспечивает уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен Федеральными законами.

Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

4.21. Работники Учреждения несут персональную ответственность за сохранность ПДн, к которым они имеют доступ.
4.22. Работники Учреждения, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн, могут быть привлечены к ответственности, предусмотренной действующим законодательством РФ и локальными нормативными актами Учреждения.

5. Оценка угроз безопасности информации

5.1. Информация, обрабатывающаяся в ИСПДн Учреждения, телекоммуникационных сетях, представляет интерес для конкурентов, коммерческих организаций и криминальных структур.
5.2. Материальными носителями ПДн, применяющимися в технических средствах и системах, являются: бумажные носители, накопители на жестких магнитных дисках, оптические и магнитные диски и ленты, флэш-память.
5.3. Основные виды угроз и источники угроз безопасности представлены в «Частной модели угроз безопасности ПДн».

6. Организационные мероприятия по защите персональных данных при их обработке и передаче в информационных системах персональных данных

6.1. В общем случае организационные мероприятия по защите ПДн связаны с формированием системы документов по защите ПДн, их разработкой, официальным оформлением и доведением до исполнителей, а также организацией контроля за соблюдением установленных этими документами правил и требований.

6.2. Мероприятия должны исключить возможность утечки информации, обрабатываемой в ИСПДн, и обеспечить запрет передачи ПДн по открытым каналам связи без применения установленных мер по ее защите, а также исключить возможность внесения в контролируемую зону устройств регистрации и накопления информации без соответствующего разрешения.

Система документов по защите информации

6.3. Система документов по защите информации включает действующее законодательство РФ и локальные нормативные акты Учреждения.

6.4. Состав внутренних документов, разрабатываемых на основании действующего законодательства РФ и локальных нормативных актов Учреждения, определяется на этапе приведения процессов обработки ПДн в Обществе в соответствие требованиям законодательства. Состав документов определяется Учреждением при возможном привлечении организаций-лицензиатов.

6.5. В подразделении, обслуживающем ИСПДн, рекомендуется иметь комплект эксплуатационной и технической документации на ИСПДн, в том числе на систему защиты ПДн.

6.6. Обязанность поддерживать комплект документов по защите ПДн в актуальном состоянии возлагается на работника, ответственного за организацию обработки и обеспечение безопасности ПДн.

Организационные мероприятия по защите ПДн, обрабатываемых на автоматизированном рабочем месте (далее по тексту «АРМ»)

6.7. Организационные мероприятия по защите ПДн, обрабатываемых на АРМ, должны быть связаны с обеспечением:

– сохранности машинных носителей информации, материалов печати и исключения доступа к ним посторонних лиц;

– ограничения физического доступа и контроль доступа к изменению конфигурации средств электронно-вычислительной техники (замки на коммутационных шкафах, использование специальных защитных знаков, пломбирование, опечатывание и др.);

– исключения возможностей несанкционированного просмотра изображений с монитора АРМ (терминала) через дверные проемы, окна – в том числе с использованием средств телевизионной, фотографической и визуальной оптической разведки, находящихся за границами контролируемой зоны;

– режима блокирования доступа к АРМ (терминалу) во время отсутствия Пользователя;

– режима блокирования доступа в помещение с установленным АРМ (терминалом) во внерабочее время и в рабочее время при отсутствии Пользователя.

Организационные мероприятия по защите ПДн в локальных вычислительных сетях (далее по тексту «ЛВС»)

6.8. Указанные мероприятия должны, включать:

– обеспечение режима запрета на вхождение в сеть под чужой учетной записью;

– обеспечение периодической смены паролей Пользователями;

– обеспечение хранения файлов с информацией в групповых каталогах (каталогах, информация в которых является доступной для определенной группы лиц), структура которых однозначно отображает организационную структуру подразделения (управления, отдела, группы и др.) и разрешения доступа к нему только Работников соответствующей структурной единицы;

– обеспечение файлового обмена информацией между Пользователями подразделений через создаваемый каталог общего использования, информация в котором является доступной для имеющих санкционированный доступ в ЛВС Пользователей;
– обеспечение создания для каждого пользователя локальной вычислительной сети личного сетевого каталога, предназначенного для хранения пользовательских данных, и предоставление ему всех прав (чтение, запись, создание, удаление, переименование) в отношении информации указанного каталога, за исключением права изменения привилегий доступа;
– обеспечение контроля присвоения Пользователям учетных записей и их удаление или блокирование при увольнении Работника;
– обеспечение резервного копирования электронных информационных ресурсов;
– обеспечение режима разграничения и контроля доступа к аппаратным и программным ресурсам локальных вычислительных сетей и АРМ.

7. Технические мероприятия по защите персональных данных

7.1. Технические мероприятия по защите информации разрабатываются по результатам обследования объекта информатизации, предназначенного для обработки ПДн, и оценки возможностей реализации замысла защиты на основе применения организационных мер защиты и активизации встроенных механизмов защиты используемых операционных систем и аппаратного обеспечения. Соответствующие требования излагаются в техническом задании на проектирование системы защиты.
7.2. Требуется осуществлять следующие технические мероприятия:
– применение сертифицированных программных и (или) аппаратных средств защиты информации от несанкционированного доступа, контроля целостности, регистрации и учета действий пользователей ИСПДн;
– применение сертифицированных средств криптографической защиты конфиденциальной информации при ее передаче по открытым каналам связи;
– предотвращение несанкционированной записи ПДн на съемные носители информации или вывода ПДн на печать;
– регулярный анализ защищенности системы защиты ПДн;
– защита ПДн при межсетевом взаимодействии;
– применение антивирусной защиты.

8. Контроль состояния системы защиты персональных данных

Общие вопросы контроля состояния защиты ПДн

8.1. В рамках проверок состояния защиты ПДн рекомендуется осуществлять контроль:
– наличия в подразделениях нормативных документов по защите информации и доведения их до персонала с фиксацией факта ознакомления с документами;
– знания и выполнения работниками требований локальных нормативных актов Учреждения по защите ПДн при их обработке в ИСПДн Учреждения;
– наличия и комплектности эксплуатационной и технической документации на систему защиты ПДн, а так же факта ознакомления работников Учреждения с инструкциями пользователей и администраторов средств защиты информации с соответствующей отметкой об ознакомлении в инструкциях;
– работоспособности системы защиты ПДн;
– задания требований по безопасности ПДн при разработке (модернизации) ИСПДн.
8.2. Контроль состояния защиты ПДн осуществляется в плановом и внеплановом порядке ответственным за организацию обработки и обеспечение безопасности ПДн Работником (либо комиссией), назначаемым Учреждением.
8.3. Результаты проверок оформляются в виде отчетов о проведении проверки.