Приложение № 1

к приказу от «29» декабря 2017 г. № 193-ОД

УТВЕРЖДАЮ
Директор ОБУ «Уполномоченный многофункциональный центр предоставления государственных и муниципальных услуг Липецкой области»

М.В. Селянина
«29» декабря 2017 г.

Положение о защите информации

1. Определения

1.1 Информационная система, ИС – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

1.2 Пользователь – лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в информационной системе или использующее результаты ее функционирования.

В настоящем Положении под пользователями понимаются как пользователи ИС (в том числе ИС персональных данных) в административном отделе ОБУ «УМФЦ Липецкой области», так и пользователи ИС (в том числе ИС персональных данных) в структурных подразделениях ОБУ «УМФЦ Липецкой области», если не оговорено иное.

1.3 Внутренний пользователь – пользователь информационной системы персональных данных, являющийся сотрудником организации, эксплуатирующей информационную систему персональных данных.

1.4 Внешний пользователь – пользователь информационной системы персональных данных, не являющийся сотрудником организации, эксплуатирующей информационную систему персональных данных.

1.5 Администратор безопасности – пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) системы защиты информации информационной системы в соответствии с установленной ролью.

В настоящем Положении под администраторами безопасности понимаются как администраторы безопасности в административном отделе ОБУ «УМФЦ Липецкой области», так и администраторы безопасности в структурных подразделениях ОБУ «УМФЦ Липецкой области», если не оговорено иное.

1.6 Администратор системный – пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) информационной системы в соответствии с установленной ролью.

В настоящем Положении под системными администраторами понимаются как системные администраторы в административном отделе ОБУ «УМФЦ Липецкой области», так и системные администраторы в структурных подразделениях ОБУ «УМФЦ Липецкой области», если не оговорено иное.

1.7 Компьютерный вирус – компьютерная программа либо иная компьютерная информация, предназначенная для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации.

1.8 Конфигурация информационной системы и её системы защиты информации – состав и взаимосвязи (электрические, логические, программные, геометрические) составных частей информационной системы и средств защиты информации.

1.9 Событие информационной безопасности – идентифицированное возникновение состояния информационной системы (сегмента, компонента информационной системы), сервиса или сети, указывающее на возможное нарушение безопасности информации, или сбой средств защиты информации, или ранее неизвестную ситуацию, которая может быть значимой для безопасности информации.

1.10 Ответственный за организацию обработки персональных данных – лицо, организующее и контролирующее выполнение требований регламентных документов, определяющих политику оператора в отношении обработки персональных данных, в том числе требований по защите персональных данных.

2. Общие положения

2.1 Настоящее Положение по организации обработки и защиты персональных данных (далее – ПДн) при их обработке в информационной системе (далее – ИС) разработано в соответствии со следующими нормативными правовыми актами:

- Федеральный закон от 27.07.2006 № 149–ФЗ «Об информации, информационных технологиях и защите информации»;
- Федеральный закон от 27.07.2006 № 152–ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»);
- Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

2.2 Настоящее Положение регламентирует действия сотрудников Организации после ввода ИС в эксплуатацию. Ввод ИС в эксплуатацию осуществляется приказом руководителя Организации.

2.3 Настоящее Положение определяет порядок действий сотрудников ОБУ «УМФЦ Липецкой области» (далее – Организация) и внешних пользователей при организации обработки и защиты ПДн, содержащихся в ИС. Перечень ПДн, обрабатываемых в ИС, утверждает руководитель Организации.

2.4 Настоящее Положение описывает процессы организации обработки и защиты ПДн при их обработке в ИС, обеспечивающие установленный уровень защищенности ПДн. Требуемый уровень защищенности ПДн при их обработке в ИС установлен решением специальной комиссии.

2.5 Настоящее Положение вступает в силу после его утверждения руководителем Организации и действует бессрочно, до момента его замены новым.

2.6 Все пользователи ИС, должны быть ознакомлены с настоящим Положением под роспись.

