СОГЛАСОВАНО
Председатель ППО
МАУ ДО ДЮЦ СТ
_____Р.Я. Салихова
Протокол № 3 от 18.05.2020г.

УТВЕРЖДАЮ
Директор МАУ ДО ДЮЦ СТ
_____И.С. Ременникова
Приказ № 119 от 19.05.2020г.

ДОКУМЕНТ ПОДПИСАН
УСИЛЕННОЙ КВАЛИФИЦИРОВАННОЙ
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 01D6EE29185805E0000000C900060002
Владелец: Ременникова Инна Сергеевна
Действителен: с 19.01.2021 по 19.01.2022

Политика

в отношении обработки персональных данных Муниципального автономного учреждения дополнительного образования Детско-юношеский центр спорта и туризма городского округа город Нефтекамск Республики Башкортостан

Принято на заседании
общего собрания
трудового коллектива
МАУ ДО ДЮЦ СТ
Протокол № 3
от 18 мая 2020г.

г. Нефтекамск, 2020г.

1. Общие положения.

1.1 Политика Муниципального автономного учреждения дополнительного образования Детско-юношеского центра спорта и туризма городского округа город Нефтекамск (далее -Политика) определяет порядок сбора, хранения, обработки, передачи и любого другого использования персональных данных.

1.2 Политика Учреждения в отношении обработки персональных данных разработана в целях обеспечения реализаций требований законодательства России в области обработки персональных данных, направленного на обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе на неприкосновенность частной жизни, личную и семейную тайну, в частности в целях защиты от несанкционированного доступа и неправомерного распространения персональных данных, обрабатываемых в Учреждении.

1.3 Политика предназначена для работников Учреждения, осуществляющих обработку персональных данных в целях непосредственной реализации ими закрепленных в Политике принципов, а также является информационным ресурсом для субъектов персональных данных, позволяющим определить концептуальные основы деятельности Учреждения при обработке персональных данных.

1.4 Политика разработана в соответствии с частью I статьи 23, статьи 24 Конституции Российской Федерации, главы 14 Трудового Кодекса Российской Федерации «Защита персональных данных работников» от 30.12.2001 за № 197-ФЗ, Федеральным законом от 27.07.2006 за № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом 27.07.2006 за № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 23.03.2012 за № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятых в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
Постановлением Правительства Российской Федерации №1119 от 1 ноября 2012 г. «Об утверждении требований к защите персональных данных при их обработке, а информационных системах персональных данных». Приказом ФСТЭК России №21 от 18 февраля 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.5 Настоящая Политика утверждается и вводится в действие приказом начальника Учреждения и действует в отношении персональных данных, полученных как до, так и после подписания настоящей Политики.

2. Термины и определения

2.1. Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

2.2. Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических

средств.

2.3. Использование персональных данных - действия (операции) с персональными данными, совершаемые Оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

2.4. Конфиденциальность персональных данных - обязательное для соблюдения требование не допускать распространения персональных данных без согласия субъекта персональных данных или наличия иного законного основания. 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.

2.5. Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе.

2.6. Оператор персональных данных (далее - 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.

2.7. Персональные данные - любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных).

2.8. Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределённому кругу лиц.

2.9. Сотрудник (работник) - физическое лицо, состоящее в трудовых отношениях с Оператором.

2.10. Субъект - физическое лицо, обладатель собственных персональных данных.

2.11. Обработка персональных данных.

Обработка персональных данных осуществляется Учреждением с использованием средств автоматизации, а также без использования таких средств (на бумажном носителе информации).

Оператор не предоставляет и не раскрывает сведения, содержащие персональные данные субъектов, третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью, а также в случаях, установленных федеральными законами.

По мотивированному запросу исключительно для выполнения возложенных законодательством функций и полномочий персональные данные субъекта персональных без его согласия могут быть переданы:

- в судебные органы в связи с осуществлением правосудия;
- в органы федеральной службы безопасности;

- в органы прокуратуры;

- в органы полиции;

- в иные органы и организации в случаях, установленных нормативными правовыми актами, обязательными для исполнения.

Сроки хранения носителей персональных данных определены номенклатурой Учреждения. Порядок уничтожения носителей персональных данных установлен Инструкцией по делопроизводству.

2.12. Конфиденциальность персональных данных.

Информация, относящаяся к персональным данным, ставшая известной в связи с реализацией трудовых отношений и в связи с оказанием муниципальных услуг и осуществлением муниципальных функций, является конфиденциальной информацией и охраняется законом.

