УПРАВЛЕНИЕ ОБРАЗОВАНИЯ И МОЛОДЕЖНОЙ ПОЛИТИКИ
АДМИНИСТРАЦИИ РЫБНОВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА РЯЗАНСКОЙ ОБЛАСТИ

Муниципальное бюджетное учреждение дополнительного образования
«Рыбновский районный

Детско-юношеский Центр туризма»

391110, Рязанская область,
г. Рыбное, Набережный
пер., д.2

тел. (49137) 52-2-60,

ПРИКАЗ

«19» марта 2021 г. № 13

Об утверждении политики в
отношении обработки персональных данных

Во исполнение требований Федерального закона №152-ФЗ от 27 июля 2006г. «О персональных данных», а также прочих нормативных документов по защите информации,

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемую Политику в отношении обработки персональных данных МБУ ДО РР ДЮЦТ (далее – Политика) (Приложение к настоящему приказу).
2. Ответственному за организацию обработки персональных данных в срок не позднее десяти рабочих дней от даты подписания настоящего приказа опубликовать Политику на официальном сайте МБУ ДО РР ДЮЦТ
3. Контроль за исполнением настоящего приказа оставляю за собой.

Директор С.В.Новиков

Приложение
к приказу МБУ ДО РР ДЮЦТ
от «19» марта 2021 г. № 13

ПОЛИТИКА

в отношении обработки персональных данных

1. Общие положения

1.1. Настоящая Политика в отношении обработки персональных данных (далее – Политика) МБУ ДО РР ДЮЦТ юридический адрес: 391110, Рязанская область, г.Рыбное, ул. Набережный переулок, д.2 (далее – Оператор) является официальным документом, в котором определены общие принципы, цели и порядок обработки персональных данных пользователей интернет-сайта (https://p62.навигатор.дети) (далее – Сайт), а также сведения о реализуемых мерах защиты персональных данных.

1.2. Политика разработана в соответствии с законодательством Российской Федерации в области персональных данных.

1.3. Настоящая Политика применяется исключительно к Сайту. Оператор не контролирует и не несет ответственность за сайты третьих лиц, на которые Пользователь может перейти по ссылкам, доступным на Сайте.

1.4. Обработка Оператором персональных данных других категорий субъектов персональных данных регламентирована другими локальными актами Оператора.

1.5. Настоящая Политика вступает в силу с момента ее утверждения и действует бессрочно, до замены ее новой Политикой.

2. Основные термины и определения

2.1. В настоящей Политике используются следующие термины:

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

2.1.2. 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.

2.1.3. Оператор персональных данных (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.

2.1.4. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);

2.1.5. Пользователь сайта – любое лицо, посещающее сайт и использующее информацию, материалы и сервисы сайта.

2.1.6. Сайт – совокупность связанных между собой веб-страниц, размещённых в сети Интернет по уникальному адресу (URL), а также его субдоменах.

2.1.7. Cookies – небольшой фрагмент данных, отправленный веб-сервером и хранимый на компьютере Пользователя, который веб-клиент или веб-браузер каждый раз пересылает веб-серверу в HTTP-запросе при попытке открыть страницу соответствующего сайта.

2.1.8. IP-адрес – уникальный сетевой адрес узла в компьютерной сети, через который Пользователь получает доступ на сайт.

3. Порядок и условия обработки персональных данных

3.1. Основанием обработки персональных данных пользователей Сайта является согласие на обработку персональных данных. Пользователи Сайта дают свое согласие на обработку своих персональных данных в следующих случаях:

- при регистрации на Сайте в личном кабинете;
- при авторизации через социальные сети;
- при заполнении формы обратной связи / заказе обратного звонка на Сайте;
- при оформлении подписки на рассылку;
- при отправке отзывов;

3.2. В случае несогласия Пользователя с условиями настоящей Политики использование Сайта и/или каких-либо Сервисов доступных при использовании Сайта должно быть немедленно прекращено.

3.3. Персональные данные Пользователей Сайта обрабатываются в следующих целях:

- продвижения товаров, работ, услуг;
- установления с Пользователем Сайта обратной связи, включая направление уведомлений, запросов и их обработки, а также обработки запросов и заявок от Пользователя в целях дальнейшего заключения и исполнения договора;
- оказания услуг по технической поддержке Пользователей;
- получение и публикация отзывов;
- ведения статистики и анализа работы Сайта.

3.4. Перечень персональных данных пользователей, обрабатываемые на Сайте с использованием средств автоматизации:

- фамилия, имя, отчество;
- дата рождения;
- номер телефона;
- адрес электронной почты;
- адрес доставки;
- иная информация, которую пользователь решил предоставить.

3.5. Для ведения статистики и анализа работы Сайта Оператор обрабатывает с использованием метрических сервисов Google Analytics и Яндекс Метрика такие данные, как:

- IP-адрес;
- информация о браузере;

– данные из файлов cookie;
– время доступа;
– реферер (адрес предыдущей страницы).

3.6. В случае отказа от обработки файлов cookie Пользователю необходимо прекратить использование Сайта или отключить использование файлов cookie в настройках браузера, при этом некоторые функции Сайта могут стать недоступны.

3.7. Обработка биометрических персональных данных и специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, на Сайте не осуществляется.

3.8. Оператор не проверяет достоверность информации предоставляемой Пользователем и исходит из того, что Пользователь предоставляет достоверную и достаточную информацию, контролирует ее актуальность.

3.9. Оператор осуществляет следующие действия с персональными данными: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), блокирование, удаление, уничтожение.

3.10. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных не дольше, чем этого требуют цели обработки персональных данных.

3.11. Условием прекращения обработки персональных данных может являться достижение целей обработки персональных данных, истечение срока обработки персональных данных, отзыв согласия пользователя Сайта на обработку его персональных данных, а также выявление неправомерной обработки персональных данных.

3.12. Срок хранения персональных данных пользователей Сайта составляет 1 год с момента последней отправки данных.

4. Меры обеспечения безопасности персональных данных

4.1. Безопасность персональных данных, обрабатываемых Оператором, обеспечивается реализацией правовых, организационных, технических и программных мер, необходимых и достаточных для обеспечения требований законодательства Российской Федерации.

4.2. Оператором предпринимаются следующие меры для обеспечения безопасности персональных данных:

– назначение ответственных лиц за организацию обработки и обеспечение защиты персональных данных;
– ограничение состава работников Оператора, имеющих доступ к персональным данным;
– определение уровня защищенности персональных данных при обработке в информационных системах персональных данных;
– определение актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
– установление правил разграничения доступа к персональным данным, обрабатываемым в информационных системах персональных данных и

обеспечение регистрации и учета всех действий, совершаемых с персональными данными;

- ограничение доступа в помещения, где размещены основные технические средства и системы информационных систем персональных данных и осуществляется неавтоматизированная обработка персональных данных;
- ведение учета машинных носителей персональных данных;
- организация резервирования и восстановления работоспособности информационных систем персональных данных и персональных данных модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установление требований к сложности паролей для доступа к информационным системам персональных данных;
- применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации;
- осуществление антивирусного контроля, предотвращение внедрения в корпоративную сеть вредоносных программ (программ-вирусов) и программных закладок;
- организация своевременного обновления программного обеспечения, используемого в информационных системах персональных данных и средств защиты информации;
- проведение регулярной оценки эффективности принимаемых мер по обеспечению безопасности персональных данных;
- обнаружение фактов несанкционированного доступа к персональным данным и принятие мер по установлению причин и устранению возможных последствий;
- проведение аттестационных испытаний информационных систем персональных данных;
- контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровней защищенности информационных систем персональных данных.

5. Права пользователей сайта

5.1. Пользователь Сайта 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 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 персональных 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.

5.2. Пользователь Сайта 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.

5.3. Пользователь Сайта вправе запросить в структурированном, универсальном и машиночитаемом формате перечень своих персональных данных, предоставленных Оператору для обработки, и поручить Оператору передать свои персональные третьему лицу при наличии соответствующей технической возможности. В данном случае Оператор не несет ответственности за действия третьего лица, совершенные в дальнейшем с персональными данными.

5.4. Все вопросы касательно обработки персональных следует сообщать по адресу: 391110, Рязанская область, г.Рыбное, ул. Набережный переулок, д.2.

6. Ответственность

6.1. Пользователь несет полную ответственность за соблюдение требований действующего законодательства Российской Федерации, в том числе законов о рекламе, о защите авторских и смежных прав, об охране товарных знаков и знаков обслуживания, но не ограничиваясь перечисленным, включая полную ответственность за содержание и форму материалов, в случае цитирования и иного использования информации, полученной в связи с использованием сервисов Сайта.

7. Заключительные положения

7.1. Оператор имеет право вносить изменения в настоящую Политику в одностороннем порядке в случае изменения нормативных правовых актов Российской Федерации, а также по своему усмотрению.

7.2. Контроль исполнения требований настоящей Политики осуществляется ответственным за организацию обработки персональных данных.

7.3. Лица, виновные в нарушении норм, регулирующих обработку и защиту персональных, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, законодательством Российской Федерации.

УПРАВЛЕНИЕ ОБРАЗОВАНИЯ И МОЛОДЕЖНОЙ ПОЛИТИКИ
АДМИНИСТРАЦИИ РЫБНОВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА РЯЗАНСКОЙ ОБЛАСТИ
Муниципальное бюджетное учреждение дополнительного образования
«Рыбновский районный
Детско-юношеский Центр туризма»

391110, Рязанская область,
г. Рыбное, Набережный
пер., д.2

тел. (49137) 52-2-60,

ПРИКАЗ

«19» марта 2021 г. № 14

О создании комиссии по защите персональных данных

В целях защиты персональных данных, обрабатываемых в МБУ ДО РР ДЮЦТ, ПРИКАЗЫВАЮ:

1. Создать комиссию для организации работ по защите персональных данных, обрабатываемых в МБУ ДО РР ДЮЦТ в составе:
Председатель комиссии: директора Новикова С.В.

Члены комиссии:

- Педагог-организатор А.С.Новиков.

2. Комиссии при работе руководствоваться следующими нормативными документами:
- Федеральным законом от 27 июля 2006г. №152-ФЗ «О персональных данных»;
- Постановлением Правительства Российской Федерации от 1 ноября 2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказом ФСТЭК России от 18 февраля 2013г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Постановлением Правительства Российской Федерации от 15 сентября 2008г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- Порядком обращения со съемными машинными носителями персональных данных в МБУ ДО РР ДЮЦТ;
- Регламентом проведения внутреннего контроля соответствия обработки персональных данных в МБУ ДО РР ДЮЦТ требованиям к защите персональных данных;
- Регламентом реагирования на инциденты информационной безопасности в информационных системах персональных данных МБУ ДО РР ДЮЦТ.

3. Комиссии необходимо:
   - определить уровень защищенности персональных данных, обрабатываемых в информационных системах в соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
   - провести оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства Российской Федерации в области персональных данных;
   - отбирать и уничтожать материальные носители персональных данных, обработка которых в МБУ ДО РР ДЮЦТ прекращена;
   - проводить внутренний контроль соответствия обработки персональных данных в соответствии с планом, утвержденном в «Регламенте проведения внутреннего контроля соответствия обработки персональных данных в МБУ ДО РР ДЮЦТ требованиям к защите персональных данных»;
   - проводить разбирательства по фактам возникновения инцидентов информационной безопасности, фиксировать их в журнале учета нештатных ситуаций и своевременно реагировать на инциденты информационной безопасности в информационных системах персональных данных.
4. Требования настоящего Приказа довести до председателя и членов назначенной комиссии.
5. Утвердить формы актов оценки потенциального вреда субъектам персональных данных (приложение 1) и уровня защищенности персональных данных (приложение 2).
6. Контроль за исполнением настоящего Приказа оставляю за собой.

Директор С.В.Новиков

Приложение 1

к приказу МБУ ДО РР ДЮЦТ
от «19» марта 2021 г. № 14

УТВЕРЖДАЮ

Директор МБУ ДО РР ДЮЦТ

_____ С.В.Новиков

«___» _____ 20__г.

АКТ

«___» _____ 20__ г. № _____

Рязань

Оценки потенциального вреда
субъектам персональных данных

Комиссия в составе:

Председатель:

Директор	С.В.Новиков
(должность)	(ФИО)

Члены комиссии:

1. Педагог-организатор — А.С.Новиков
   (должность) — (ФИО)
2. _____ — _____
   (должность) — (ФИО)
3. _____ — _____
   (должность) — (ФИО)

в соответствии с п.5 ч.1 ст.18.1 Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»), произвела экспертную оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения ОГБУДО «ДЭБЦ» обязанностей, предусмотренных ФЗ «О персональных данных».

Размер вреда, который может быть причинен субъектам персональных данных в случае нарушения ФЗ «О персональных данных», определяется в соответствии со статьями 15, 151, 152, 1101 Гражданского кодекса Российской Федерации.

Комиссия, проанализировав перечень персональных данных, обрабатываемых в МБУ ДО РР ДЮЦТ и состав реализованных организационных и технических мер по защите персональных данных, пришла к выводу, что в результате нарушения одного из свойств безопасности персональных данных (конфиденциальности, целостности, доступности), возможны незначительные негативные последствия в социальной, финансовой или иных областях деятельности субъекта персональных данных, а МБУ ДО РР ДЮЦТ, как оператор персональных данных, может выполнять возложенные на него функции с незначительным снижением эффективности.