2.7 Для организации обработки ПДн в ИС в соответствии с требованиями п. 1 части 1 ст. 18.1 Федерального закона «О персональных данных» руководитель Организации приказом назначает должностное лицо, ответственное за организацию обработки ПДн в ОБУ «УМФЦ Липецкой области», и должностных лиц, ответственных за организацию обработки ПДн в структурных подразделениях (далее – СП) ОБУ «УМФЦ Липецкой области».

2.8 При выполнении своих обязанностей ответственный за организацию обработки ПДн в ОБУ «УМФЦ Липецкой области» действует в соответствии с требованиями документа «Должностная инструкция ответственного за организацию обработки конфиденциальной информации, в том числе персональных данных, в ОБУ «УМФЦ Липецкой области», содержащего должностные обязанности ответственного за организацию обработки ПДн в ОБУ «УМФЦ Липецкой области».

2.9 При выполнении своих обязанностей ответственные за организацию обработки ПДн в СП ОБУ «УМФЦ Липецкой области» действуют в соответствии с требованиями документа «Должностная инструкция ответственного за организацию обработки конфиденциальной информации, в том числе персональных данных, в структурных подразделениях ОБУ «УМФЦ Липецкой области», содержащего должностные обязанности ответственных за организацию обработки ПДн в СП ОБУ «УМФЦ Липецкой области».

2.10 Для непосредственного выполнения работ с программными и программно-аппаратными средствами защиты информации (далее – СЗИ), а также для сопровождения и контроля работы пользователей ИС руководитель Организации в соответствии с требованиями постановления Правительства Российской Федерации от 01.11.2012 № 1119 п. 14 назначает должностное лицо, ответственное за обеспечение безопасности ПДн, обрабатываемых в ИС, в административном отделе ОБУ «УМФЦ Липецкой области» (далее – администратор безопасности в ОБУ «УМФЦ Липецкой области»), и должностных лиц, ответственных за обеспечение

безопасности ПДн, обрабатываемых в ИС, в СП ОБУ «УМФЦ Липецкой области» (далее – администраторы безопасности в СП ОБУ «УМФЦ Липецкой области»).

2.11 При выполнении своих обязанностей по обеспечению безопасности ПДн, обрабатываемых в ИС, администратор безопасности в ОБУ «УМФЦ Липецкой области» действует в соответствии с требованиями документа «Должностная инструкция администратора безопасности в ОБУ «УМФЦ Липецкой области» и требованиями эксплуатационной документации на СЗИ.

2.12 При выполнении своих обязанностей по обеспечению безопасности ПДн, обрабатываемых в ИС, администраторы безопасности в СП ОБУ «УМФЦ Липецкой области» действуют в соответствии с требованиями документа «Должностная инструкция администраторов безопасности в структурных подразделениях ОБУ «УМФЦ Липецкой области» и требованиями эксплуатационной документации на СЗИ.

2.13 Обязанности системных администраторов, уполномоченных выполнять некоторые действия по администрированию ИС в соответствии с установленной ролью, осуществляют инженеры-программисты в административном отделе ОБУ «УМФЦ Липецкой области» и инженеры-программисты в СП ОБУ «УМФЦ Липецкой области».

2.14 Все пользователи ИС участвуют в защите ПДн и обязаны знать и выполнять требования:

- нормативных правовых документов по защите ПДн;
- настоящего Положения и перечисленных в нем инструкций в части, их касающейся.

2.15 В соответствии с требованиями пункта 2 части 1 ст. 18.1 Федерального закона «О персональных данных» руководителем Организации утверждаются документы, определяющие политику Организации в отношении обработки ПДн, локальные акты по вопросам обработки ПДн, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

3. Состав организационно-распорядительной документации:

- Приказ о назначении ответственных лиц:
  - комиссии по классификации и установлению уровня защищенности ИС;
  - ответственного за организацию обработки конфиденциальной информации, в том числе ПДн;
  - администраторов безопасности;
- Приказ об организации контроля (мониторинга) за обеспечением уровня защищенности информации;
- Приказ об организации режима безопасности помещений;
- Приказ об обращении со средствами криптографической защиты информации (далее – СКЗИ);
- Должностная инструкция системного администратора;
- Должностная инструкция пользователя информационной системы;
- Инструкция по обращению с СКЗИ;

