«Утверждаю»

Директор МБУ МЦФОСМР «Надежда»

_____ А.В. Евсиков

«____» _____20___г.

Положение о политике

Политика муниципального бюджетного учреждения

«Межпоселенческий центр физкультурно-оздоровительной и спортивно-массовой работы «Надежда» по обработке и защите персональных данных

1. Общие положения

Политика муниципального бюджетного учреждения «Межпоселенческий центр физкультурно-оздоровительной и спортивно-массовой работы «Надежда» по обработке и защите персональных данных (далее - политика) определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, требований и принципов в области информационной безопасности, которыми руководствуется муниципальное бюджетное учреждение «Межпоселенческий центр физкультурно-оздоровительной и спортивно-массовой работы «Надежда» в своей деятельности.

Основными целями политики являются защита обрабатываемых персональных данных и обеспечение эффективной работы всей информационно-вычислительной системы муниципального бюджетного учреждения «Межпоселенческий центр физкультурно-оздоровительной и спортивно-массовой работы «Надежда» (далее - Оператор) при осуществлении своей деятельности.

Общее руководство обеспечением информационной безопасности Оператора осуществляет Директор муниципального бюджетного учреждения «Межпоселенческий центр физкулььтурно-оздоровительной и спортивно-массовой работы «Надежда».

Сотрудники Оператора обязаны соблюдать порядок обращения с конфиденциальными документами, ключевыми носителями и другой защищаемой информацией, соблюдать требования настоящей политики и иных документов, регламентирующих деятельность в области информационной безопасности.

Настоящая политика распространяется на всех сотрудников Оператора и обязательна, к исполнению всеми ее сотрудниками.

Положения настоящей политики применимы для использования во внутренних нормативных и методических документах Оператора.

Настоящая политика является общедоступным документом, декларирующим основы деятельности Оператора при обработке персональных данных.

2. Информация об операторе, осуществляющем обработку персональных данных

Наименование: Муниципальное бюджетное учреждение «Межпоселенческий центр физкультурно-оздоровительной и спортивно-массовой работы «Надежда»

ИНН: 5077010184

Адрес местонахождения: Московская область, Серпуховский район, п. Большевик, ул. Ленина, д. 36

Почтовый адрес: 142253, Московская область, Серпуховский район, п. Большевик, ул. Спортивная, д. 13, дворец спорта «Надежда», каб. 209

Тел. +7 (4967) 70-51-96

E-mail: gvk_nadegda@mail/ru. Интернет-страница: www.mfco-sport.ru.

Регистрационный номер в реестре операторов персональных данных - _____, приказ № ____ от _____ г.

## 3. Ответственный за обработку персональных данных

В соответствии со ст. 18.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» оператор назначил ответственного за организацию обработки персональных данных.

Ответственный за организацию обработки персональных данных осуществляет внутренний контроль соответствия обработки персональных данных согласно Федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, требованиям к защите персональных данных, настоящей политике и другим локальным актам.

Ответственным за организацию обработки персональных данных Оператора назначен Заместитель директора по безопасности

## 4. Термины и определения

В настоящей политике используются следующие термины:

Автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аудит информационной безопасности Оператора - процесс проверки выполнения установленных требований по обеспечению информационной безопасности. Может проводиться как самим Операторром (внутренний аудит), так и с привлечением независимых внешних организаций (внешний аудит).

Информационная технология - совокупность правил, приемов и методов применения средств вычислительной техники для выполнения функций хранения, обработки, передачи и использования производственной, финансовой, аналитической или иной информации, связанной с функционированием Оператора.

Информационный технологический процесс - часть производственного технологического процесса, содержащая операции над информацией, необходимой для функционирования Оператора.

Информационная безопасность Оператора - состояние защищенности информационных активов в условиях угроз в информационной сфере. Защищенность достигается обеспечением совокупности свойств информационной безопасности - конфиденциальностью, целостностью, доступностью информационных активов и инфраструктуры Оператора.

Информационные активы Оператора – активы муниципального бюджетного учреждения «Межпоселенческий центр физкультурно-оздоровительной и спортивно-массовой работы «Надежда», имеющие отношение к его информационной сфере и представляющие ценность для нее с точки зрения достижения уставных целей.

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных

данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Субъект персональных данных - физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.

Инцидент информационной безопасности - действительное, предпринимаемое или вероятное нарушение информационной безопасности, приводящее к нарушению доступности, конфиденциальности и целостности информационных активов Оператора.