Исходя из полученных данных, комиссия установила, что уровень потенциального вреда, который может быть причинен субъекту персональных данных в случае нарушения одного из свойств безопасности персональных данных, оценивается как – **низкий**.

Председатель комиссии:

Директор		С.В.Новиков
(должность)	(подпись)	(ФИО)

Члены комиссии:

1. Педагог-организатор		А.С.Новиков
(должность)	(подпись)	(ФИО)
2.		
(должность)	(подпись)	(ФИО)
3.		
(должность)	(подпись)	(ФИО)

Приложение 2

к приказу МБУ ДО РР ДЮЦТ
от «19» марта 2021 г. № 14

УТВЕРЖДАЮ

Директор МБУ ДО РР ДЮЦТ

_____ С.В.Новиков

«___» _____ 20__ г.

АКТ

«___» _____ 20__ г. № _____

Рязань

Определения уровня защищенности

персональных данных, при их обработке в

ИС «Региональный навигатор дополнительного образования детей в Рязанской области»

Комиссия в составе:

Председатель:

Директор	С.В.Новиков
(должность)	(ФИО)

Члены комиссии:

1.	Педагог-организатор	А.С.Новиков
	(должность)	(ФИО)
2.		
	(должность)	(ФИО)
3.		
	(должность)	(ФИО)

на основании исходных данных об информационной системе персональных данных «» (далее – ИСПДн) определила:

1. В ИСПДн обрабатываются **ИНЫЕ** категории персональных данных не сотрудников МБУ ДО РР ДЮЦТ, менее 100 000 субъектов ПДн;

2. Системное и прикладное программное обеспечение, используемое в ИСПДн, регулярно обновляется и поддерживается производителями и с учетом характера обрабатываемых данных, для ИСПДн нет объективных предпосылок для проведения работ по внедрению недокументированных (недекларированных) возможностей в программные компоненты ИСПДн.

3. С учетом п. 2 для ИСПДн признаются актуальными угрозы 3 типа, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИСПДн.

В соответствии с постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», установила необходимость обеспечения **4 уровня защищенности** персональных данных при обработке в ИСПДн.

Председатель комиссии:

Директор		С.В.Новиков
(должность)	(подпись)	(ФИО)

Члены комиссии:

1. Педагог-организатор		А.С.Новиков
(должность)	(подпись)	(ФИО)
(должность)	(подпись)	(ФИО)
3.		
(должность)	(подпись)	(ФИО)

УПРАВЛЕНИЕ ОБРАЗОВАНИЯ И МОЛОДЕЖНОЙ ПОЛИТИКИ
АДМИНИСТРАЦИИ РЫБНОВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА РЯЗАНСКОЙ ОБЛАСТИ
Муниципальное бюджетное учреждение дополнительного образования
«Рыбновский районный
Детско-юношеский Центр туризма»

391110, Рязанская область,
г. Рыбное, Набережный
пер., д.2

тел. (49137) 52-2-60,

ПРИКАЗ

«19» марта 2021 г. № 15

О назначении ответственных по защите персональных данных

Во исполнение требований Федерального закона №152-ФЗ от 27 июля 2006г. «О персональных данных», приказа ФСТЭК России №21 от 18 февраля 2013г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и прочих нормативных документов по защите информации,

ПРИКАЗЫВАЮ:

1. Назначить Ответственным за организацию обработки персональных данных директора Новикова С.В.
2. Назначить Ответственным за обеспечение безопасности персональных данных в информационных системах персональных данных, а также Администратором информационных систем персональных данных педагога-организатора Новикова А.С.
3. На время временного отсутствия (болезнь, отпуск и т.д.) ответственных лиц, указанных в п. 1–3 настоящего Приказа, ответственность за организацию обработки персональных данных, осуществление организационных и технических мероприятий по защите персональных данных и осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону №152-ФЗ от 27 июля 2006 г. и принятыми в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, и иным локальным

нормативным актам, возложить на лиц, исполняющих их обязанности, назначенных и допущенных в установленном порядке.

4. Утвердить и ввести в действие Инструкцию ответственного за организацию обработки персональных данных в МБУ ДО РР ДЮЦТ (Приложение 1 к настоящему Приказу).

5. Утвердить и ввести в действие Инструкцию ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных МБУ ДО РР ДЮЦТ (Приложение 2 к настоящему Приказу).

6. Утвердить и ввести в действие Инструкцию администратора информационных систем персональных данных МБУ ДО РР ДЮЦТ (Приложение 3 к настоящему Приказу).

7. Требования настоящего Приказа довести до назначенных ответственных лиц.

8. Контроль за исполнением настоящего Приказа оставляю за собой.

Директор С.В.Новиков

Приложение 1

к приказу МБУ ДО РР ДЮЦТ

от «19» марта 2021 г. № 15

ИНСТРУКЦИЯ

ответственного за организацию обработки персональных данных

в МБУ ДО РР ДЮЦТ

1. Термины и определения

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

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

Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

2.1. Настоящая Инструкция определяет функции, права и ответственность ответственного за организацию обработки персональных данных (далее – Ответственный) в МБУ ДО РР ДЮЦТ (далее – Учреждение).

2.2. Настоящая Инструкция разработана в соответствии с нормативными правовыми актами Российской Федерации в области защиты персональных данных (далее – ПДн), методическими и руководящими документами уполномоченных федеральных органов исполнительной власти.

2.3. Ответственный назначается приказом директора Учреждения.

2.4. Ответственный непосредственно подчиняется директору Учреждения.

2.5. На время временного отсутствия (болезнь, отпуск, пр.) Ответственного, его обязанности возлагаются на работника, назначенного и допущенного к обработке ПДн в установленном порядке.

2.6. Ответственный в своей работе руководствуется настоящей Инструкцией.

2.7. Настоящая Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности информации, и не исключает обязательного выполнения их требований.

3. Функции

3.1. Ответственный выполняет следующие функции:

- осуществляет внутренний контроль за соблюдением работниками, обрабатывающих ПДн, требований законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн;
- актуализирует перечень должностей работников, имеющих доступ к обработке ПДн;

- актуализирует перечень работников, допущенных в помещения, в которых осуществляется обработка ПДн;
- доводит до сведения работников, обрабатывающих ПДн положения законодательства Российской Федерации о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн, в том числе требований к защите ПДн;
- организовывает прием и обработку обращений и запросов субъектов ПДн, чьи ПДн обрабатываются в Учреждении, или их представителей, и осуществляет контроль за приемом и обработкой таких обращений и запросов;
- разрабатывает и корректирует эксплуатационную документацию и организационно-распорядительные документы по защите ПДн.
- принимает участие в деятельности:
  - по подготовке, пересмотру, уточнению локальных актов по защите информации;
  - по аттестации объектов информатизации.

4. Права

4.1. Ответственный имеет право:

- требовать от работников, обрабатывающих ПДн, соблюдения установленной технологии обработки ПДн и выполнения локальных нормативных актов (внутренних документов) по обеспечению безопасности ПДн;
- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, уничтожения ПДн и технических средств, обрабатывающих ПДн;
- требовать прекращения обработки ПДн в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;
- участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа;
- подавать свои предложения по, совершенствованию организационных и технических мер по защите ПДн.

5. Ответственность

5.1. На Ответственного возлагается персональная ответственность за качество выполняемых им функций.

5.2. Ответственный несет ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации. За несоблюдение требований законодательства Российской Федерации о ПДн предусмотрена гражданская, уголовная, административная, дисциплинарная ответственность.

5.3. Ответственный несет ответственность по действующему законодательству Российской Федерации за разглашение информации ограниченного доступа, ставшей ему известной при выполнении служебных обязанностей, в том числе предусмотренных настоящей Инструкцией.

6. Срок действия и порядок внесения изменений

6.1. Настоящая Инструкция вступает в силу с момента её утверждения и действует бессрочно.

6.2. Настоящая Инструкция подлежит пересмотру не реже одного раза в три года.

6.3. Изменения и дополнения в настоящую Инструкцию вносятся приказом директора Учреждения.

Приложение 2

к приказу МБУ ДО РР ДЮЦТ

от «19» марта 2021 г. № 15

ИНСТРУКЦИЯ

ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных

МБУ ДО РР ДЮЦТ

1. Термины и определения

Доступность информации – свойство безопасности информации, при котором субъекты доступа, имеющие право доступа к информации в соответствии с локальными актами и законодательством Российской Федерации, могут беспрепятственно реализовывать данное право;

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

Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность. Инцидентами информационной безопасности являются:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по информационной безопасности;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

Конфиденциальность информации – свойство безопасности информации, при котором доступ к информации осуществляют только те субъекты доступа, которые имеют на это право в соответствии с локальными актами и законодательством Российской Федерации;

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;

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

Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации;

Целостность информации – свойство безопасности информации, при котором изменение информации осуществляют только те субъекты доступа, которые имеют на это право в соответствии с локальными актами и законодательством Российской Федерации.

2. Общие положения

2.1. Настоящая Инструкция определяет функциональные обязанности, ответственность и права ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных (далее – Ответственный) ОГБУДО «ДЭБЦ» (далее – Учреждение).

2.2. Настоящая Инструкция разработана в соответствии с нормативными правовыми актами Российской Федерации в области защиты персональных данных (далее – ПДн), методическими и руководящими документами уполномоченных федеральных органов исполнительной власти.

2.3. Ответственный назначается приказом директора Учреждения.

2.4. На время временного отсутствия (болезнь, отпуск, пр.) Ответственного его обязанности по осуществлению организационных и технических мероприятий по защите ПДн в информационных системах персональных данных (далее – ИСПДн) Учреждения, возлагаются на работника, назначенного и допущенного к обработке ПДн в установленном порядке.

2.5. Ответственный в своей работе руководствуется настоящей Инструкцией.

2.6. Настоящая Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности информации и не исключает обязательного выполнения их требований.

3. Функциональные обязанности

3.1. Ответственный выполняет следующие функции:

3.1.1. Управляет доступом пользователей в ИСПДн;

3.1.2. Управляет полномочиями пользователей в ИСПДн;

3.1.3. Поддерживает установленные правила разграничения доступа в ИСПДн;

3.1.4. Управляет (администрирует) системой защиты информации (далее – СиЗИ) ИСПДн:

- управляет средствами защиты информации (далее – СЗИ)
- управляет параметрами настройки программного обеспечения СЗИ;
- восстанавливает работоспособность СЗИ;
- устанавливает обновления программного обеспечения СЗИ, выпускаемые разработчиками (производителями) СЗИ;
- анализирует события в ИСПДн, связанные с защитой информации (события безопасности);
- информирует пользователей об угрозах безопасности информации;
- информирует пользователей о правилах эксплуатации СЗИ;
- обучает пользователей работе со СЗИ;
- управляет доступом к съемным машинным носителям информации, используемым в ИСПДн (определяет должностных лиц, имеющих доступ к съемным машинным носителям информации);
- сопровождает функционирование СиЗИ в ходе ее эксплуатации;

- поддерживает конфигурацию СиЗИ (структуру СиЗИ, состав, места установки и параметры настройки СЗИ, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на СиЗИ (поддержание базовой конфигурации СиЗИ);
- определяет лиц, которым разрешены действия по внесению изменений в базовую конфигурацию СиЗИ;
- управляет изменениями конфигурации СиЗИ, в том числе:
  - определяет типы возможных изменений;
  - разрешает или отказывает во внесении изменений;
  - документирует действия по внесению изменений;
  - хранит данные об изменениях.

3.1.5. Поддерживает конфигурацию ИСПДн (структуру ИСПДн, состава, мест установки и параметров программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на ИСПДн;

3.1.6. Анализирует потенциальные воздействия планируемых изменений в базовой конфигурации СиЗИ на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность ИСПДн;

3.1.7. Определяет параметры настройки программного обеспечения, включая программное обеспечение СЗИ, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию ИСПДн и СиЗИ;

3.1.8. Выявляет инциденты (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования ИСПДн и (или) к возникновению угроз безопасности информации (далее– Инциденты), и реагирует на них.

3.1.9. Обнаруживает и идентифицирует Инциденты, в том числе:

- отказы в обслуживании;
- сбои (перезагрузки) в работе средств защиты информации;
- нарушения правил разграничения доступа;
- неправомерные действия по сбору информации;
- иные события, приводящие к возникновению Инцидентов.

3.1.10. Анализирует Инциденты, в том числе определяет источники и причины возникновения Инцидентов, а также оценивает их последствия;

3.1.11. Планирует меры по устранению Инцидентов, в том числе:

- по восстановлению ИСПДн и ее сегментов в случае отказа в обслуживании или после сбоев;
- устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению Инцидентов.

3.1.12. Планирует и принимает меры по предотвращению повторного возникновения Инцидентов.

3.1.13. Контролирует обеспечение уровня защищенности ПДн, обрабатываемых в ИСПДн:

- контролирует события безопасности и действия пользователей в ИСПДн;
- контролирует (анализирует) уровень защищенности ПДн;

- контролирует перемещение съемных машинных носителей информации за пределы контролируемой зоны лицами, которым оно необходимо для выполнения своих должностных обязанностей (функции);
- анализирует и оценивает функционирование СиЗИ ИСПДн, включая выявление, анализ и устранение недостатков в функционировании СиЗИ ИСПДн;
- выполняет периодический анализ изменения угроз безопасности ПДн в ИСПДн, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности ПДн;
- документирует процедуры и результаты контроля (мониторинга) за обеспечением уровня защищенности ПДн, обрабатываемых в ИСПДн;
- принимает решения по результатам контроля (мониторинга) за обеспечением уровня защищенности ПДн о доработке (модернизации) СиЗИ ИСПДн.