2.13. Объекты защиты

Основными объектами системы безопасности персональных данных в Учреждении являются:

- информационные ресурсы с ограниченным доступом, содержащие персональные данные;

- процессы обработки персональных данных в информационной системе персональных данных Учреждения, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков и пользователей системы и ее обслуживающий персонал;

- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых расположены технические средства обработки персональных данных.

3. Интересы затрагиваемых субъектов информационных отношений

Субъектами информационных отношений при обеспечении безопасности персональных данных Учреждения являются:

- Учреждение, как собственник информационных ресурсов;

- руководство и сотрудники Учреждения, в соответствии с возложенными на них функциями.

Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

- своевременного доступа к необходимым им персональным данным (их доступности);

- достоверности (полноты, точности, адекватности, целостности) персональных данных;

- конфиденциальности (сохранения в тайне) персональных данных;

- защиты от навязывания им ложных (недостоверных, искаженных) персональных данных;

- разграничения ответственности за нарушения их прав (интересов) и установленных правил обращения с персональными данными;

- возможности осуществления непрерывного контроля и управления процессами обработки и передачи персональных данных;

- защиты персональных данных от незаконного распространения.

Сотрудники Учреждения и иные лица, получившие доступ к обрабатываемым персональным данным, подписали обязательство о неразглашении конфиденциальной информации, а также предупреждены о возможной дисциплинарной, административной, гражданско-правовой и уголовной ответственности в случае нарушения норм и требований действующего законодательства Российской Федерации в области обработки персональных данных.

4. Цели защиты

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита субъектов информационных отношений Учреждения от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на персональные данные, их носители, процессы обработки и передачи.

Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств персональных данных:

- доступности персональных данных для легальных пользователей (устойчивого функционирования информационной системы Учреждения, при котором пользователи имеют возможность получения необходимых персональных данных и результатов решения задач за приемлемое для них время);

- целостности и аутентичности (подтверждение авторства) персональных данных, хранимых и обрабатываемых в информационной системе Учреждения и передаваемой по каналам связи;

- конфиденциальности - сохранения в тайне определенной части персональных данных, хранимых, обрабатываемых и передаваемых по каналам связи.

Необходимый уровень доступности, целостности и конфиденциальности персональных данных обеспечивается соответствующими множеству значимых угроз методами и средствами.

5. Основные задачи системы обеспечения безопасности персональных данных

Для достижения основной цели защиты и обеспечения указанных свойств персональных данных система обеспечения информационной безопасности Учреждения должна обеспечивать эффективное решение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, нарушению нормального функционирования информационной системы Учреждения;

- создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;

- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;

- защиту от вмешательства в процесс функционирования информационной системы Учреждения посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);

разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам Учреждения (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа;

обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);

- защиту от несанкционированной модификации используемых в информационной системе Учреждения программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы:

- защиту информации ограниченного пользования от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

6. Основные пути решения задач системы защиты

Поставленные основные цели защиты и решение перечисленных выше задач достигаются:

- строгим учетом всех подлежащих защите ресурсов информационной системы

Учреждения (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);

- учетом действий персонала, осуществляющего обслуживание и модификацию программных и технических средств информационной системы;

-полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов Учреждения по вопросам обеспечения безопасности информации;

- подготовкой должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности персональных данных и процессов их обработки;

наделением каждого сотрудника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам Учреждения;

- четким знанием и строгим соблюдением всеми пользователями информационной системы Учреждения требований организационно - распорядительных документов по вопросам обеспечения безопасности персональных данных;

- персональной ответственностью за свои действия каждого сотрудника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам Учреждения;

- непрерывным поддержанием необходимого уровня защищенности элементов информационной среды Учреждения;

- применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их

использования;

- эффективным контролем над соблюдением пользователями информационных ресурсов Учреждения требований по обеспечению безопасности информации;

- юридической защитой интересов Учреждения при взаимодействии с внешними организациями (связанном с обменом персональными данными) от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц.

7. Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности персональных данных и системы их обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

8. Минимизация полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью. Доступ к персональным данным должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

9. Исключение конфликта интересов (разделение функций)

Эффективная система обеспечения информационной безопасности предполагает четкое разделение обязанностей сотрудников и исключение ситуаций, когда сфера ответственности сотрудников допускает конфликт интересов. Сферы потенциальных конфликтов должны выявляться, минимизироваться, и находится под строгим независимым контролем.