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств в соответствии с законодательством.

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя, если иное не предусмотрено.

Мониторинг информационной безопасности Операторра - постоянное наблюдение за объектами, влияющими на обеспечение информационной безопасности, сбор, анализ и обобщение результатов наблюдения под заданные цели. Объектом мониторинга в зависимости от целей может быть автоматизированная система или ее часть, информационные технологические процессы, информационные услуги и прочее.

Несанкционированный доступ к информации - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем.

Политика муниципального бюджетного учреждения «Межпоселенческий центр фзкультурно-оздоровительной и спортивно-массовой работы «Надежда» по обработке и защите персональных данных - комплекс взаимоувязанных руководящих принципов, разработанных на их основе правил, процедур и практических приемов, принятых Оператором для обеспечения информационной безопасности.

Риск - мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы.

Роль - заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между субъектом и объектом Оператора. К субъектам относятся сотрудники Оператора, посетители, а также инициируемые от их имени действия над объектами. Объектами являются аппаратные и программные средства, информационные ресурсы, услуги и процессы, составляющие автоматизированную систему.

Доступ к АС - процедура регистрации (создания учетной записи пользователя) для сотрудника Оператора и предоставления ему (или изменения его) прав доступа к ресурсам АС.

Режим конфиденциальности информации - организационно-технические мероприятия по обеспечению конфиденциальности информации (защите информации), включающие в себя:

- определение перечня информации, составляющей конфиденциальную информацию;

- ограничение доступа к конфиденциальной информации путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

- учет лиц, получивших доступ к конфиденциальной информации, и (или) лиц, которым такая информация была предоставлена или передана;

- регулирование отношений по использованию конфиденциальной информации работниками на основании трудовых договоров, контрагентами на основании гражданско-правовых договоров и соглашений, работниками со срочными трудовыми договорам и проходящих у Оператора практику (стажировку).

Средство криптографической защиты информации - средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности.

Угроза - опасность, предполагающая возможность потерь (ущерба).

Управление информационной безопасностью Оператора - совокупность целенаправленных действий, осуществляемых в рамках настоящей политики в условиях угроз в информационной сфере, включающая в себя оценку состояния объекта управления (например, оценку и управление рисками), выбор управляющих воздействий и их реализацию (планирование, внедрение и обслуживание защитных мер - защита информации).

Уязвимость - недостатки или слабые места информационных активов, которые могут привести к нарушению информационной безопасности Оператора при реализации угроз в информационной сфере.

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

## 5. Обозначения и сокращения

| | |
|---|---|
| АСП - аналог собственноручной подписи; | АС - автоматизированная система;<br><br>ИС - информационная система; |
| ИБ - информационная безопасность;<br><br>ПДн – персональные данные;<br><br>ИСПДн – информационная система персональных данных; | СКЗИ - средство криптографической защиты информации;<br><br>СУБД - система управления базами данных; |
| ЛВС - локальная вычислительная сеть; | ЭВМ - электронная вычислительная машина; |
| НСД - несанкционированный доступ; | ЭП - электронная подпись. |

## 6. Нормативные ссылки

Настоящая политика разработана с учетом следующих документов:

- Федеральный закон от 6 октября 2003 г. № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации»;

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

- Федеральный закон от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»;

- постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- постановление Правительства Российской Федерации от 21 марта 2012 г. № 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»;

- постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- приказ Федеральной службы по техническому и экспертному контролю от 18 февраля 2013 г. № 21 «Об утверждении состава и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- устав Муниципального бюджетного учреждения «Межпоселенческий центр физкультурно-оздоровительной и спортивно-массовой работы «Надежда».

## 7. Основные принципы обеспечения ИБ

Основными принципами обеспечения ИБ являются:

- Постоянный и всесторонний анализ АС и информационных технологий с целью выявления уязвимостей информационных активов Оператора. Защита от угроз, исходящих от противоправных действий, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

- Своевременное обнаружение проблем, потенциально способных повлиять на ИБ Оператора, корректировка моделей угроз. Необходимо учитывать, что с течением времени меняется характер угроз, поэтому следует своевременно, используя данные мониторинга и аудита, обновлять модели угроз.

- Разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию и совместимости этих мер с действующим технологическим процессом. При

этом меры, принимаемые для обеспечения ИБ, не должны усложнять деятельность Оператора, а также повышать трудоемкость технологических процессов обработки информации и создавать дополнительные сложности.