3.1.14. Ведет учет:

- используемых шифровальных (криптографических) СЗИ в ИСПДн, эксплуатационной и технической документации к ним;
- съемных машинных носителей (при их наличии).

3.1.15. Обеспечивает защиту информации при выводе из эксплуатации ИСПДн или после принятия решения об окончании обработки информации:

- обеспечивает архивирование информации, содержащейся в ИСПДн (архивирование должно осуществляться при необходимости дальнейшего использования информации);
- обеспечивает уничтожение (стирание) информации и остаточной информации с машинных носителей информации, при необходимости передачи машинного носителя информации в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения;
- при выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка ПДн, осуществляет физическое уничтожение этих съемных машинных носителей информации.

4. Права

4.1. Ответственный имеет право:

- требовать от работников – пользователей ИСПДн соблюдения установленной технологии обработки ПДн и выполнения требований локальных нормативных актов и иной организационно-распорядительной документации по обеспечению безопасности ПДн;
- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, порчи информации ограниченного доступа и технических средств, входящих в состав ИСПДн;
- требовать прекращения обработки ПДн в случае нарушения установленного порядка работ или нарушения функционирования СиЗИ;

- участвовать в анализе ситуаций, касающихся функционирования СЗИ и расследования фактов несанкционированного доступа к ПДн;
- подавать свои предложения по совершенствованию организационных и технических мер по защите ПДн.

5. Ответственность

5.1. На Ответственного возлагается персональная ответственность за качество проводимых им работ по обеспечению защиты ПДн.

5.2. Ответственный несет ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации. За несоблюдение требований законодательства Российской Федерации о ПДн предусмотрена гражданская, уголовная, административная, дисциплинарная ответственность.

5.3. Ответственный несет ответственность по действующему законодательству Российской Федерации за разглашение информации ограниченного доступа, ставшей ему известной при выполнении служебных обязанностей, в том числе предусмотренных настоящей Инструкцией.

6. Срок действия и порядок внесения изменений

6.1. Настоящая Инструкция вступает в силу с момента его утверждения и действует бессрочно.

6.2. Настоящая Инструкция подлежит пересмотру не реже одного раза в три года.

6.3. Изменения и дополнения в настоящую Инструкцию вносятся приказом директора Учреждения.

Приложение 3

к приказу МБУ ДО РР ДЮЦТ

от «19» марта 2021 г. № 15

Инструкция

администратора информационных систем персональных данных МБУ ДО РР ДЮЦТ

1. Термины и определения

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

Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность. Инцидентами информационной безопасности являются:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по информационной безопасности;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

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;

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

Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

2.1. Настоящая Инструкция определяет функциональные обязанности, ответственность и права администратора информационных систем персональных данных (далее – Администратор) МБУ ДО РР ДЮЦТ (далее – Учреждение).

2.2. Настоящая Инструкция разработана в соответствии с нормативными правовыми актами Российской Федерации в области защиты персональных данных (далее – ПДн), методическими и руководящими документами уполномоченных федеральных органов исполнительной власти.

2.3. Администратор назначается приказом директора Учреждения.

2.4. На время временного отсутствия (болезнь, отпуск, пр.) Администратора, его обязанности возлагаются на работника, назначенного и допущенного к обработке ПДн в установленном порядке.

2.5. Администратор в своей работе руководствуется настоящей Инструкцией.

2.6. Настоящая Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности информации и не исключает обязательного выполнения их требований.

3. Функциональные обязанности

3.1. Администратор выполняет следующие функции:

3.1.1. Управляет параметрами ИСПДн:

- управляет заведением и удалением учетных записей пользователей ИСПДн;
- управляет полномочиями пользователей ИСПДн;
- поддерживает правила разграничения доступа в ИСПДн;
- управляет параметрами настройки программного обеспечения;
- управляет учетными записями пользователей программных средств обработки ПДн;
- оказывает помощь в смене и восстановлению паролей;
- управляет установкой обновлений программного обеспечения;
- регистрирует события в ИСПДн, связанные с защитой ПДн (события безопасности);

3.1.2. Администратор выявляет инциденты (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования ИСПДн и (или) к возникновению угроз безопасности информации (далее – Инциденты), и реагирует на них:

- отказы в обслуживании;
- сбои (перезагрузки) в работе средств защиты информации;
- нарушения правил разграничения доступа;
- неправомерные действия по сбору информации;
- иные события, приводящие к возникновению инцидентов.

3.1.3. Своевременно информирует ответственного за обеспечение безопасности ПДн в ИСПДн, о возникновении Инцидентов в ИСПДн;

3.1.4. Принимает меры по устранению Инцидентов, в том числе:

- по восстановлению ИСПДн и ее сегментов в случае отказа в обслуживании или после сбоев;
- по устранению последствий нарушения правил разграничения доступа, несанкционированного доступа к защищаемой информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению Инцидентов.

3.1.5. Ведет учет пользователей ИСПДн;

3.1.6. Принимает участие в деятельности по:

- подготовке, пересмотру, уточнению локальных актов по защите информации;
- аттестации объектов информатизации.

4. Права

4.1. Администратор имеет право:

- требовать от работников – пользователей ИСПДн соблюдения установленной технологии обработки ПДн и выполнения требований локальных нормативных актов и иной организационно-распорядительной документации по обеспечению безопасности ПДн;
- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, порчи информации ограниченного доступа и технических средств, входящих в состав ИСПДн;
- требовать прекращения обработки ПДн в случае нарушения установленного порядка работ или нарушения функционирования средств защиты информации;
- участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа в ИСПДн;
- подавать свои предложения по совершенствованию организационных и технических мер по защите ПДн.

5. Ответственность

5.1. На Администратора возлагается персональная ответственность за качество проводимых им работ по обеспечению бесперебойного и стабильного функционирования ИСПДн.

5.2. Администратор несет ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации. За несоблюдение требований законодательства Российской Федерации о ПДн предусмотрена гражданская, уголовная, административная, дисциплинарная ответственность.

5.3. Администратор несет ответственность по действующему законодательству Российской Федерации за разглашение информации ограниченного доступа, ставшей ему известной при выполнении служебных обязанностей, в том числе предусмотренных настоящей Инструкцией.

6. Срок действия и порядок внесения изменений

6.4. Настоящая Инструкция вступает в силу с момента её утверждения и действует бессрочно.

6.5. Настоящая Инструкция подлежит пересмотру не реже одного раза в три года.

6.6. Изменения и дополнения в настоящую Инструкцию вносятся приказом директора Учреждения.

УПРАВЛЕНИЕ ОБРАЗОВАНИЯ И МОЛОДЕЖНОЙ ПОЛИТИКИ
АДМИНИСТРАЦИИ РЫБНОВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА РЯЗАНСКОЙ ОБЛАСТИ
Муниципальное бюджетное учреждение дополнительного образования
«Рыбновский районный
Детско-юношеский Центр туризма»

391110, Рязанская область,
г. Рыбное, Набережный
пер., д.2

тел. (49137) 52-2-60,

ПРИКАЗ

«19» марта 2021 г. № 16

Об утверждении перечня персональных данных,

информационных систем персональных данных

и допущенных работников

Во исполнение требований Федерального закона №152-ФЗ от 27 июля 2006 г. «О персональных данных» и прочих нормативных документов по защите информации,

ПРИКАЗЫВАЮ:

1. Утвердить Перечень персональных данных, обрабатываемых в МБУ ДО РР ДЮЦТ (Приложение 1 к настоящему Приказу).
2. Утвердить Перечень информационных систем персональных данных МБУ ДО РР ДЮЦТ (Приложение 2 к настоящему Приказу).
3. Утвердить Перечень должностей работников МБУ ДО РР ДЮЦТ, допущенных к обработке персональных данных (Приложение 3 к настоящему Приказу).
4. Ответственному за организацию обработки персональных данных ознакомить работников, которым в связи со служебными обязанностями необходим доступ к персональным данным с прилагаемыми перечнями.
5. Контроль за исполнением настоящего Приказа оставляю за собой.

Директор Новиков С.В.

Приложение 1

к приказу МБУ ДО РР ДЮЦТ

от «19» марта 2021 г. № 16

ПЕРЕЧЕНЬ

персональных данных, обрабатываемых

в МБУ ДО РР ДЮЦТ

№ п/п	Категории субъектов персональных данных	Способы обработки персональных данных	Цели обработки персональных данных	Перечень обрабатываемых персональных данных	Правовое основание обработки персональных данных	Срок хранения и обработки персональных данных
1	Работники, бывшие работники	Неавтоматизированный; Автоматизированный в ИСПДн «Бухгалтерия»	- ведение кадрового, бухгалтерского и воинского учета; - содействие работникам в продвижении по службе; - обеспечение пропускного режима, сохранности имущества Оператора,	Иные категории: - фамилия, имя, отчество; - сведения об изменении фамилии, имени, отчества (причина изменения, дата); - пол; - дата рождения (число, месяц, год); - место рождения (в соответствии с паспортными данными); - гражданство;	- ст. ст. 65, 86-90 Трудового кодекса РФ; - Налоговый кодекс РФ; - Федеральный закон №167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации»; - Федеральный закон №402-ФЗ «О	-

№ п/п	Категории субъектов персональных данных	Способы обработки персональных данных	Цели обработки персональных данных	Перечень обрабатываемых персональных данных	Правовое основание обработки персональных данных	Срок хранения и обработки персональных данных
			обеспечение личной безопасности; - исполнение Оператором функции работодателя, оформления трудовых отношений и обеспечение установленных законодательством Российской Федерации условий труда; - осуществление видов деятельности, предусмотренных уставом.	- знание иностранных языков (наименование, степень владения); - сведения об образовании, в том числе и послевузовском профессиональном образовании (вид образования, наименование и год окончания образовательного учреждения, квалификация, специальность по документу об образовании); - профессия; - стаж работы; - состояние в браке; - состав семьи (степень родства, фамилия, имя, отчество, год рождения); - реквизиты документа, удостоверяющего личность (вид, серия, номер, дата выдачи, наименование органа, выдавшего документ);	бухгалтерском учете»; - Федеральный закон №255-ФЗ «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством»; - ст. 8 Федерального закона от 31.05.1996 №61-ФЗ «Об обороне»; - Федеральный закон № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации».	

№ п/п	Категории субъектов персональных данных	Способы обработки персональных данных	Цели обработки персональных данных	Перечень обрабатываемых персональных данных	Правовое основание обработки персональных данных	Срок хранения и обработки персональных данных
				- адрес места жительства (адрес регистрации, фактического проживания); - дата регистрации по месту жительства; - идентификационный номер налогоплательщика (ИНН); - номер страхового свидетельства государственного пенсионного страхования (СНИЛС); - контактные данные (номер телефона и адрес электронной почты); - сведения о воинском учете (категория запаса, воинское звание, состав (профиль), полное кодовое обозначение ВУС, категория годности к военной службе, наименование военного комиссариата по месту жительства, отметка о		

№ п/п	Категории субъектов персональных данных	Способы обработки персональных данных	Цели обработки персональных данных	Перечень обрабатываемых персональных данных	Правовое основание обработки персональных данных	Срок хранения и обработки персональных данных
				постановке и снятии с воинского учета); - номер и дата трудового договора; - табельный номер; - сведения о приеме на работу и переводах на другую работу (дата, структурное подразделение, должность, тарифная ставка (оклад), основание); - сведения о предыдущем месте работы по трудовому договору (организация, адрес расположения, должность); - сведения о прохождении аттестации (дата, решение комиссии, номер и дата документа о прохождении аттестации, основание); - сведения о повышении квалификации (даты начала и окончания обучения, вид повышения квалификации, наименование образовательного		

№ п/п	Категории субъектов персональных данных	Способы обработки персональных данных	Цели обработки персональных данных	Перечень обрабатываемых персональных данных	Правовое основание обработки персональных данных	Срок хранения и обработки персональных данных
				учреждения, серия, номер, наименование документа о повышении квалификации); - сведения о профессиональной переподготовке (даты начала и окончания переподготовки, специальность, номер и дата документа о прохождении профессиональной переподготовки); - сведения о наградах (поощрениях), почетных званиях (наименование награды, наименование, номер и дата подтверждающего документа); - сведения об отпусках (вид отпуска, количество календарных дней отпуска, даты начала и окончания отпуска); - сведения о социальных льготах (наименование		

№ п/п	Категории субъектов персональных данных	Способы обработки персональных данных	Цели обработки персональных данных	Перечень обрабатываемых персональных данных	Правовое основание обработки персональных данных	Срок хранения и обработки персональных данных
				льготы, номер и дата выдачи документа); - основание прекращения трудового договора (увольнения); - дата увольнения; - банковские реквизиты для перечисления заработной платы и иных выплат; - фотография (не является биометрическими персональными данными, т.к. не используется для установления личности и не соответствует требованиям ГОСТ Р ИСО/МЭК 19794-5-2013); - сведения о деловых и иных личных качествах, носящих оценочный характер.		
		Неавтоматизированный; Автоматизированный в ИСПДн «Бухгалтерия»	- ведение единого справочника работников, адресной книги	<u>Общедоступные категории:</u> - фамилия, имя, отчество; - должность;	- согласие на обработку персональных данных.	-

№ п/п	Категории субъектов персональных данных	Способы обработки персональных данных	Цели обработки персональных данных	Перечень обрабатываемых персональных данных	Правовое основание обработки персональных данных	Срок хранения и обработки персональных данных
			(информационное обеспечение); - реклама, продвижение товаров и услуг.	- номер городского рабочего телефона, номер внутреннего телефона; - адрес электронной почты; - фотография (не является биометрическими персональными данными, т.к. не используется для установления личности и не соответствует требованиям ГОСТ Р ИСО/МЭК 19794-5-2013).		
2	Ближайшие родственники работников	Неавтоматизированный; Автоматизированный в ИСПДн «Бухгалтерия»	- содействие в получении социальных льгот и налоговых вычетов	<u>Иные категории:</u> - степень родства; - фамилия, имя, отчество; - дата рождения; - данные о несовершеннолетних детях (свидетельство о рождении; справка об очном обучении – для налогового вычета).	- ст. 218 Налогового кодекса РФ; - Постановление Госкомстата РФ №1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты».	-
3	Кандидаты на замещение	Неавтоматизированный; Автоматизированный в	- подбор персонала,	<u>Иные категории:</u> - фамилия, имя, отчество;	- Согласие на обработку	-

№ п/п	Категории субъектов персональных данных	Способы обработки персональных данных	Цели обработки персональных данных	Перечень обрабатываемых персональных данных	Правовое основание обработки персональных данных	Срок хранения и обработки персональных данных
	вакантных должностей	ИСПДн «Бухгалтерия»	содействие в трудоустройстве и выборе подходящей должности.	- пол; - дата рождения (число, месяц, год); - знание иностранных языков (наименование, степень владения); - сведения об образовании, в том числе и послевузовском профессиональном образовании (вид образования, наименование и год окончания образовательного учреждения, квалификация, специальность по документу об образовании); - контактные данные (номер телефона и адрес электронной почты); - сведения о предыдущем месте работы по трудовому договору (организация, адрес расположения, должность, трудовой стаж); - фотография (не является биометрическими	персональных данных.	