- Инструкция ответственного за организацию работ по криптографической защите информации;
- Инструкция по выявлению и реагированию на инциденты безопасности обработки информации;
- Инструкция по организации резервного копирования и восстановления информации;
- Инструкция по организации учёта, использования и уничтожения машинных носителей информации;
- Инструкция по организации парольной защиты;
- Инструкция по антивирусной защите;
- Инструкция по обеспечению защиты информации при выводе из эксплуатации;
- Правила работы с обезличенными ПДн;
- Правила обработки конфиденциальной информации, в том числе ПДн;
- Правила рассмотрения запросов субъектов ПДн или их представителей;
- Правила осуществления внутреннего контроля;
- Положение о защите информации;
- Положение о разрешительной системе доступа;
- Порядок доступа в помещения, в которых размещены компоненты информационных систем и (или) используемые СКЗИ;
- Перечень должностей, замещение которых предусматривает использование СКЗИ;
- Перечень должностей сотрудников, замещение которых предусматривает осуществление обработки информации ограниченного доступа, либо осуществление доступа к ней;
- Перечень должностей сотрудников, замещение которых предусматривает осуществление доступа к содержанию электронных журналов сообщений;
- Перечень информационных систем;
- Перечень конфиденциальной информации, в том числе ПДн;
- Перечень мест хранения машинных носителей информации и назначение ответственных за их хранение и учёт;
- Перечень должностей сотрудников, ответственных за проведение мероприятий по обезличиванию обрабатываемых ПДн;
- Перечень ответственных за помещения, в которых обрабатывается конфиденциальная информация, в том числе ПДн, или где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ;
- Журнал учёта проверок юридического лица;
- Журнал поэкземплярного учёта средств защиты информации, эксплуатационной и технической документации;
- Технический (аппаратный) журнал;
- Журнал инструктажа пользователей;

- Журнал учёта обращений субъектов ПДн и их законных представителей;
- Журнал учёта запросов уполномоченного органа по защите прав субъектов ПДн;
- Журнал учёта передачи ПДн;
- Журнал учёта и выдачи машинных носителей информации ограниченного доступа;
- Журнал учёта выдачи паролей;
- Журнал учёта аппаратных средств аутентификации;
- Журнал учёта инцидентов безопасности информации;
- Журнал по учёту мероприятий по контролю защищённости информации ограниченного доступа;
- Журнал учёта ключей от сейфов и помещений;
- Журнал поэкземплярного учёта СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;
- Типовая форма согласия на обработку ПДн;
- Типовая форма разъяснения субъекту ПДн юридических последствий отказа предоставить свои ПДн;
- Типовое обязательство сотрудника, непосредственно осуществляющего обработку конфиденциальной информации, в том числе ПДн, в случае расторжения с ним трудового договора прекратить обработку конфиденциальной информации, в том числе ПДн, ставших известными ему в связи с исполнением должностных обязанностей;
- Уведомление об обработке ПДн;
- Заявление на блокировку ПДн;
- Заявление на уничтожение ПДн;
- Заявление на уточнение ПДн;
- Акт об уничтожении машинных носителей информации ограниченного доступа;
- Акты классификации информационных систем;
- Акты об оценке вреда, который может быть причинён субъектам ПДн;
- Акты об уничтожении криптографических ключей, содержащихся на ключевых носителях, и ключевых документов;
- Акты определения уровня защищённости ПДн;
- Модель угроз безопасности информации и Модель нарушителя безопасности информации.

4. Реализация мер защиты персональных данных

4.1 Идентификация и аутентификация

4.1.1 Процесс идентификации и аутентификации пользователей ИС осуществляется на этапе эксплуатации ИС и предназначен для защиты конфиденциальной информации, в том числе ПДн, от несанкционированного доступа.

4.1.2 Порядок действий пользователей ИС в процессе идентификации (узнавании) и аутентификации (подтверждении подлинности узнанного

пользователя) при входе в ИС описаны в «Инструкции по организации парольной защиты».