Реализация данного принципа предполагает, что ни один сотрудник не должен иметь полномочий, позволяющих ему единолично осуществлять выполнение критичных операций. Наделение сотрудников полномочиями, порождающими конфликт интересов, дает ему возможность подтасовывать информацию в корыстных целях или с тем, чтобы скрыть проблемы или понесенные убытки. Для снижения риска манипулирования персональными данными и риска хищения, такие полномочия должны в максимально возможной степени быть разделены между различными сотрудниками или подразделениями Учреждения. Необходимо проводить периодические проверки обязанностей, функций и деятельности сотрудников, выполняющих ключевые функции, с тем, чтобы они не имели возможности скрывать совершение неправомерных действий. Кроме того, необходимо принимать специальные меры по недопущению сговора между сотрудниками.

10. Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективе Учреждения. В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие деятельности администратора безопасности информационной системы персональных данных.

Важным элементом эффективной системы обеспечения безопасности

персональных данных в Учреждении является высокая культура работы с информацией. Руководство Учреждения несет ответственность за строгое соблюдение этических норм и стандартов профессиональной деятельности, подчеркивающей и демонстрирующей персоналу на всех уровнях важность обеспечения информационной безопасности Учреждения. Все сотрудники должны понимать свою роль в процессе обеспечения информационной безопасности и принимать участие в этом процессе. Несмотря на то, что высокая культура обеспечения информационной безопасности не гарантирует автоматического достижения целей, ее отсутствие создает больше возможностей для нарушения безопасности или не обнаружения фактов ее нарушения.

11. Меры, методы и средства обеспечения требуемого уровня защиты информационных ресурсов

11.1. Меры обеспечения информационной безопасности

Все меры обеспечения безопасности информационной системы Учреждения подразделяются на:

- правовые (законодательные);
- морально-этические;
- технологические;
- организационные (административные);
- физические;
- технические (аппаратурные и программные).

11.2. Законодательные (правовые) меры защиты

К правовым мерам защиты относятся действующие в Российской Федерации законы, указы и нормативные акты, регламентирующие правила обращения с персональными данными, закрепляющие права и обязанности участников информационных отношений в процессе их обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационной системы Учреждения.

11.3. Морально-этические меры защиты

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение может привести к падению авторитета, престижа человека, группы лиц или администрации в целом. Морально- этические нормы бывают как неписаные, так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний. Морально- этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективе.

11.4. Технологические меры защиты

К данному виду мер защиты относятся разного рода технологические решения и приемы, основанные на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий.

11.5. Организационные (административные) меры защиты

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования системы обработки персональных данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

11.6. В Учреждении:

1) утверждены Положение об обработке персональных данных, другие локальные акты, устанавливающее процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований;

2) применяются предусмотренные соответствующими нормативными правовыми актами правовые, организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;

3) при обработке персональных данных, осуществляемой без использования средств автоматизации, выполняются требования, установленные постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

12. Формирование политики безопасности

Главная цель административных мер, предпринимаемых на высшем управленческом уровне - сформировать политику в области обеспечения безопасности персональных данных (отражающую подходы к защите персональных данных) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

С практической точки зрения политику в области обеспечения безопасности персональных данных в Учреждение целесообразно разбить на два уровня. К верхнему уровню относятся решения руководства, затрагивающие деятельность Учреждения в целом. Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности персональных данных, определить какими ресурсами (материальные, структурные, организационные) они будут достигнуты, и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью.

Политика нижнего уровня, определяет процедуры, и правила достижения целей и решения задач безопасности персональных данных и детализирует (регламентирует) эти правила:

- каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности персональных данных;
- кто имеет права доступа к персональным данным, кто и при каких условий может читать и модифицировать персональные данные и т.д.

Политика нижнего уровня должна:

- предусматривать регламент информационных отношений, заключающих возможность произвольных, монопольных или несанкционированных действий в отношении информационных ресурсов;
- определять коалиционные и иерархические принципы и методы разделения информации и разграничения доступа к персональным данным;
- выбирать программно-технические (аппаратные) средства противодействия НСД, аутентификации, авторизации, идентификации и других защитных механизмов, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

13. Категории обрабатываемых персональных данных и цели обработки.

В Учреждении обрабатываются следующие категории персональных данных:

Цель обработки: регистрация и учет обучающихся, воспитанников и их родителей (законных представителей), сотрудников; лиц, с которыми заключены договора.

Фамилия, имя, отчество;	паспортные данные;
год, месяц, дата рождения	адрес, телефон;
данные о социальном номере (ИНН)	стаж;
документы воинского учета;	семейное, социальное, имущественное положение;
образование;	место рождения
сведения о судимости.	профессия;
сведения о трудовом и общем стаже;	состояние здоровья:
доходы, полученные мной в данном учреждении;	доходы;
СНИЛС;	квалификация;

14. Сроки обработки персональных данных

Сроки обработки указанных выше персональных данных определяются в соответствии со сроком действия договора с субъектом персональных данных, приказом Министерства культуры РФ от 25 августа 2010 года № 558 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения».