№ п/п	Категории субъектов персональных данных	Способы обработки персональных данных	Цели обработки персональных данных	Перечень обрабатываемых персональных данных	Правовое основание обработки персональных данных	Срок хранения и обработки персональных данных
				персональными данными, т.к. не используется для установления личности и не соответствует требованиям ГОСТ Р ИСО/МЭК 19794-5-2013); - сведения о предпочитаемой заработной плате; - сведения о деловых и иных личных качествах, носящих оценочный характер; - иные сведения, содержащиеся в резюме кандидата на замещение вакантных должностей.		
4	Физические лица, выполняющие работу по договорам гражданско-правового характера	Неавтоматизированный; Автоматизированный в ИСПДн «___»	- выполнение договорных обязательств.	<u>Иные категории:</u> - фамилия, имя, отчество; - дата рождения (число, месяц, год); - место рождения (в соответствии с паспортными данными); - гражданство; - реквизиты документа, удостоверяющего личность	- Гражданский кодекс РФ; - договор гражданско-правового характера; - согласие на обработку персональных данных.	-

№ п/п	Категории субъектов персональных данных	Способы обработки персональных данных	Цели обработки персональных данных	Перечень обрабатываемых персональных данных	Правовое основание обработки персональных данных	Срок хранения и обработки персональных данных
				(вид, серия, номер, дата выдачи, наименование органа, выдавшего документ); - адрес места жительства (адрес регистрации, фактического проживания); - дата регистрации по месту жительства; - идентификационный номер налогоплательщика (ИНН); - контактные данные (номер телефона и адрес электронной почты); - сведения о заработной плате; - банковские реквизиты для перечисления заработной платы и иных выплат.		
5	Пользователи сайта	Неавтоматизированный; Автоматизированный в ИСПДн «Навигатор»	- продвижение товаров, работ, услуг; - установление с пользователем сайта обратной	<u>Иные категории:</u> - фамилия, имя, отчество; - дата рождения; - номер телефона; - адрес электронной почты;	- согласие на обработку персональных данных.	-

№ п/п	Категории субъектов персональных данных	Способы обработки персональных данных	Цели обработки персональных данных	Перечень обрабатываемых персональных данных	Правовое основание обработки персональных данных	Срок хранения и обработки персональных данных
			связи, включая направление уведомлений, запросов и их обработки, а также обработки запросов и заявок от пользователя в целях дальнейшего заключения и исполнения договора; - получение и публикация отзывов; - подбор персонала.	- адрес доставки; - информация, содержащиеся в резюме; - иная информация, которую пользователь решил предоставить.		
		Неавтоматизированный; Автоматизированный в ИСПДн «Навигатор»	- ведение статистики и анализа работы Сайта.	<u>Иные категории:</u> - файлы cookie; - сведения о действиях пользователей Сайта; - сведения об оборудовании и браузере пользователя; - IP-адрес; - дата и время сессии;	- согласие на обработку персональных данных.	-

№ п/п	Категории субъектов персональных данных	Способы обработки персональных данных	Цели обработки персональных данных	Перечень обрабатываемых персональных данных	Правовое основание обработки персональных данных	Срок хранения и обработки персональных данных
				- реферер (адрес предыдущей страницы).		
6	Дети и родители	Неавтоматизированная; Автоматизированная в ИСПДн «Навигатор»	- обработка заявок на обучение и учет обучающихся.	<u>Иные категории:</u> - фамилия, имя, отчество ребенка; - фамилия, имя, отчество родителей; - дата рождения; - СНИЛС; - Номер сертификата персонифицированного финансирования дополнительного образования ребенка; - Email; - телефон; - муниципалитет.	- согласие на обработку персональных данных.	- 3 года

Приложение 2

к приказу МБУ ДО РР ДЮЦТ

от «19» марта 2021 г. № 16

ПЕРЕЧЕНЬ

информационных систем персональных данных

МБУ ДО РР ДЮЦТ

№ п/п	Характеристики информационной системы	Значение характеристики информационной системы
1	Информационная система персональных данных «Бухгалтерия» / Автоматизированный в ИСПДн «Бухгалтерия»	
1.1	Категории субъектов ПДн	Работники, бывшие работники; ближайшие родственники работников
1.2	Категории ПДн	Иные категории ПДн
1.3	Количество субъектов, ПДн которых обрабатываются в ИСПДн	Менее чем 100 000 субъектов
1.4	Перечень действий (операций), совершаемых с ПДн	Сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, доступ, удаление, уничтожение ПДн
1.5	Месторасположение баз данных	Адрес: 391110, Рязанская обл., г.Рыбное, Набережный переулок, д.2
1.6	Расположение рабочих мест	Адрес: 391110, Рязанская обл., г.Рыбное, Набережный переулок, д.2
2	Информационная система персональных данных «Навигатор» / ИСПДн «Навигатор»	
2.1	Категории субъектов ПДн	Работники, бывшие работники; ближайшие родственники работников
2.2	Категории ПДн	Иные категории ПДн
2.3	Количество субъектов, ПДн которых обрабатываются в ИСПДн	Менее чем 100 000 субъектов
2.4	Перечень действий (операций), совершаемых с ПДн	Сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение,

№ п/п	Характеристики информационной системы	Значение характеристики информационной системы
		использование, доступ, удаление, уничтожение ПДн
2.5	Месторасположение баз данных	Сервер в ЦОД «Colocat»

Приложение 3

к приказу МБУ ДО РР ДЮЦТ

от «19» марта 2021 г. № 16

ПЕРЕЧЕНЬ

должностей работников МБУ ДО РР ДЮЦТ**,**

допущенных к обработке персональных данных

№ п/п	Должность	Наименование информационных систем	Имеет ли доступ к неавтоматизированной обработке (да, нет)	Категории обрабатываемых персональных данных
1	Директор	ИСПДН «Навигатор»	Да	Дети и родители; Пользователи сайта
2	Методист		Да	
3.	Педагог-организатор		Да	
4.	Педагог дополнительного образования		Да	

УПРАВЛЕНИЕ ОБРАЗОВАНИЯ И МОЛОДЕЖНОЙ ПОЛИТИКИ
АДМИНИСТРАЦИИ РЫБНОВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА РЯЗАНСКОЙ ОБЛАСТИ
Муниципальное бюджетное учреждение дополнительного образования
«Рыбновский районный
Детско-юношеский Центр туризма»

391110, Рязанская область,
г. Рыбное, Набережный
пер., д.2

тел. (49137) 52-2-60,

ПРИКАЗ

«19» марта 2021 г. № 17

Об организации режима обеспечения безопасности помещений, в которых ведется обработка персональных данных

В целях исключения неконтролируемого пребывания в помещениях МБУ ДО РР ДЮЦТ лиц, не имеющих доступа к персональным данным, а также во исполнение Федерального закона №152-ФЗ от 27 июля 2006 г. «О персональных данных» и прочих нормативных документов по защите информации,

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемый Перечень помещений, в которых ведется обработка персональных данных в МБУ ДО РР ДЮЦТ (далее – Перечень) (Приложение 1 к настоящему Приказу).
2. Утвердить прилагаемые Правила доступа работников в помещения, в которых ведется обработка персональных данных в МБУ ДО РР ДЮЦТ (далее – Правила) (Приложение 2 к настоящему Приказу).
3. Возложить персональную ответственность за обеспечение режима безопасности в защищаемых помещениях на директора учреждения.
4. Все помещения контролируемой зоны в нерабочее время подлежат закрытию на ключ.
5. Ответственному за организацию обработки персональных данных в МБУ ДО РР ДЮЦТ ознакомить работников, которым в связи со служебными обязанностями необходим доступ в помещения, в которых ведется обработка персональных данных, с прилагаемыми Перечнем и Правилами.
6. Контроль за исполнением настоящего Приказа оставляю за собой.

Директор С.В.Новиков

Приложение № 1

к приказу МБУ ДО РР ДЮЦТ

от «19» марта 2021 г. № 17

ПЕРЕЧЕНЬ

помещений, в которых ведется обработка персональных данных

в МБУ ДО РР ДЮЦТ

№ п/п	Наименование/номер помещения	Адрес расположения помещения	Допущенные должностные лица
1	Методический	391110, Рязанская обл., г.Рыбное, Набережный переулок, д.2	Директор Новиков С.В.
2			Педагог-организатор Новиков А.С.
3			Педагог-организатор Ганина А.С.
4			Методист Новикова С.В.

Приложение 2

к приказу МБУ ДО РР ДЮЦТ

от «19» марта 2021 г. № 17

ПРАВИЛА

доступа работников в помещения,

в которых ведется обработка персональных данных

в МБУ ДО РР ДЮЦТ

1. Термины и определения

Контролируемая зона — это территория или пространство, на которых исключено неконтролируемое пребывание лиц или транспортных средств;

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;

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

2. Общие положения

2.1. Настоящие Правила доступа работников в помещения, в которых ведется обработка персональных данных в МБУ ДО РР ДЮЦТ (далее – Правила) устанавливают единые требования к доступу работников в помещения, в которых ведется обработка персональных данных (далее – ПДн).

2.2. Настоящие Правила разработаны в соответствии с нормативными правовыми актами Российской Федерации в области защиты ПДн, методическими и руководящими документами уполномоченных федеральных органов исполнительной власти.

2.3. Правила обязательны для исполнения всеми работниками, которые участвуют в обработке ПДн.

2.4. Нарушение Правил влечёт материальную, дисциплинарную, гражданскую, административную и уголовную ответственность в соответствии с нормами действующего законодательства Российской Федерации.

2.5. В здании, расположенном по адресу: 391110, Рязанская область, г. Рыбное, ул. Набережный переулок, д.2 установлен пропускной режим: проход работников и посетителей в здание по рабочим дням в рабочее время (с 8.00 до 17.00), а также в выходные дни согласно расписанию работы объединений.

3. Организация доступа в помещения

3.1. Право на бесконтрольный доступ в помещения, в которых ведется обработка ПДн (далее – Помещения), имеют только работники, указанные в «Перечне помещений, в

которых ведется обработка персональных данных в МБУ ДО РР ДЮЦТ» (далее – Уполномоченные работники).

3.2. Нахождение в Помещениях лиц, не имеющих права доступа к ПДн, возможно только в сопровождении (в присутствии в соответствующем Помещении) Уполномоченного работника.

3.3. Уборка Помещений должна производиться в присутствии Уполномоченного работника, с соблюдением мер, исключающих доступ посторонних лиц к защищаемым ресурсам. При этом экраны мониторов должны быть выключены (либо осуществлена временная блокировка экранов/учетных записей пользователей автоматизированных рабочих мест), документы, находящиеся в печатающих устройствах, и учтенные носители информации должны быть убраны.

3.4. Доступ в Помещения разрешается по рабочим дням в рабочее время (с 8:00 до 17:00) и выходные дни согласно расписанию работы объединений.

3.5. В случае, если в течение рабочего дня Помещение, в котором осуществляется обработка ПДн в Учреждении, покидают все Уполномоченные работники (в том числе во время перерыва для отдыха и приема пищи, в связи с убытием в служебные поездки и т.п.), входная дверь этого помещения должна быть закрыта на ключ.

3.6. Последний работник, покидающий (в том числе в течение рабочего дня и по его завершении) помещение, в котором осуществляется обработка ПДн в Учреждении, обязан:

- проверить закрытие на запоры окон и фрамуг;
- проверить отключение от электросети всех видов электрооборудования и электроприборов, не требующих по условиям эксплуатации постоянного подключения к электросети, отсутствие признаков загорания (запах гари, задымление и т.п.);
- выключить освещение в Помещении;
- закрыть помещение на ключ.