4.2 Управление доступом субъектов доступа к объектам доступа

4.2.1 Процесс управления доступом пользователей ИС к ПДн осуществляется на этапе эксплуатации ИС и предназначен для защиты ПДн от несанкционированного доступа.

4.2.2 Порядок управления доступом пользователей к информационным ресурсам ИС описан в «Положении о разрешительной системе доступа».

4.3 Управление программным обеспечением ИС и СЗИ

4.3.1 Процесс управления программным обеспечением технических средств ИС и средств защиты информации осуществляется на этапе эксплуатации ИС и предназначен для обеспечения целостности и доступности ПДн, а также защиты конфиденциальной информации, в том числе ПДн, от несанкционированного доступа.

4.3.2 Установку (обновление) программного обеспечения (далее – ПО) ИС осуществляет системный администратор, имеющий необходимые полномочия в соответствии с «Положением о разрешительной системе доступа».

4.3.3 Установку (обновление) ПО системы защиты информации ИС, осуществляет администратор безопасности.

4.3.4 Установка ПО производится с рабочих копий оригинальных лицензионных дистрибутивных носителей (дискет, компакт-дисков и т. п.), полученных законным порядком. Устанавливаемое ПО должно иметь необходимую эксплуатационную документацию и Инструкции пользователя.

4.3.5 Устанавливаемое ПО должно быть предварительно проверено (протестировано) администратором безопасности на работоспособность, отсутствие опасных функций, а также на совместимость с установленными в ИС программными и техническими средствами, в том числе ПО СЗИ.

4.3.6 После установки (обновления) программного обеспечения системный администратор и администратор безопасности, каждый в своей части, выполняют необходимые настройки, выполняют тестирование работоспособности и вносят необходимые изменения в эксплуатационную документацию на ИС и ее систему защиты информации.

4.3.7 Администратор безопасности и системный администратор ИС, каждый в своей части, проводят оценку изменений в ПО на условия отклонения технологического процесса обработки ПДн в ИС от ранее принятого. При обнаружении отклонений администратор безопасности и системный администратор ИС, каждый в своей части, докладывают об обнаруженных отклонениях ответственному за организацию обработки ПДн.

4.3.8 После обновления ПО администратор безопасности заменяет носители с дистрибутивом неактуального программного обеспечения на носители с дистрибутивом обновленного ПО.

4.4 Защита машинных носителей ПДн

4.4.1 Процесс защиты машинных носителей персональных данных осуществляется на этапе эксплуатации ИС и предназначен для обеспечения целостности ПДн, а также защиты персональных данных от несанкционированного доступа к информации, содержащейся на машинных носителей.

4.4.2 Порядок действий пользователей ИС при работе с машинными носителями информации, правила учёта, хранения и доступа к машинным носителям и к ПДн, содержащихся на машинных носителях описаны в «Инструкции по организации учёта, использования и уничтожения машинных носителей информации».

4.5 Управление событиями информационной безопасности

4.5.1 Процесс управления событиями информационной безопасности осуществляется на этапе эксплуатации ИС и предназначен для обеспечения целостности и доступности ПДн, а также защиты ПДн от несанкционированного доступа к информации за счёт своевременного распознавания технических неисправностей и попыток несанкционированного доступа на основе анализа фиксируемых событий, связанных с отклонениями от штатного режима работы ИС.

4.5.2 Настройку журналов регистрации событий информационной безопасности в программном обеспечении ИС и СЗИ осуществляет системный администратор ИС на основании предоставленных полномочий и администратор безопасности каждый в своей части. Настройка осуществляется на основе перечня состава и содержания информации о событиях безопасности в соответствии с эксплуатационной документацией на программно–технические средства ИС.

4.5.3 Системный администратор ИС и администратор безопасности должны не реже 1 раза в неделю просматривать электронные журналы регистрации событий безопасности.

4.5.4 Настройки электронных журналов регистрации событий информационной безопасности должны обеспечивать запись в память технических средств ИС и СЗИ информации о поступающих событиях безопасности без переполнения памяти в течение 1 месяца.