15. Обязанности Оператора и субъектов персональных данных

Сотрудники Учреждения обязаны:

- использовать персональные данные только в соответствии с целями обработки, определившими их получение;
- в порядке, установленном законодательством России, обеспечить защиту персональных данных субъекта от неправомерного их использования или утраты;
- осуществлять передачу персональных данных субъекта только в соответствии с законодательством Российской Федерации;
- по требованию субъекта или его законного представителя предоставить ему полную информацию о его персональных данных и порядке обработки данных

Субъект персональных данных или его законный представитель обязуется

предоставлять персональные данные, соответствующие действительности.

16. Права Оператора и субъектов персональных данных

Оператор имеет право:

- ограничить доступ субъекта к его персональным данным в соответствии с федеральными законами;
- требовать от субъекта предоставления достоверных персональных данных;
- передавать персональные данные субъекта без его согласия, если это предусмотрено федеральными законами.

Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных Оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые Оператором способы обработки персональных данных;
- наименование и место нахождения Оператора, сведения о лицах (за исключением сотрудников/работников Оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Оператором 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 Федеральным законом «О персональных данных»;
- информацию об осуществленной или о 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 Федеральным законом «О персональных данных» или другими федеральными законами.

17. Принципы обработки персональных данных

Обработка персональных данных в Учреждении осуществляется на основе следующих принципов:

- обработка ограничивается достижением конкретных, заранее определённых и законных целей;
- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- хранение персональных данных осуществляется не дольше, чем этого требуют цели их обработки;
- недопустимости объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

Субъект персональных данных вправе требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно

полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Оператора в вышестоящий орган по защите прав субъектов персональных данных (Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций - Роскомнадзор) 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.

18. Безопасность персональных данных

Учреждение предпринимает необходимые правовые, организационные и технические меры для обеспечения безопасности персональных данных от случайного или несанкционированного доступа, уничтожения, изменения, блокирования доступа и других несанкционированных действий.

К мерам обеспечения безопасности относятся:

- утверждение приказом директора Учреждения перечня должностей работников, деятельность которых предусматривает обработку персональных данных;
- утверждение приказом директора Учреждения списка обрабатываемых персональных данных;
- регламентация процессов сбора, хранения, накопления, уточнения, систематизации, обезличивания, блокирования и уничтожения персональных данных;
- регламентация процессов резервного копирования и восстановления информации;
- повышение квалификации сотрудников в области зашиты персональных данных;
- установка сертифицированных средств защиты информации от несанкционированного доступа, межсетевого экранирования и антивирусных средств;
- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных;
- периодический контроль выполнения установленных мер по защите персональных данных:
- актуализация нормативных документов, принятых в Учреждении, при внесении изменений в законодательные акты России.

Приказом директора Учреждения назначено лицо, ответственное за организацию обработки персональных данных.

19. Контроль состояния и эффективности защиты ИСПДн

В ИСПДн должен осуществляться контроль и (или) аудит соответствия обработки ПДн действующим в России законодательству и требованиям к защите ПДн, а так же настоящей Политике и локальным актам Учреждения.

Контроль заключается в оценке выполнения требований нормативных документов, обоснованности принятых мер и оценке эффективности принятых мер по обеспечению ПДн.

Контроль подразделяется на оперативный и плановый (периодический).

В процессе эксплуатации ИСПДн в целях защиты информации от НСД осуществляются оперативный контроль и периодический контроль за выполнениемисполнителями требований действующих нормативных документов по вопросам обеспечения безопасности и защиты ПДн.

С целью своевременного выявленияи предотвращения утечки информации, исключения или существенного затруднения НСД и предотвращения специальных воздействий (программно-технических и др.), вызывающих нарушение целостности информации или работоспособность технических средств, в ИСПДн Учреждения проводится плановый периодический (не реже одного раза в год) контроль состояния защиты информации.

При проведении плановых проверок осуществляется контроль ведения учетной документации, защищенности ИСПДн от утечки ПДн по техническим каналам, выборочный контроль содержимого накопителей и носителей информации, и т.п.

Результаты контроля оформляются актами и заключениями.

20. Заключительные положения

Настоящая Политика является общедоступной и подлежит размещению на официальном сайте (или опубликованию в общедоступных источниках).

Пронумеровано, прошнуровано,
скреплено печатью 13
(тринадцать) листов
Директор МАУ ДО ДЮЦ СТ
/И.С. Ременникова/