3.7. В случае возникновения нештатной ситуации (пожар, затопление, сбой в работе или выход из строя инженерных систем, совершение незаконных действий) работники коммунальных и аварийно-технических служб имеют право незамедлительного, беспрепятственного доступа в Помещения, в которых ведется обработка ПДн, в любое время суток, без какого-либо предварительного уведомления с целью предотвращения или ликвидации нештатной ситуации, или последствий нештатной ситуации. По результатам предотвращения или ликвидации нештатной ситуации, или последствий нештатной ситуации оставляется Акт вскрытия помещения при чрезвычайных ситуациях.

3.8. Ответственным за организацию доступа в Помещение и организацию обработки ПДн в Учреждении является директор учреждения.

4. Ограничение доступа в помещения

4.1. В целях соблюдения требований к ограничению доступа в Помещения обеспечивается:

- использование Помещений строго по назначению;
- наличие на входах в Помещения дверей, оборудованных запорными устройствами;
- содержание дверей Помещений в нерабочее время в закрытом на запорное устройство состоянии;
- содержание окон в Помещениях в нерабочее время в закрытом состоянии.

5. Срок действия и порядок внесения изменений

a. Настоящие Правила вступают в силу с момента их утверждения и действуют бессрочно.
b. Настоящие Правила подлежат пересмотру не реже одного раза в три года.
c. Изменения и дополнения в настоящие Правила вносятся приказом директора Учреждения.

УПРАВЛЕНИЕ ОБРАЗОВАНИЯ И МОЛОДЕЖНОЙ ПОЛИТИКИ
АДМИНИСТРАЦИИ РЫБНОВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА РЯЗАНСКОЙ ОБЛАСТИ
Муниципальное бюджетное учреждение дополнительного образования
«Рыбновский районный
Детско-юношеский Центр туризма»

391110, Рязанская область,
г. Рыбное, Набережный
пер., д.2

тел. (49137) 52-2-60,

ПРИКАЗ

«19» марта 2021 г. № 18

Об утверждении инструкций по защите персональных данных

Во исполнение Федерального закона Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона №152-ФЗ от 27.07.2006 г. «О персональных данных» и прочих нормативных документов по защите информации, а также с целью обеспечения безопасности персональных данных в МБУ ДО РР ДЮЦТ, ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие Инструкцию пользователя информационных систем персональных данных МБУ ДО РР ДЮЦТ (Приложение 1 к настоящему Приказу).
2. Утвердить и ввести в действие Инструкцию по парольной защите информации в МБУ ДО РР ДЮЦТ (Приложение 2 к настоящему Приказу).
3. Утвердить и ввести в действие Инструкцию по организации антивирусной защиты информации в МБУ ДО РР ДЮЦТ (Приложение 3 к настоящему Приказу).
4. Утвердить и ввести в действие Инструкцию по организации резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных МБУ ДО РР ДЮЦТ (Приложение 4 к настоящему Приказу).
5. Утвердить и ввести в действие Порядок обращения со съемными машинными носителями персональных данных в МБУ ДО РР ДЮЦТ (Приложение 5 к настоящему Приказу).

6. Требования настоящего приказа довести до работников, осуществляющих обработку персональных данных в информационных системах персональных данных в МБУ ДО РР ДЮЦТ.

7. Контроль за исполнением настоящего Приказа оставляю за собой.

Директор С.В.Новиков

Приложение 1

к приказу МБУ ДО РР ДЮЦТ

от «19» марта 2021 г. № 18

ИНСТРУКЦИЯ

пользователя информационных систем персональных данных

МБУ ДО РР ДЮЦТ

1. Термины и определения

Автоматизированное рабочее место – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида;

Антивирусная защита – защита информации и компонентов информационной системы от вредоносных компьютерных программ (вирусов) (обнаружение вредоносных компьютерных программ (вирусов), блокирование, изолирование "зараженных" объектов, удаление вредоносных компьютерных программ (вирусов) из "зараженных" объектов);

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

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;

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

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

Пользователь информационной системы персональных данных – работник, осуществляющий обработку персональных данных в информационной системе персональных данных;

Средство антивирусной защиты – программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации;

Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

2.1. Настоящая Инструкция пользователя информационных систем персональных данных МБУ ДО РР ДЮЦТ (далее – Инструкция) определяет обязанности, права и ответственность работников при работе в информационных системах персональных данных (далее – ИСПДн).

2.2. Требования настоящей Инструкции являются обязательными для всех работников, осуществляющих обработку и защиту персональных данных (далее – ПДн) в ИСПДн – пользователей ИСПДн (далее – Пользователи).

2.3. К защищаемой информации, обрабатываемой в ИСПДн МБУ ДО РР ДЮЦТ (далее – Учреждение), относятся ПДн, служебная (технологическая) информация системы защиты и другая информация ограниченного доступа.

2.4. Все пользователи ИСПДн Учреждения должны быть ознакомлены с требования настоящей Инструкции под подпись.

2.5. Настоящая Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности сведений конфиденциального характера, в том числе и ПДн, и не исключает обязательного выполнения их требований.

3. Допуск пользователей к информационным системам персональных данных

3.1. Допуск пользователей к работе с ПДн в ИСПДн осуществляется в соответствии с Матрицей доступа к информационным ресурсам.

3.2. К самостоятельной работе на автоматизированных рабочих местах (далее – АРМ), входящих в состав ИСПДн, допускаются лица, изучившие требования настоящей Инструкции и локальных нормативных актов по защите информации, освоившие правила эксплуатации АРМ и технических средств защиты.

3.3. Допуск производится после проверки знания настоящей Инструкции и практических навыков в работе.

4. Обязанности пользователя

4.1. Каждый Пользователь имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

4.1.1. Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн.

4.1.2. Знать и строго выполнять правила работы со средствами защиты информации, установленными в ИСПДн.

4.1.3. Выполнять требования по антивирусной защите в части, касающейся действий Пользователей.

4.1.4. Немедленно ставить в известность ответственного за обеспечение безопасности ПДн в ИСПДн или администратора ИСПДн:

- при подозрении компрометации личного пароля;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ИСПДн;
- некорректного функционирования установленных средств защиты;

- обнаружения непредусмотренных отводов кабелей и подключенных устройств;
- обнаружения фактов, попыток несанкционированного доступа и случаев нарушения установленного порядка обработки ПДн.

4.1.5. Экран видеомонитора в помещении располагать во время работы так, чтобы исключалась возможность ознакомления с отображаемой на них информацией посторонними лицами.

4.2. Пользователям ИСПДн запрещается:

- отключать (блокировать) средства защиты информации, предусмотренные организационно-распорядительными документами на ИСПДн;
- производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств;
- самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
- обрабатывать в ИСПДн информацию и выполнять другие работы, не предусмотренные перечнем прав Пользователя по доступу к ИСПДн;
- сообщать (или передавать) посторонним лицам личные атрибуты и пароли доступа к ресурсам ИСПДн;
- работать в ИСПДн при обнаружении каких-либо неисправностей;
- оставлять включенным без присмотра АРМ, не активизировав средства защиты от несанкционированного доступа;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к ознакомлению с защищаемой информацией посторонних лиц;
- производить перемещения технических средств АРМ без согласования с ответственным за обеспечение безопасности ПДн в ИСПДн;
- вскрывать корпуса технических средств АРМ и вносить изменения в схему и конструкцию устройств.

5. Организация работы со съемными машинными носителями информации

5.1. Организация работы со съемными машинными носителями информации (далее – СМНИ), содержащие ПДн и иную информацию конфиденциального характера, осуществляется в соответствии с «Порядком обращения со съемными машинными носителями информации в МБУ ДО РР ДЮЦТ».

5.2. Пользователи обязаны знать и соблюдать установленные требования по учету и хранению СМНИ.

5.3. СМНИ должен быть зарегистрирован в «Журнале учета съемных машинных носителей информации».

5.4. СМНИ закрепляется за определенным лицом, несущим ответственность за сохранность и местонахождение данного СМНИ.

5.5. При необходимости передачи информации на СМНИ, лицо ответственное за хранение уведомляет ответственного за обеспечение безопасности ПДн в ИСПДн о необходимости передачи информации с помощью СМНИ, доставляет СМНИ по месту назначения, передает информацию с него и возвращает его на место хранения.

5.6. Хранение СМНИ осуществляется:

- для флеш-карт, смарт-карт, компакт дисков и др.) в защищенных сейфах;
- для СМНИ, входящих в состав ИСПДн, производится опечатывание корпуса АРМ.

5.7. Пользователям запрещается:

- записывать и хранить ПДн и иную информацию конфиденциального характера на неучтенных СМНИ;
- оставлять СМНИ без присмотра, передавать их другим лицам и выносить за пределы контролируемой зоны, за исключением случаев, в которых разрешена передача СМНИ;
- хранить СМНИ вблизи сильных источников электромагнитных излучений и прямых солнечных лучей;
- хранить на учтенных СМНИ программы и данные, не относящиеся к рабочей информации.

6. Организация парольной защиты

6.1. Организация парольной защиты производится в соответствии с «Инструкцией по парольной защите информации в МБУ ДО РР ДЮЦТ».

6.2. Лица, использующие пароли, обязаны:

- хранить в тайне свой пароль
- четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов;
- своевременно сообщать ответственному за обеспечение безопасности ПДн в ИСПДн обо всех нештатных ситуациях, нарушениях работы систем защиты от несанкционированного доступа, возникающих при работе с паролями.

6.3. Во время ввода паролей необходимо исключить возможность его просмотра посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или отражённом свете) или техническими средствами (видеокамеры, фотоаппараты и др.)

6.4. Для предотвращения доступа к персональным данным, пользователь во время перерыва в работе обязан осуществить блокирование системы нажатием комбинации Ctrl+Alt+Delete и кнопки «Блокировать» или нажатием комбинации Win+L.

6.5. Блокирование сеанса доступа пользователя в ИСПДн осуществляется после 15 минут его бездействия (неактивности).

6.6. В случае утери пароля сотрудник ставит в известность своего непосредственного руководителя и ответственного за обеспечение безопасности ПДн в ИСПДн для принятия последующих решений.

6.7. В случае компрометации пароля (просмотр посторонними, разглашение пароля и др.) необходимо известить своего непосредственного руководителя и ответственного за обеспечение безопасности ПДн в ИСПДн для принятия последующих решений.

7. Правила работы в сетях общего доступа и (или) международного обмена

7.1. Работа в сетях общего доступа и на элементах ИСПДн, должна осуществляться исключительно в служебных целях.

7.2. При работе в сетях общего доступа запрещается:

- осуществлять работу при отключенных средствах защиты;

- передавать по сетям общего доступа защищаемую информацию без использования средств шифрования;
- запрещается скачивать из сети Интернет программное обеспечение и другие файлы, если это не определено его должностными обязанностями;
- запрещается посещение и использование сети Интернет в личных целях.

8. Порядок установки обновлений программного обеспечения

8.1. Установке крупных обновлений программного обеспечения должно предшествовать тестирование информационной инфраструктуры на отсутствие негативных воздействий от устанавливаемых обновлений.

8.2. В случае обнаружения негативного воздействия устанавливаемого обновления на штатное функционирование информационной инфраструктуры, данное обновление устанавливаться не должно по согласованию с администратором ИСПДн.

8.3. Установке новых версий программного обеспечения или внесению серьезных изменений и дополнений в действующее программное обеспечение должно предшествовать тестирование информационной инфраструктуры на отсутствие негативных воздействий указанного программного обеспечения.

8.4. Установка протестированных обновлений, новых версий программного обеспечения или внесение изменений и дополнений в действующее программное обеспечение может быть произведено только по согласованию с администратором ИСПДн и ответственным за обеспечение безопасности ПДн в ИСПДн.

9. Технология обработки персональных данных

9.1. При первичном допуске к работе в ИСПДн Пользователь знакомится с требованиями руководящих, нормативно-методических и организационно-распорядительных документов по вопросам автоматизированной обработки информации, изучает Инструкцию, получает персональный идентификатор или личный пароль у ответственного за обеспечение безопасности ПДн в ИСПДн.

9.2. В процессе работы Пользователь производит обработку ПДн в ИСПДн.

9.3. При необходимости вывод ПДн из ИСПДн осуществляется следующим образом:

- копированием ПДн на учтенные СМНИ;
- передача ПДн по каналам связи с обязательным применением средств криптографической защиты.

10. Срок действия и порядок внесения изменений

10.1. Настоящая Инструкция вступает в силу с момента его утверждения и действует бессрочно.

10.2. Настоящая Инструкция подлежит пересмотру не реже одного раза в три года.

10.3. Изменения и дополнения в настоящую Инструкцию вносятся приказом директора Учреждения.

Приложение 2

к приказу МБУ ДО РР ДЮЦТ

от «19» марта 2021 г. № 18

ИНСТРУКЦИЯ

по парольной защите информации в МБУ ДО РР ДЮЦТ

1. Термины и определения

Автоматизированное рабочее место – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида;

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

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;

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

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

Пользователь информационной системы персональных данных – работник, осуществляющий обработку персональных данных в информационной системе персональных данных;

Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

2.1. Настоящая Инструкция по парольной защите информации в МБУ ДО РР ДЮЦТ (далее – Инструкция) устанавливает требования и ответственность при организации парольной защиты информации, а также определяет порядок контроля за действиями пользователей и обслуживающего персонала информационных систем персональных данных (далее – ИСПДн) при работе с паролями.