- Контроль эффективности принимаемых защитных мер.

- Персонификация и адекватное разделение ролей и ответственности между работниками Оператора, исходя из принципа персональной и единоличной ответственности за совершаемые операции.

## 8. Цели и задачи информационной безопасности

Основными целями ИБ Оператора являются:

- повышение стабильности функционирования Оператора целом;

- достижение адекватности мер по защите от реальных угроз ИБ;

- предотвращение или снижение ущерба от инцидентов ИБ.

Основными задачами деятельности по обеспечению ИБ Оператора являются:

- выполнение требований действующего законодательства Российской Федерации по обеспечению ИБ;

- контроль выполнения установленных требований по обеспечению ИБ;

- повышение эффективности мероприятий по обеспечению и поддержанию ИБ с учетом требований системы менеджмента качества;

- разработка и совершенствование организационно-распорядительных документов Оператора в области обеспечения ИБ;

- выявление, оценка и прогнозирование угроз ИБ;

- выработка рекомендаций по устранению уязвимостей;

- организация антивирусной защиты информационных активов;

- защита информации от НСД и утечки по техническим каналам связи.

## 9. Объекты защиты, виды защищаемой информации

Объектами защиты информации Оператора являются:

- персональные данные;

- управленческий процесс;

- межведомственное взаимодействие;

- финансово-экономическая информация;

- информационный технологический процесс;

- различного рода носители защищаемой информации, в том числе информационные ресурсы, документы на бумажных и машинных носителях, определенные как защищаемые.

Защищаемая информация делится на следующие виды:

- информация, составляющая коммерческую тайну (научно-техническая, технологическая, производственная, финансово-экономическая или иная информация, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны);

- персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

- иная информация, не относящаяся ни к одному из указанных выше видов, которая определена как защищаемая в соответствии с нормативно-правовыми актами Российской Федерации.

Защищаемая информация определяется «Перечнем информации, содержащей сведения конфиденциального характера» Оператора.

## 10. Меры по обеспечению безопасности персональных данных при их обработке

Оператор при обработке персональных данных принимает все необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении них. Обеспечение безопасности персональных данных достигается, в частности, следующими способами:

- Назначением ответственного за организацию обработки персональных данных.

- Утверждением Директором МБУ МЦФОСМР «Надежда» локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

- Осуществлением внутреннего контроля соответствия обработки персональных данных Федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

- Ознакомлением сотрудников Оператора, непосредственно осуществляющих обработку персональных данных, с требованиями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, локальными актами в отношении обработки персональных данных, и обучением указанных работников.

- Выполнением требований, установленных постановлением Правительства РФ от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" при обработке персональных данных, осуществляемой без использования средств автоматизации.

- Применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

- Учетом машинных носителей персональных данных.

- Выявлением фактов несанкционированного доступа к персональным данным и принятием мер направленных на пресечение аналогичного доступа.

- Восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

- Установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых в информационной системе персональных данных.

## 11. Права субъектов персональных данных

Субъект персональных данных имеет право на получение сведений об обработке его персональных данных, а именно:

- подтверждение факта обработки персональных данных Оператором;

- правовые основания и цели обработки персональных данных;

- цели и применяемые Оператором способы обработки персональных данных;

- сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Администрацией или на основании федерального закона;

- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

- сроки обработки персональных данных, в том числе сроки их хранения;

- порядок осуществления субъектом персональных данных прав, предусмотренных Законом о персональных данных;

- информацию об осуществленной или предполагаемой трансграничной передаче данных;

- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу;

- иные сведения, предусмотренные Законом о персональных данных или другими федеральными законами.

Субъект персональных данных вправе требовать от оператора, который их обрабатывает, уточнения этих персональных данных, их блокирования или уничтожения в случае, если они являются неполными, устаревшими, неточными, незаконно полученными или не могут быть призваны необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами.

Для реализации своих прав и защиты законных интересов субъект персональных данных имеет право обратиться к оператору с жалобой на нарушение данной политики. Оператор рассматривает любые обращения и жалобы со стороны субъектов персональных данных, тщательно расследует факты нарушений и принимает все необходимые меры для их немедленного устранения, наказания виновных лиц и урегулирования спорных и конфликтных ситуаций в досудебном порядке.

Жалобы и заявления по поводу соблюдения требований обработки данных рассматриваются в течение тридцати рабочих дней с момента поступления.