4.5.5 Информация о событиях безопасности в ИС, не подлежащая автоматической регистрации (нерегистрируемые программно-аппаратные сбои и неисправности, нарушения организационно-правового плана) должна фиксироваться администратором безопасности при её обнаружении в Журнале учёта инцидентов безопасности информации.

4.5.6 Администратор безопасности должен подробно исследовать наиболее часто повторяющиеся события безопасности, выяснять причины их возникновения и устранять эти причины.

4.5.7 На основании регистрируемой и сохраняемой информации о событиях информационной безопасности в ИС администратор безопасности отчитывается перед ответственным за организацию обработки конфиденциальной информации, в том числе ПДн.

4.5.8 Права доступа к файлам отчетов журналов безопасности и настройкам журналов установлены администратору безопасности и системным администраторам ИС и отражены в «Положении о разрешительной системе доступа».

4.6 Антивирусная защита

4.6.1 Процесс антивирусной защиты осуществляется на этапе эксплуатации ИС и предназначен для обеспечения целостности и доступности персональных данных, а также защиты персональных данных от несанкционированного доступа к информации с помощью своевременного распознавания атак вредоносных программ (вирусов) и их нейтрализации.

4.6.2 Порядок действий пользователей при обнаружении в ИС компьютерных вирусов, описаны в «Инструкции по антивирусной защите».

4.7 Обнаружение вторжений

4.7.1 Процесс обнаружения вторжений осуществляется на этапе эксплуатации ИС и предназначен для обеспечения целостности и доступности персональных данных, а также защиты персональных данных от несанкционированного доступа к информации с помощью своевременного распознавания программных вторжений с целью получения несанкционированного доступа к ресурсам ИС, их нейтрализации.

4.7.2 Цель обнаружения вторжений: выявить проникновение в информационную систему. С этой целью в систему защиты информации, обрабатываемой в информационной системе (далее – ИС) должна быть включена система обнаружения вторжений (далее – СОВ).

4.7.3 СОВ представляет собой программно-аппаратный комплекс, который для эффективного обнаружения вторжений необходимо настроить перед началом эксплуатации и в дальнейшем контролировать состояние настроек и производить их изменение при необходимости.

4.7.4 За управление СОВ и за действия при обнаружении вторжений отвечает администратор безопасности в ОБУ «УМФЦ Липецкой области».

4.7.5 К действиям по управлению СОВ относятся:

- подключение и настройка параметров работы СОВ;
- загрузка в СОВ решающих правил;
- настройка параметров автоматической загрузки решающих правил;
- назначение решающих правил детекторам атак;
- добавление в СОВ собственных и корректировка уже имеющихся правил при такой необходимости;
- настройка и контроль обновлений базы решающих правил.

4.7.6 Доступ к управлению СОВ разрешен только администратору безопасности в ОБУ «УМФЦ Липецкой области» с помощью пароля,

устанавливаемого самим администратором безопасности в ОБУ «УМФЦ Липецкой области». Правила назначения пароля в соответствии с «Инструкцией по организации парольной защиты».

4.7.7 Конфигурация настроек СОВ должна быть сохранена на съемном носителе.

4.7.8 Хранение и учёт съемных носителей, содержащих настройки СОВ, обеспечивает администратор безопасности в соответствии с «Инструкцией по организации учёта, использования и уничтожения машинных носителей информации».

4.7.9 Конкретные действия администратора безопасности в ОБУ «УМФЦ Липецкой области» по управлению СОВ приведены в Руководстве администратора СОВ.

4.7.10 Действия при обнаружении СОВ вторжения должны быть определены ответственным за организацию обработки персональных данных в ОБУ «УМФЦ Липецкой области» совместно с администратором безопасности в ОБУ «УМФЦ Липецкой области» исходя из возможностей СОВ и требований к технологии обработки персональных данных. На основе принятых решений администратор безопасности в ОБУ «УМФЦ Липецкой области» настраивает параметры СОВ.

4.7.11 Обнаруженные вторжения квалифицируются как инциденты и обрабатываются по правилам, установленным в документе «Инструкция по управлению инцидентами».