2.2. Требования настоящей Инструкции являются обязательными для исполнения всеми пользователями и администраторами ИСПДн МБУ ДО РР ДЮЦТ (далее – Учреждение), использующими в своей работе средства вычислительной техники.

2.3. Все пользователи и администраторы ИСПДн Учреждения, использующие в своей работе средства вычислительной техники, должны быть ознакомлены с требованиями настоящей Инструкции под подпись.

2.4. Настоящая Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности сведений конфиденциального характера, в том числе и персональных данных (далее – ПДн), и не исключает обязательного выполнения их требований.

3. Требования, предъявляемые к идентификаторам (кодам) и паролям (порядок формирования и обращения с ними)

3.1. Авторизация пользователей ИСПДн осуществляется путем ввода идентификатора и/или пароля.

3.2. Требования к формированию паролей и обращению с ними.

3.2.1. Пароль формируется при создании учетной записи ответственным обеспечение безопасности ПДн в ИСПДн или администратором ИСПДн, при первичном входе в учетную запись пароль должен быть изменен владельцем.

3.2.2. Владельцы личных паролей обязаны обеспечить их тайну.

3.2.3. Пароли генерируются с учетом следующих требований:

- пароль должен знать только его владелец;
- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать смысловую нагрузку (имена, фамилии, наименования организаций, улиц, городов и т.д.), общепринятые сокращения (userOl, password02 и т.п.) и последовательные сочетания клавиш клавиатуры (qwertyOl, Ицукен12);
- максимальный срок действия пароля составляет 120 дней;
- минимальный срок действия пароля составляет 2 дня;
- количество неудачных попыток входа в систему, приводящее к блокировке учетной записи пользователя должно быть не более 6.

3.2.4. Требования к формированию паролей обеспечиваются техническими возможностями используемых операционных систем, средств защиты информации и информационных ресурсов.

3.2.5. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в полгода. Внеплановая смена пароля производится в случае его компрометации, а также по просьбе пользователя ИСПДн.

3.2.6. Хранение пользователями ИСПДн своих паролей на бумажном носителе ЗАПРЕЩЕНО.

3.2.7. Пользователь не имеет права сообщить личный пароль другим лицам (разрешается только с согласования ответственного за обеспечение безопасности или администратора ИСПДн при наличии технологической необходимости использования имен и паролей работников в их отсутствие в случае возникновения нештатбных ситуаций, форс-мажорных обстоятельств и т.п. По возращению работники обязаны сразу же сменить свои пароли на новые значения согласно данной Инструкции).

3.3. Порядок смены паролей и идентификаторов при изменениях в организационно-штатной структуре (кадровые перестановки, увольнение работников):

3.3.1. При прекращении действия трудового договора с работником все созданные для этого работника учетные записи (пользовательское имя) подлежат блокированию не позднее, чем в день увольнения работника. Полное удаление учетных записей производится в течении 5 рабочих дней со дня увольнения работника. Основанием для блокирования и последующего удаления учетных записей работника является заявка, представленная непосредственным руководителем увольняемого не позднее, чем за 3 рабочих дня до дня его увольнения.

3.3.2. При проведении организационно-штатных мероприятий (кадровые перестановки) непосредственный руководитель структурного подразделения обязан представить администратору ИСПДн заявку на изменение в правах доступа.

3.4. Порядок действий при компрометации идентификаторов и паролей.

3.4.1. Под компрометацией понимается: утрата пароля учетной записи и (или) пароля идентификатора, разглашение учетной записи пароля или пароля идентификатора (явная компрометация), или иная ситуация, которая дает основание для предположения о нарушении конфиденциальности паролей и идентификаторов (неявная компрометация).

3.4.2. При выявлении факта утраты пароля, разглашения пароля, пароля идентификатора, самого идентификатора пользователь обязан незамедлительно сообщить о данных фактах своему непосредственному руководителю и ответственному за обеспечение безопасности ПДн в ИСПДн или администратору ИСПДн.

3.4.3. В случае выявления факта компрометации идентификаторов и паролей пользователя администратор ИСПДн или ответственный за обеспечение безопасности ПДн в ИСПДн обязан немедленно заблокировать учетную запись данного пользователя и незамедлительно произвести внеплановую смену пароля для этого пользователя.

4. Права и обязанности

4.1. Основные задачи администратора ИСПДн:

- организация установки средств идентификации и аутентификации;
- организация парольной защиты во всех ИСПДн;
- выдача первичных паролей, и электронных персональных идентификаторов и паролей к ним;
- осуществление контроля за состоянием системы парольной защиты информации в ИСПДн.

4.2. Администратор ИСПДн имеет право:

- вносить предложения по совершенствованию системы парольной защиты информации в ИСПДн;
- принимать участие в планировании мероприятий по парольной защите информации в ИСПДн и планировании оснащения средствами идентификации и аутентификации;
- осуществлять контроль состояния средств идентификации и аутентификации в ИСПДн;
- инициировать служебные проверки и участвовать в проведении расследований по фактам компрометации;

- оказывать помощь в решении проблем, возникающих при эксплуатации средств идентификации и аутентификации.

4.3. Обязанности в части парольной защиты информации отражены в инструкции администратора ИСПДн.

4.4. Пользователям ИСПДн в своей работе запрещается:

- сообщать кому-либо свой личный пароль и/или пароль к электронному персональному идентификатору;
- передавать кому-либо выданный электронный персональный идентификатор;
- осуществлять вход в операционные системы ИСПДн и в информационные ресурсы под чужими идентификаторами и паролями;
- отключать средства идентификации и аутентификации.

4.5. В случае появления подозрений на факт компрометации пароля, а также в случае выявления инцидентов (фактов и т.п.), связанных со сбоями в работе средств идентификации и аутентификации, пользователи обязаны немедленно проинформировать об этом ответственного за обеспечение безопасности ПДн в ИСПДн или администратора ИСПДн.

5. Ответственность должностных лиц в рамках системы парольной защиты информации

5.1. Пользователи, ответственный за обеспечение безопасности ПДн в ИСПДн и администратор ИСПДн несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации. За несоблюдение требований законодательства Российской Федерации предусмотрена гражданская, уголовная, административная, дисциплинарная ответственность.

5.2. Пользователи, ответственный за обеспечение безопасности ПДн в ИСПДн и администратор ИСПДн несут ответственность по действующему законодательству Российской Федерации за разглашение сведений конфиденциального характера, ставших известными при выполнении служебных обязанностей, в том числе предусмотренных настоящей Инструкцией.

6. Срок действия и порядок внесения изменений

6.1. Настоящая Инструкция вступает в силу с момента его утверждения и действует бессрочно.

6.2. Настоящая Инструкция подлежит пересмотру не реже одного раза в три года.

6.3. Изменения и дополнения в настоящую Инструкцию вносятся приказом директора Учреждения.

Приложение 3

к приказу МБУ ДО РР ДЮЦТ

от «19» марта 2021 г. № 18

ИНСТРУКЦИЯ

по антивирусной защите

МБУ ДО РР ДЮЦТ

1. Термины и определения

Автоматизированное рабочее место – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида;

Антивирусная защита – защита информации и компонентов информационной системы от вредоносных компьютерных программ (вирусов) (обнаружение вредоносных компьютерных программ (вирусов), блокирование, изолирование "зараженных" объектов, удаление вредоносных компьютерных программ (вирусов) из "зараженных" объектов);

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

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;

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

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

Пользователь информационной системы персональных данных – работник, осуществляющий обработку персональных данных в информационной системе персональных данных;

Средство антивирусной защиты – программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации;

Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

2.1. Настоящая Инструкция по антивирусной защите МБУ ДО РР ДЮЦТ (далее – Инструкция) регулирует вопросы организации антивирусной защиты и требования к порядку проведения антивирусного контроля.

2.2. Инструкция устанавливает требования и ответственность при организации защиты информации от разрушающего воздействия вредоносных программ – компьютерных вирусов.

2.3. Требования настоящей Инструкции являются обязательными для исполнения всеми работниками МБУ ДО РР ДЮЦТ (далее – Учреждения), использующими в своей работе средства вычислительной техники.

2.4. Все работники Учреждения, использующие антивирусные средства, должны быть ознакомлены с требованиями настоящей Инструкцией под подпись.

2.5. Настоящая Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности сведений конфиденциального характера, в том числе и персональных данных (далее – ПДн), и не исключает обязательного выполнения их требований.

3. Требования к антивирусным средствам

3.1. В Учреждении к применению допускаются только лицензионные антивирусные программные и (или) программно-аппаратные средства (антивирусные средства), закупленные у разработчика указанных средств или его официальных дилеров.

3.2. Антивирусные средства должны функционировать в течение всего времени работы средств вычислительной техники (от момента загрузки операционной системы до момента ее выгрузки).

3.3. Антивирусное средство не должно существенно затруднять работоспособность средств вычислительной техники информационных систем персональных данных (далее – ИСПДн).

4. Права и обязанности

4.1. Антивирусной защите подлежит вся, обрабатываемая в Учреждении при помощи средств вычислительной техники, информация, независимо от ограничений доступа к ней.

4.2. Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль.

4.3. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

4.4. В ИСПДн запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

4.5. Сопровождение (регулярное обновление, антивирусный контроль, выявление фактов заражения и проведение служебных расследований) правил антивирусной защиты возлагаются на ответственного за обеспечение безопасности ПДн в ИСПДн.

4.6. Основные задачи ответственного за обеспечение безопасности ПДн в ИСПДн:

- организация процесса установки антивирусных средств в ИСПДн;
- сопровождение антивирусных средств (обновление, антивирусный контроль, сопровождение действий пользователей в случаях обнаружения вирусов, обеспечение работоспособности антивирусных средств);
- контроль состояния системы антивирусной защиты информации в Учреждении.

4.7. Ответственный за обеспечение безопасности ПДн в ИСПДн несет ответственность за:

- за своевременную установку антивирусных средств;
- за эксплуатацию (антивирусный контроль, работоспособность антивирусных средств, сопровождение действий пользователей в случаях обнаружения вирусов) системы антивирусной защиты информации;
- за своевременное обновление лицензий на антивирусные средства;
- за своевременное обновление антивирусных баз.

4.8. Ответственный за обеспечение безопасности ПДн в ИСПДн имеет право:

- вносить предложения по совершенствованию системы антивирусной защиты информации;
- принимать участие в планировании мероприятий по антивирусной защите информации и планировании оснащения антивирусными средствами;
- осуществлять контроль состояния средств антивирусной защиты информации в Учреждении;
- инициировать служебные проверки и участвовать в проведении расследований по фактам заражения вирусами ИСПДн и средств вычислительной техники;
- оказывать помощь в решении проблем, возникающих при эксплуатации средств антивирусной защиты.

4.9. Пользователь антивирусного средства – лицо, на рабочем месте которого применяется антивирусное средство.

4.10. Пользователям антивирусных средств запрещается:

- менять настройки или отключать средства антивирусной защиты во время работы;
- использовать средства антивирусной защиты, отличные от установленных средств;
- без разрешения ответственного за обеспечение безопасности ПДн в ИСПДн копировать любые файлы на съемные носители информации, устанавливать и использовать любое программное обеспечение, не предназначенное для выполнения служебных задач.

5. Порядок и периодичность обновления антивирусных баз

5.1. Своевременное обновление баз данных средств антивирусной защиты информации является неотъемлемой частью обеспечения эффективной политики антивирусной защиты информации.

5.2. Установке обновлений должно предшествовать тестирование ИСПДн на отсутствие негативных воздействий от вновь устанавливаемых обновлений.

5.3. Установке новых версий программного обеспечения или внесению изменений и дополнений в действующее программное обеспечение должно предшествовать тестирование ИСПДн на отсутствие негативных воздействий указанного программного обеспечения.

5.4. Периодичность обновления антивирусных баз:

- обновление антивирусных баз для всех ИСПДн, имеющих подключение к сетям общего пользования и сетям международного информационного обмена, должно быть ежедневным. Источник обновления – сервер разработчика антивирусного средства, либо собственный централизованный сетевой источник обновлений, получающий обновления с сервера разработчика антивирусного средства.
- обновление антивирусных баз для ИСПДн, не имеющих подключение к сетям общего пользования и сетям международного информационного обмена, обновление должно быть не менее 1 раза в неделю. Источником обновления в данном случае являются антивирусные базы, записанные на предварительно учтенный в установленном порядке съемный машинный носитель информации.

6. Порядок и периодичность проведения антивирусного контроля

6.1. Объектами антивирусного контроля являются:

- жесткие магнитные диски рабочих станций и серверов ИСПДн;
- сетевые хранилища (системы хранения данных);
- оперативная и системная память средств вычислительной техники;
- съемные машинные носители информации;
- входящий и исходящий контент (веб-трафик);
- файлы, получаемые и передаваемые через сети общего пользования и международного информационного обмена;
- почтовые сообщения электронной почты.

6.2. Антивирусный контроль входящей информации со съемных машинных носителей информации необходимо проводить до переноса информации на жёсткий магнитный диск рабочей станции или сетевой диск. Информация, получаемая по телекоммуникационным каналам, должна проверятся во время, или сразу после получения. Контроль исходящей информации необходимо проводить непосредственно перед отправкой (записью на съемный носитель).

6.3. Виды и периодичность антивирусных проверок представлены в таблице 1.