Субъект персональных данных вправе обжаловать действия или бездействие Оператора путем обращения в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

## 12.Персональные данные обрабатываемые Оператором

В рамках исполнения своих полномочий Оператором обрабатываются персональные данные:

- в ходе обращений граждан к Оператору;

- в ходе организации предоставления муниципальных услуг;

- в ходе выполнения иных функций Оператора, направленных на удовлетворения потребностей местного населения.

При этом обрабатываются персональные данные граждан, официальных представителей юридических лиц, индивидуальных предпринимателей, обратившихся к Оператору.

Кроме того, обработка персональных данных у Оператора, осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Оператор выступает в качестве работодателя, в связи с реализацией Оператором своих прав и обязанностей как юридического лица.

Оператор вправе:

- Отстаивать свои интересы в суде.

- Предоставлять персональные данные субъектов государственным, муниципальным и иным уполномоченным органам, и организациям, если это предусмотрено действующим законодательством Российской Федерации.

- Отказывать в предоставлении персональных данных в случаях предусмотренных законодательством Российской Федерации.

- Обрабатывать персональные данные субъекта без его согласия, в случаях предусмотренных законодательством Российской Федерации

## 13. Требования по обеспечению информационной безопасности

Общие требования по обеспечению ИБ формулируются для следующих областей:

- назначение и распределение ролей и доверия к сотрудникам;

- стадия жизненного цикла АС;

- эксплуатация АС;

- защита информационных технологических процессов;

- защита от аварийных сбоев в электроснабжении и телекоммуникационных каналах связи.

Требования по обеспечению ИБ при определении доступа и обеспечении доверия к сотрудникам Оператора:

- Для эффективного выполнения целей Оператора и задач по управлению информационными системами определяются соответствующий доступ сотрудников Оператора. Доступ определяются исходя из задач, функциональных и процедурных требований, и обеспечиваются соответствующими ресурсами, а также персонифицируются с установлением ответственности за их исполнение. Ответственность фиксируется в должностных инструкциях.

- С целью снижения рисков нарушения ИБ не рекомендуется в рамках одной роли совмещать следующие функции:

  - разработки и сопровождения системы или программного обеспечения;

  - разработки и эксплуатации системы или программного обеспечения;

  - сопровождения и эксплуатации системы или программного обеспечения;

  - администратора системы и администратора ИБ системы;

  - выполнения операций в системе и контроля их выполнения.

- Организация и координация действий сотрудников Оператора направленных на исполнение требований ИБ осуществляется Директором МБУ МЦФОСМР «Надежда».

- Сотрудники Оператора, а также лица, принимаемые на работу по срочным трудовым договорам и для прохождения практики (стажировки), подписывают обязательство о неразглашении конфиденциальной информации.

- Компетентность персонала Оператора в области обеспечения ИБ достигается с помощью обучения правилам безопасной (с точки зрения ИБ) работы, изучения соответствующих регламентирующих документов, осведомленности сотрудников об источниках потенциальных угроз и уязвимостях, а также периодических проверок его знаний и навыков.

- Обязанности сотрудников по выполнению требований ИБ включаются в должностные инструкции.

Требования по обеспечению ИБ АС Оператора на стадиях жизненного цикла:

- ИБ АС должна обеспечиваться на всех стадиях жизненного цикла АС, автоматизирующих технологические и управленческие процессы Оператора, с учетом всех сторон, вовлеченных в процессы жизненного цикла АС.

- Ввод в действие и снятие с эксплуатации СКЗИ, средств защиты от НСД АС осуществляется при участии работников ответственных за ИБ.

Требования по обеспечению ИБ при эксплуатации АС:

- Разграничение прав доступа ролей пользователей;

- Соблюдение требований документов по парольной, антивирусной защите и резервному копированию;

- Использование в составе АС только сертифицированных или разрешенных к применению средств защиты информации.

- Соблюдение организационно-технической документации АС;

- Соблюдение требований регламента использования ресурсов глобальной сети Интернет Оператором.

- Соблюдение документов, описывающих порядок применения СКЗИ в технологических процессах Оператора.

Требования по обеспечению ИБ информационных технологических процессов Оператора:

- Система обеспечения ИБ информационного технологического процесса Оператора строится в соответствии с требованиями пункта11настоящей Политики и иных нормативных документов по вопросам ИБ.

- Информационный технологический процесс Оператора определяется в положениях, распоряжениях и других нормативно-методических документах.