4.7.12 Решающие правила, используемые в СОВ, определяют эффективность обнаружения вторжений. Решающие правила загружаются в СОВ при вводе ее в эксплуатацию.

4.7.13 В условиях постоянно изменяющихся способов и алгоритмов вторжений решающие правила для надежного обнаружения вторжений должны быть актуальны. Актуальность решающих правил обеспечивается своевременным обновлением баз решающих правил.

4.7.14 Контроль обновлений баз решающих правил в СОВ осуществляет администратор безопасности в ОБУ «УМФЦ Липецкой области».

4.8 Контроль (анализ) защищенности ИС

4.8.1 Процесс контроля защищенности ИС осуществляется на этапе эксплуатации ИС и предназначен для обеспечения целостности и доступности персональных данных, а также защиты персональных данных от неучтенных и вновь возникающих угроз информационной безопасности.

4.8.2 Порядок действий системных администраторов и администраторов безопасности с целью:

- выявления ошибок и недостатков программного обеспечения и аппаратных средств ИС и СЗИ;
- контроля установки обновлений программного обеспечения, контроля работоспособности и настроек программного обеспечения;

– контроля состава технических средств ИС и системы защиты информации;
– контроля правил работы с паролями и учётными записями, –

описан в «Правилах осуществления внутреннего контроля».

4.9 Обеспечение целостности ИС и ПДн

4.9.1 Контроль и поддержание целостности программного обеспечения ИС, в том числе программного обеспечения средств защиты информации, обеспечивают администраторы безопасности и системные администраторы ИС.

4.9.2 Способы контроля целостности программного обеспечения определяются администратором безопасности перед началом эксплуатации ИС. В зависимости от принятого способа контроля администратор безопасности организует безопасное хранение между проверками контрольных сумм или ключей хеширования для используемого программного обеспечения (далее – ПО).

4.9.3 Контроль целостности программного обеспечения осуществляется периодически не реже 1 раза в три месяца по определенному плану, неизвестному пользователям ИС. План контроля целостности программного обеспечения ИС разрабатывает администратор безопасности.

4.9.4 Контроль целостности программного обеспечения осуществляется комиссией под председательством администратора безопасности с использованием специального программного обеспечения.

4.9.5 Защиту от спама в ИС организует администратор безопасности с помощью установки специального программного обеспечения и настройкой фильтров.

4.9.6 Администратор безопасности должен периодически, не реже 1 раза в три месяца контролировать эффективность специального программного обеспечения, защищающего ИС от спама и уточнять настройки фильтров.

4.10 Обеспечение доступности ПДн

4.10.1 Порядок действий пользователей по обеспечению доступности ПДн, описан в «Инструкции по организации резервного копирования и восстановления информации».

4.11 Защита технических средств ИС

4.11.1 Порядок доступа пользователей к техническим средствам ИС и СЗИ, описаны в «Порядок доступа в помещения, в которых размещены компоненты информационных систем и (или) используемые СКЗИ».

4.12 Управление инцидентами

4.12.1 Порядок действий пользователей, администраторов безопасности и системных администраторов при возникновении инцидентов и их устранении, описан в «Инструкции по выявлению и реагированию на инциденты безопасности обработки информации».

5. Заключительные положения

5.1 Пользователи ИС должны быть предупреждены об ответственности за действия с персональными данными, содержащимися в ИС и действия с

техническими средствами ИС и СЗИ, нарушающие требования настоящего Положения.

5.2 Пользователи ИС должны быть ознакомлены в части их касающейся, с настоящим Положением до начала работы в ИС под роспись.

5.3 Обязанность ознакомления сотрудников административного отдела ОБУ «УМФЦ Липецкой области» с настоящим Положением лежит на ответственном за организацию обработки ПДн в ОБУ «УМФЦ Липецкой области».

5.4 Обязанность ознакомления сотрудников СП ОБУ «УМФЦ Липецкой области» с настоящим Положением лежит на ответственных за организацию обработки конфиденциальной информации, в том числе персональных данных, в соответствующих СП, а также в СП, закреплённых за соответствующими СП Приказом от 01.08.2017 № 108-ОД.