Таблица 1

№ п/п	Объект контроля	Вид проверки	Периодичность проверки
1	Жесткие магнитные диски рабочих станций и серверов ИСПДн	Полная проверка	1 раз в месяц
		Быстрое сканирование	1 раз в неделю

№ п/п	Объект контроля	Вид проверки	Периодичность проверки
2	Сетевые хранилища (системы хранения данных)	Полная проверка	1 раз в месяц
3	Оперативная и системная память средств вычислительной техники	Полная проверка	1 раз в месяц
		Быстрое сканирование	1 раз в неделю
4	Съемные машинные носители информации	Полная проверка	При каждом подключении
5	Веб-трафик	Минимально необходимое требование - настройка антивирусного средства по умолчанию	Постоянно
6	Файлы, получаемые и передаваемые через сети общего пользования и международного информационного обмена	Полная проверка	При каждом получении и отправке
7	Почтовые сообщения электронной почты	Минимально необходимое требование - настройка антивирусного средства по умолчанию	При каждом получении и отправке

7. Порядок действий при обнаружении вирусов

7.1. Основными путями проникновения вирусов в ИСПДн являются: любые съемные машинные носители информации, электронные почтовые сообщения, трафик, получаемый из сетей общего пользования и сетей международного информационного обмена, ранее зараженные рабочие станции и сервера.

7.2. В случае обнаружения вирусов при входном контроле съемных машинных носителей информации, файлов или электронных почтовых сообщений, пользователь должен:

- немедленно приостановить все работы на своей рабочей станции;
- сообщить ответственному за обеспечение безопасности ПДн в ИСПДн о факте обнаружения вируса;
- принять согласованные с ответственным за обеспечение безопасности ПДн в ИСПДн меры по локализации и удалению вируса с использованием антивирусных средств.

7.3. При невозможности ликвидации последствий вирусного заражения ответственному за обеспечение безопасности ПДн в ИСПДн необходимо:

- сообщить о факте обнаружения программных вирусов в организацию, осуществляющую техническую поддержку эксплуатации средств антивирусной защиты информации;

- заархивировать зараженные файлы и направить с приложением соответствующего сопроводительного документа в организацию, осуществляющую техническую поддержку эксплуатации средств антивирусной защиты информации.

7.4. При получении информации о возможном нарушении либо выявлении факта нарушения требований настоящей Инструкции работа на рабочей станции данного пользователя незамедлительно блокируется по решению ответственного за обеспечение безопасности ПДн в ИСПДн.

7.5. Факты модификации и разрушения данных на серверах или рабочих станциях, заражение их вирусами, а также обнаружение других вредоносных программ – все это относится к значимым нарушениям безопасности информации и должны быть проанализированы посредством проведения служебного расследования.

7.6. Служебное расследование проводится комиссией, назначаемой приказом Директора Учреждения. В состав комиссии в обязательном порядке включается администратор ИСПДн, ответственный за обеспечение безопасности ПДн в ИСПДн, непосредственный руководитель работника, допустившего факт компрометации. При необходимости в состав комиссии могут включаться другие сотрудники.

7.7. Результаты работы комиссии оформляются актом. Акт подлежит утверждению Директора Учреждения.

7.8. В процессе работы комиссии обязательными для установления являются:

- дата и время заражения (обнаружения заражения);
- ФИО, должность и подразделение сотрудника, техническое средство которого заражено вирусной программой;
- уровень критичности заражения;
- обстоятельства, способствовавшие заражению;
- информационные ресурсы, затронутые заражением;
- характер и размер реального и потенциального ущерба.

7.9. В ходе своей работы комиссия может запрашивать объяснительные записки от работников, подозреваемых в виновности заражения (путем письменного запроса их непосредственным руководителям). Объяснительная записка должна быть представлена комиссии в течение 3 (трех) рабочих дней с момента поступления запроса. В случае отказа предоставить объяснительную записку, данный факт отражается в акте.

7.10. Уничтожение материалов расследования фактов заражения осуществляется в соответствии с установленными требованиями по делопроизводству и номенклатурой дел.

8. Ответственность

8.1. Пользователи и Ответственный за обеспечение безопасности ПДн в ИСПДн несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации. За несоблюдение требований законодательства Российской Федерации предусмотрена гражданская, уголовная, административная, дисциплинарная ответственность.

9. Срок действия и порядок внесения изменений

9.1. Настоящая Инструкция вступает в силу с момента его утверждения и действует бессрочно.

9.2. Настоящая Инструкция подлежит пересмотру не реже одного раза в три года.

9.3. Изменения и дополнения в настоящую Инструкцию вносятся приказом Директора Учреждения.

Приложение 4

к приказу МБУ ДО РР ДЮЦТ

от «19» марта 2021 г. № 18

ИНСТРУКЦИЯ

по организации резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации

в информационных системах персональных данных

МБУ ДО РР ДЮЦТ

1. Термины и определения

Автоматизированное рабочее место – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида;

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

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;

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

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

Пользователь информационной системы персональных данных – работник, осуществляющий обработку персональных данных в информационной системе персональных данных;

Средство антивирусной защиты – программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации;

Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенные или используемые для защиты информации.

2. Общие положения

2.1. Настоящая Инструкция по организации резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных МБУ ДО РР ДЮЦТ (далее – Инструкция) устанавливает основные требования к организации резервного копирования (восстановления) программ и данных, хранящихся в базах данных информационных систем персональных данных (далее – ИСПДн) МБУ ДО РР ДЮЦТ (далее – Учреждение), а также к резервированию аппаратных средств.

2.2. Настоящая Инструкция разработана с целью:

- определения категории информации, подлежащей обязательному резервному копированию;
- определения процедуры резервирования данных для последующего восстановления работоспособности ИСПДн при полной или частичной потере информации, вызванной сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);
- определения порядка восстановления информации в случае возникновения такой необходимости;
- упорядочения работы и определения ответственности должностных лиц, связанной с резервным копированием и восстановлением информации.

2.3. Действие настоящей Инструкции распространяется на всех пользователей ИСПДн Учреждения, а также на основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения технических средств;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;

2.4. Под резервным копированием информации понимается создание избыточных копий защищаемой информации в электронном виде для быстрого восстановления работоспособности ИСПДн в случае возникновения аварийной ситуации, повлекшей за собой повреждение или утрату данных.

2.5. Резервному копированию подлежит информация следующих основных категорий:

- информация, обрабатываемая пользователями в ИСПДн, а также информация, необходимая для восстановления работоспособности ИСПДн, в т.ч. систем управления базами данных (далее – СУБД) общего пользования и справочно-информационных систем общего использования;
- рабочие копии установочных компонентов программного обеспечения общего назначения и специализированного программного обеспечения серверов и рабочих станций;
- информация, необходимая для восстановления серверов и систем управления базами данных ИСПДн, локальной вычислительной сети, системы электронного документооборота;
- регистрационная информация систем защиты информации;
- другая информация ИСПДн, по мнению пользователей, администраторов ИСПДн и ответственного за обеспечение безопасности персональных данных

(далее – ПДн) в ИСПДн, являющаяся критичной для работоспособности ИСПДн.

2.6. Настоящая Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности сведений конфиденциального характера, в том числе и ПДн, и не исключает обязательного выполнения их требований.

3. Общие требования к резервному копированию

3.1. В Инструкции резервного копирования описываются действия при выполнении следующих мероприятий:

- резервное копирование с указанием конкретных резервируемых данных и аппаратных средств (в случае необходимости);
- контроль резервного копирования;
- хранение резервных копий;
- полное или частичное восстановление данных.

3.2. Архивное копирование резервируемой информации производится при помощи специализированных программно-аппаратных систем резервного копирования. Система резервного копирования должна обеспечить производительность, достаточную для сохранения информации, указанной в п. 2.5, в установленные сроки и с заданной периодичностью.

3.3. Требования к техническому обеспечению систем резервного копирования:

- комплекс взаимосвязанных технических средств на единой технологической платформе, обеспечивающих процессы сбора, передачи, обработки и хранения информации;
- имеет возможность расширения (замены) состава технических средств, входящих в комплекс, для улучшения их эксплуатационно-технических характеристик по мере возрастания объемов обрабатываемой информации;
- обеспечивает выполнение функций, перечисленных в п. 3.1.

3.4. Требования к программному обеспечению систем резервного копирования:

- лицензионное системное программное обеспечение и программное обеспечение резервного копирования;
- программное обеспечение резервного копирования обеспечивает простоту процесса инсталляции, конфигурирования и сопровождения.

3.5. Хранение отдельных магнитных носителей архивных копий организуется в отдельном хранилище. Физический доступ к архивным копиям строго ограничен.

3.6. Доступ к носителям архивных копий имеют только уполномоченные сотрудники, которые несут персональную ответственность за сохранность архивных копий и невозможность ознакомления с ними лиц, не имеющих на то полномочий.

3.7. Уничтожение отделяемых магнитных носителей архивных копий производится установленным порядком в случае прихода их в негодность или замены типа носителя с обязательным составлением акта об уничтожении.

4. Ответственность за состояние резервного копирования

4.1. Ответственность за контроль над своевременным осуществлением резервного копирования и соблюдением соответствующей Инструкции, а также за выполнением требований по хранению архивных копий и предотвращению несанкционированного

доступа к ним возлагается на ответственного за обеспечение безопасности ПДн в ИСПДн и администраторов ИСПДн.

4.2. В случае обнаружения попыток несанкционированного доступа к носителям архивной информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, сообщается ответственному за обеспечение безопасности ПДн в ИСПДн в течение рабочего дня после обнаружения указанного события.

5. Периодичность резервного копирования

5.1. Резервное копирование специализированного программного обеспечения производится при его получении (если это предусмотрено инструкцией по его применению и не противоречит условиям его распространения), а также при его обновлении и получении исправленных и обновленных версий.

5.2. Резервное копирование открытой информации делается не позднее чем через сутки после ее изменения, но не реже одного раза в месяц.

5.3. Информация, содержащаяся в постоянно изменяемых базах данных, сохраняется в соответствии со следующим графиком:

- ежемесячно производится резервное копирование на специально выделенный носитель длительного хранения, информация на котором хранится постоянно.

5.4. Не реже одного раза в год на носители длительного хранения записывается информация, не относящаяся к постоянно изменяемым базам данных (приказы, распоряжения, открытые издания и т.д.).

6. Восстановление информации из резервных копий

6.1. В случае необходимости, восстановление данных из резервных копий производится ответственными сотрудниками.

6.2. Восстановление данных из резервных копий происходит в случае ее исчезновения или нарушения вследствие несанкционированного доступа в систему, воздействия вирусов, программных ошибок, ошибок работников и аппаратных сбоев.

6.3. Восстановление системного программного обеспечения и программного обеспечения общего назначения производится с их носителей в соответствии с инструкциями производителя.

6.4. Восстановление специализированного программного обеспечения производится с дистрибутивных носителей или их резервных копий в соответствии с инструкциями по установке или восстановлению данного программного обеспечения.

6.5. Восстановление информации, не относящейся к постоянно изменяемым базам данных, производится с резервных носителей. При этом используется последняя копия информации.

6.6. При частичном нарушении или исчезновении записей баз данных восстановление производится с последней ненарушенной ежедневной копии. Полностью информация восстанавливается с последней еженедельной копии, которая затем дополняется ежедневными частичными резервными копиями.

7. Срок действия и порядок внесения изменений

7.1. Настоящая Инструкция вступает в силу с момента ее утверждения и действует бессрочно.

7.2. Настоящая Инструкция подлежит пересмотру не реже одного раза в три года.

7.3. Изменения и дополнения в настоящую Инструкцию вносятся приказом директора Учреждения.

Приложение 5

к приказу МБУ ДО РР ДЮЦТ

от «19» марта 2021 г. № 18

ПОРЯДОК

обращения со съемными машинными носителями персональных данных

в МБУ ДО РР ДЮЦТ

1. Термины и определения

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

Съемный машинный носитель персональных данных – сменный носитель персональных данных, предназначенный для записи и считывания персональных данных, представленных в стандартных кодах;

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;

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

Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

2.1. Настоящий Порядок обращения со съемными машинными носителями персональных данных в МБУ ДО РР ДЮЦТ (далее – Порядок), разработан в соответствии с законодательством Российской Федерации о персональных данных (далее – ПДн) и нормативно-методическими документами исполнительных органов государственной власти по вопросам безопасности ПДн при их обработке в информационных системах персональных данных (далее – ИСПДн).

2.2. Настоящий Порядок определяет:

- правила обращения со съемными машинными носителями информации, в том числе и ПДн (далее – СМНИ);
- порядок организации учета СМНИ;
- порядок уничтожения СМНИ.

2.3. Под СМНИ в настоящем Порядке понимаются следующие носители информации:

- оптические диски (CD, DVD) однократной и многократной записи;
- электронные накопители информации (флэш-память, съемные жесткие диски);
- иные носители информации.

2.4. Требования настоящего Порядка являются обязательными для исполнения всеми работниками МБУ ДО РР ДЮЦТ (далее – Учреждение), использующими в своей работе СМНИ.

2.5. Все работники Учреждения, использующие СМНИ, должны быть ознакомлены с требованиями настоящим Порядком под подпись.

2.6. Настоящий Порядок является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности сведений конфиденциального характера, в том числе и ПДн, и не исключает обязательного выполнения их требований.

3. Правила обращения со съемными машинными носителями персональных данных

3.1. Обращение со СМНИ должно осуществляется таким образом, чтобы исключались их утрата, порча и несанкционированный доступ к ним посторонних лиц.