- Сотрудники Оператора, в том числе администраторы АС и администраторы ИБ, не должны обладать всей полнотой полномочий для бесконтрольного создания, уничтожения и изменения информации, а также проведения операций по изменению состояния записей в базах данных.

- При работе с информацией должны проводиться контроль целостности данной информации.

- Обязанности по администрированию доступа пользователей к информации, передаваемой по электронным каналам связи, возлагаются на администраторов соответствующих ИС с отражением этих функций в их должностных инструкциях.

- Комплекс мер по обеспечению ИБ технологического процесса Оператора должен предусматривать:

- Защиту информации от искажения, фальсификации, переадресации, несанкционированного доступа и (или) уничтожения;

- Минимально необходимый, гарантированный доступ работника Оператора только к тем ресурсам информационного технологического процесса, которые необходимы ему для исполнения служебных обязанностей или реализации прав, предусмотренных технологией обработки информации;

- Контроль исполнения установленной технологии подготовки, обработки, передачи и хранения информации;

- Восстановление информации в случае ее умышленного или случайного разрушения (искажения) или выхода из строя средств вычислительной техники;

- Гарантированную доставку сообщений администрации информационного обмена.

## 14. Общие требования по обработке персональных данных

Оператором должен быть определен и документально зафиксирован перечень ИСПДн.

Для каждой ИСПДн Оператора должны быть определены и документально зафиксированы:

- цель обработки персональных данных в ИСПДн;

- объем и содержание персональных данных, обрабатываемых в ИСПДн;

- перечень действий с персональными данными и способы обработки персональных данных в ИСПДн.

Объем и содержание персональных данных, а также перечень действий и способы обработки персональных данных должны соответствовать действующему законодательству Российской Федерации.

Информационные технологические процессы, в рамках которых обрабатываются персональные данные в ИСПДн, должны быть документированы.

У Оператора должен быть определен и документально зафиксирован перечень (список) работников, осуществляющих обработку персональных данных в ИСПДн, либо имеющих доступ к персональным данным.

Доступ работников к персональным данным и обработка персональных данных работниками администрации должны осуществляться только для выполнения их должностных обязанностей.

Сотрудники Оператора, осуществляющие обработку персональных данных в ИСПДн, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также должны быть ознакомлены под роспись со всей совокупностью требований по обработке и обеспечению безопасности персональных данных в части касающихся их должностных обязанностей.

У Оператора должен быть определен и документально зафиксирован порядок доступа работников в помещения, в которых ведется обработка персональных данных.

Оператором должен быть определен и документально зафиксирован порядок хранения материальных носителей персональных данных, устанавливающий:

- места хранения материальных носителей персональных данных;

- требования по обеспечению безопасности персональных данных;

- работников, ответственных за реализацию требований по обеспечению безопасности персональных данных;

- порядок контроля выполнения требований по обеспечению безопасности персональных данных.

## 15. Управление информационной безопасностью, функции по обеспечению ИБ

Управление информационной безопасностью Оператора включает в себя:

- актуализацию настоящей политики;

- разработку нормативных и методических документов обеспечения ИБ;

- обеспечение штатного функционирования комплекса средств ИБ Оператора;

- осуществление контроля (мониторинга) функционирования системы ИБ;

- обучение с целью поддержки (повышения) квалификации сотрудников Оператора;

- оценку рисков, связанных с нарушениями ИБ.

Основными функциями по обеспечению ИБ являются:

- разработка технических, организационных и административных планов реализации политики ИБ;

- проведение единой технической политики, организация и координация работ по защите информации;

- участие в согласовании проектов всех внутренних документов, затрагивающих вопросы безопасности технологий, используемых у Оператора;

- подготовка рекомендаций по выбору средств защиты информации;

- администрирование средств защиты информации в части обеспечения работоспособности прикладного программного обеспечения и их обновления;

- участие в обеспечении бесперебойной работы АС и восстановлении её работы после сбоев;

- обучение пользователей безопасной работе с информационными активами;

- контроль соблюдения требований по использованию антивирусных средств;

- участие в расследовании событий, связанных с инцидентами ИБ, и в случае необходимости выход с предложениями по применению санкций в отношении лиц, осуществивших НСД, например, нарушивших требования инструкций и т.п. по обеспечению ИБ Оператора;

- организация аттестации объектов по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности и (или) конфиденциальности;

- организация и проведение работ по контролю эффективности проводимых мероприятий и принимаемых мер по защите информации;