5.5 Контроль выполнения и соблюдения пользователями ИС в административном отделе ОБУ «УМФЦ Липецкой области» требований, инструкций, положений и правил, перечисленных в пункте 4 и его подпунктах, обеспечивает администратор безопасности в ОБУ «УМФЦ Липецкой области».

5.6 Контроль выполнения и соблюдения пользователями ИС в СП ОБУ «УМФЦ Липецкой области» требований, инструкций, положений и правил, перечисленных в пункте 4 и его подпунктах, обеспечивают администраторы безопасности в соответствующих СП, а также в СП, закреплённых за соответствующими СП Приказом от 01.08.2017 № 108-ОД.

5.7 Контроль выполнения и соблюдения администраторами безопасности в ОБУ «УМФЦ Липецкой области» требований, инструкций, положений и правил, перечисленных в пункте 4 и его подпунктах, обеспечивает ответственный за организацию обработки конфиденциальной информации, в том числе персональных данных, в ОБУ «УМФЦ Липецкой области».

5.8 Контроль выполнения и соблюдения администраторами безопасности в СП ОБУ «УМФЦ Липецкой области» требований, инструкций, положений и правил, перечисленных в пункте 4 и его подпунктах, обеспечивают ответственные за организацию обработки конфиденциальной информации, в том числе персональных данных, в соответствующих СП, а также в СП, закреплённых за соответствующими СП Приказом от 01.08.2017 № 108-ОД.

ОБУ «УМФЦ Липецкой области»

(наименование организации)

ЖУРНАЛ
учёта средств защиты информации, установленных в информационной системе персональных данных

Дата начала «___» _____ 201__

Дата окончания «___» _____ 201__

ПОРЯДОК ЗАПОЛНЕНИЯ ЖУРНАЛА УЧЁТА

1. Журнал учёта заполняется шариковой ручкой синего цвета.

2. Не допускается написание более одной строчки текста в строке журнала, т.е. текст переносится на следующую строку журнала.

3. № пункта, номера – необходимо проставлять арабскими цифрами без точки на конце.

4. Наименование средств писать полностью без сокращений.

5. Формат даты: ЧЧ. ММ. ГГ.

6. Для исправления ошибок необходимо перечеркнуть (одной чертой) неправильное написание, вписать правильное и поставить подпись должностного лица организации, заверив ее печатью организации, с указанием даты исправления. Не допускается исправления ошибок с помощью корректирующего средства.

№ п/п	Регистрационный номер	Наименование	Сведения об установке средства защиты информации			Сведения об изъятии/удалении средства защиты информации			Примечание
			Дата установки	Место установки (использования)	Ф.И.О. производившего установку, подпись	Дата изъятия/ удаления	Ф.И.О. производившего изъятие/удаление, подпись	Причина изъятия/ удаления	

ОБУ «УМФЦ Липецкой области»

(наименование организации)

ТЕХНИЧЕСКИЙ (АППАРАТНЫЙ) ЖУРНАЛ

Дата начала «___» _____ 201__
Дата окончания «___» _____ 201__

№ п.п.	Наименование ТС, ПО или эксплуатационной и технической документации	Серийные номера ТС или ПО, эксплуатационной и технической документации	Лицо, установившее ТС или ПО			Дата уничтожения	Прим.
			ФИО	Роспись	Дата		
1	2	3	4	5	6	7	8

ОБУ «УМФЦ Липецкой области»

(наименование организации)

ЖУРНАЛ

инструктажа пользователей информационных систем персональных данных и обслуживающего персонала по правилам обработки персональных данных

Дата начала «___» _____ 201__

Дата окончания «___» _____ 201__

№ п/п	Наименование инструктажа	Дата проведения инструктажа	Фамилия И.О. проводившего инструктаж	Должность и структурное подразделение лица, проводившего инструктаж	Фамилия И.О. пользователя или обслуживающего персонала	Подпись лица, получившего инструктаж	Подпись лица, проводившего инструктаж	Примечание
1	2	3	4	5	6	7	8	9