3.2. При обращении со СМНИ, выполняются следующие основные правила:

- СМНИ учитываются и выдаются под подпись;
- СМНИ, срок эксплуатации которых истек, уничтожаются в установленном порядке;
- для выноса СМНИ за пределы контролируемой зоны, запрашивается специальное разрешение у ответственного за обеспечение безопасности ПДн в ИСПДн (далее – Ответственный), а факт выноса фиксируется;
- право на перемещение СМНИ за пределы контролируемой зоны, имеют только те лица, которым оно необходимо для выполнения своих должностных обязанностей (функции);
- все СМНИ должны хранится в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособленными для опечатывания замочных скважин или кодовыми замками;
- допускается хранение СМНИ вне сейфов (металлических шкафов) при условиях уничтожения (стирания) ПДн и остаточной информации (информации, которую можно восстановить после удаления с помощью нештатных средств и методов) с использованием средств стирания данных и остаточной информации, либо если на съемном машинном носителе ПДн хранятся только ПДн в зашифрованном виде с использованием средств криптографической защиты информации.

3.3. СМНИ должен использоваться, не более срока эксплуатации, установленного изготовителем материального носителя.

4. Порядок хранения и учета съемных машинных носителей персональных данных

4.1. СМНИ, должны иметь специальную маркировку. Тип маркировки выбирается Ответственным.

4.2. Все находящиеся на хранении и в обращении СМНИ учитываются Ответственным в «Журнале учета съемных машинных носителей персональных данных в МБУ ДО РР ДЮЦТ», форма которого установлена в Приложении 1 к настоящему Порядку.

4.3. В нерабочее время и время отсутствия необходимости использования ПДн СМНИ должны храниться в хранилищах СМНИ.

4.4. Перечень хранилищ определяется в «Журнале учета хранилищ носителей персональных данных в МБУ ДО РР ДЮЦТ».

4.5. Пользователи для выполнения работ получают СМНИ у Ответственного. При получении делаются соответствующие записи в «Журнале учета съемных машинных носителей персональных данных в МБУ ДО РР ДЮЦТ.

5. Порядок уничтожения съемных машинных носителей персональных данных

5.1. Уничтожение ПДн производится только в следующих случаях:

- обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом;
- ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки;
- в случае выявления неправомерной обработки ПДн, если обеспечить правомерность обработки ПДн невозможно;
- в случае достижения цели обработки ПДн;
- в случае отзыва субъектом ПДн согласия на обработку его ПДн и в случае, если сохранение ПДн более не требуется для целей обработки ПДн.

5.2. СМНИ, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению.

5.3. Уничтожение СМНИ осуществляется комиссией по уничтожению, назначенной приказом Директора Учреждения.

5.4. При уничтожении СМНИ необходимо:

- убедиться в необходимости уничтожения СМНИ;
- убедиться в том, что уничтожаются только та информация, которая предназначена для уничтожения;
- уничтожить СМНИ подходящим способом, в соответствии с настоящим Порядком или способом, указанным в соответствующем требовании или распорядительном документе.

5.5. При уничтожении СМНИ применяются следующие способы:

- измельчение в бумагорезательной (бумагоуничтожительной) машине – для документов, исполненных на бумаге;
- тщательное вымарывание (с проверкой тщательности вымарывания) информации, подлежащей уничтожению – для сохранения возможности обработки иных данных, зафиксированных в документе;
- измельчение в специальной мультирезательной (мультиуничтожительной) машине или физическое уничтожение (разрушение) носителей информации – для СМНИ на оптических дисках;
- физическое уничтожение частей СМНИ – разрушение или сильная деформация – для носителей информации на жестком магнитном диске (уничтожению подлежат внутренние диски и микросхемы); SSD-дисках, USB- и Flash-

носителях (уничтожению подлежат модули и микросхемы долговременной памяти);

- стирание с помощью сертифицированных средств уничтожения информации – для записей в базах данных и отдельных документов на машинном носителе.

5.6. По результатам уничтожения СМНИ комиссией составляется «Акт уничтожения съемных машинных носителей персональных данных», форма которого установлена в Приложении 2 к настоящему Порядку.

6. Ответственность

6.1. Ответственным за хранение, учет и выдачу СМНИ, является Ответственный.

6.2. Все работники Учреждения, использующие СМНИ и Ответственный, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящим Порядком, в пределах, определенных действующим законодательством Российской Федерации. За несоблюдение требований законодательства Российской Федерации предусмотрена гражданская, уголовная, административная, дисциплинарная ответственность.

7. Срок действия и порядок внесения изменений

7.1. Настоящий Порядок вступает в силу с момента его утверждения и действует бессрочно.

7.2. Настоящий Порядок подлежит пересмотру не реже одного раза в три года.

7.3. Изменения и дополнения в настоящий Порядок вносятся приказом директора Учреждения.

Приложение 1

к порядку обращения со съемными машинными носителями персональных данных в МБУ ДО РР ДЮЦТ

ФОРМА

Журнал учета съемных машинных носителей персональных данных

в МБУ ДО РР ДЮЦТ

№ п/п	Тип носителя	Номер (серийный/ инвентарный)	Расписка в получении			Подпись ответственного лица	Место хранения	Примечание	Дата и номер акта уничтожения
			ФИО	Дата	Подпись				
1	2	3	4	5	6	7	8	9	10

Приложение 2

к порядку обращения со съемными машинными носителями персональных данных в МБУ ДО РР ДЮЦТ

ФОРМА

АКТ

«___» _____ 20__ г. № _____

Рязань

Об уничтожении съемных машинных

носителей персональных данных

Комиссия в составе:

Председатель:

_____ _____

Члены комиссии:

1. _____ _____
2. _____ _____
3. _____ _____

составили настоящий акт о том, что в результате проведенной экспертной оценки подлежат уничтожению следующие съемные машинные носители персональных данных:

№ п/п	Дата окончания срока обработки зафиксированных на носителе персональных данных	Учетный номер съемного носителя или наименование технического средства, на котором уничтожаются файлы	Примечание
1	2	3	4

Всего съемных носителей_____

(цифрами и прописью)

Перечисленные съемные носители уничтожены путем _____

_____

.

(механического уничтожения, сжигания, разрезания, деформирования и т.п.)

Председатель:

_____ _____ _____

Члены комиссии:

_____ _____ _____

_____ _____ _____

_____ _____ _____

УПРАВЛЕНИЕ ОБРАЗОВАНИЯ И МОЛОДЕЖНОЙ ПОЛИТИКИ
АДМИНИСТРАЦИИ РЫБНОВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА РЯЗАНСКОЙ ОБЛАСТИ
Муниципальное бюджетное учреждение дополнительного образования
«Рыбновский районный
Детско-юношеский Центр туризма»

391110, Рязанская область,
г. Рыбное, Набережный
пер., д.2

тел. (49137) 52-2-60,

ПРИКАЗ

«19» марта 2021 г. № 19

Об утверждении регламента реагирования на инциденты информационной безопасности в информационных системах персональных данных

Во исполнение требований Федерального закона №152-ФЗ от 27.07.2006 «О персональных данных», приказа 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» и прочих нормативных документов по защите информации,

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие Регламент реагирования на инциденты информационной безопасности в информационных системах персональных данных МБУ ДО РР ДЮЦТ (далее – Регламент) (Приложение к настоящему Приказу).

2. Требования прилагаемого Регламента довести до работников, непосредственно осуществляющих защиту персональных данных в информационных системах персональных данных.

3. Контроль за исполнением настоящего приказа оставляю за собой.

Директор С.В.Новиков

Приложение
к приказу МБУ ДО РР ДЮЦТ
от «19» марта 2021 г. № 19

РЕГЛАМЕНТ
реагирования на инциденты информационной безопасности в информационных системах персональных данных

МБУ ДО РР ДЮЦТ

1. Термины и определения

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

Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность. Инцидентами информационной безопасности являются:

a. утрата услуг, оборудования или устройств;
b. системные сбои или перегрузки;
c. ошибки пользователей;
d. несоблюдение политики или рекомендаций по информационной безопасности;
e. нарушение физических мер защиты;
f. неконтролируемые изменения систем;
g. сбои программного обеспечения и отказы технических средств;
h. нарушение правил доступа.

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;

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

Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

2.1. Настоящий Регламент реагирования на инциденты информационной безопасности в информационных системах персональных данных МБУ ДО РР ДЮЦТ (далее – Регламент), разработан в соответствии с законодательством Российской Федерации о персональных данных (далее – ПДн) и нормативно-методическими документами федеральных органов исполнительной власти по вопросам безопасности ПДн при их обработке в информационных системах персональных данных (далее – ИСПДн).

2.2. Настоящий Регламент определяет:

- порядок регистрации событий безопасности;
- порядок выявления инцидентов информационной безопасности и реагированию на них;
- порядок проведения анализа инцидентов информационной безопасности, в том числе определение источников и причин возникновения инцидентов.

2.3. Регламент обязателен для исполнения всеми работниками МБУ ДО РР ДЮЦТ (далее – Учреждение), непосредственно осуществляющими защиту ПДн в ИСПДн.

3. Порядок регистрации событий безопасности

3.1. Событием информационной безопасности является состояние системы, сервиса или сети, которое свидетельствует о возможном нарушении принятых мер по защите ПДн, либо о прежде неизвестной ситуации, которая может иметь отношение к безопасности.

3.2. Регистрация событий безопасности в ИСПДн осуществляется в следующей последовательности:

1) Определение событий безопасности, подлежащих регистрации, и сроков их хранения;
2) Определение состава и содержания информации о событиях безопасности, подлежащих регистрации;
3) Сбор, запись и хранение информации о событиях безопасности;
4) Реагирование на сбои при регистрации событий безопасности;
5) Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них;
6) Генерирование временных меток и (или) синхронизация системного времени в ИСПДн;
7) Защита информации о событиях безопасности.

3.3. События безопасности, подлежащие регистрации в ИСПДн, должны определяться с учетом способов реализации угроз безопасности ПДн для ИСПДн. К событиям безопасности, подлежащим регистрации в ИСПДн, должны быть отнесены любые проявления состояния ИСПДн и ее системы защиты, указывающие на возможность нарушения конфиденциальности, целостности или доступности ПДн, доступности компонентов ИСПДн, нарушения процедур, установленных организационно-распорядительными документами по защите ПДн, а также на нарушение штатного функционирования средств защиты информации (далее – СЗИ).

3.4. События безопасности, подлежащие регистрации в ИСПДн, и сроки хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов информационной безопасности, возникших в ИСПДн.

3.5. В ИСПДн подлежат регистрации следующие события:

- вход (выход), а также попытки входа субъектов доступа в ИСПДн и загрузки (остановка) операционной системы;
- ошибки при регистрации в информационной системе: ввод неправильных персональных регистрационных данных (пароля, имени пользователя и т.п.) более трех раз подряд (однократная);
- очистка журналов событий безопасности ИСПДн;

- подключение съемных машинных носителей ПДн и вывод ПДн на съемные машинные носители;
- запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой ПДн;
- обновление или ошибки при обновлении программных средств ИСПДн и СЗИ;
- попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;
- попытки удаленного доступа.

3.6. Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны, как минимум, обеспечить возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъекта доступа (пользователя и (или) процесса), связанного с данным событием безопасности.

3.7. При регистрации входа (выхода) субъектов доступа в ИСПДн и загрузки (остановка) операционной системы состав и содержание информации должны, как минимум, включать дату и время входа (выхода) в систему (из системы) или загрузки (остановки) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.

3.8. При регистрации подключения съемных машинных носителей ПДн и вывода ПДн на съемные носители состав и содержание регистрационных записей должны, как минимум, включать дату и время подключения съемных машинных носителей ПДн и вывода ПДн на съемные носители, логическое имя (номер) подключаемого съемного машинного носителя ПДн, идентификатор субъекта доступа, осуществляющего вывод ПДн на съемный носитель ПДн.

3.9. При регистрации запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой ПДн состав и содержание регистрационных записей должны, как минимум, включать дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).

3.10. При регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам состав и содержание регистрационных записей должны, как минимум, включать дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип).

3.11. При регистрации попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей) состав и содержание информации должны, как минимум, включать дату и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого объекта доступа (логическое имя (номер).

3.12. При регистрации попыток удаленного доступа к ИСПДн состав и содержание информации должны, как минимум, включать дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к ИСПДн.

3.13. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения должен предусматривать:

- возможность выбора Ответственным за обеспечение безопасности ПДн в ИСПДн и (или) Администратором ИСПДн событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности, определенных в пункте 3.4 настоящего Регламента;
- генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с составом и содержанием информации, определенными в соответствии с пунктами 3.6 – 3.11 настоящего Регламента;
- хранение информации о событиях безопасности в течение времени, установленного в пункте 3.3 настоящего Регламента.

3.14. Объем памяти для хранения информации о событиях безопасности должен быть рассчитан и выделен с учетом типов событий безопасности, подлежащих регистрации в соответствии с составом и содержанием информации о событиях безопасности, подлежащих регистрации, в соответствии с пунктами 3.7 – 3.11 настоящего Регламента, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности.

3.15. В ИСПДн должно осуществляться реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти.

3.16. Реагирование на сбои при регистрации событий безопасности должно предусматривать:

- предупреждение (сигнализация, индикация) о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности;
- реагирование на сбои при регистрации событий безопасности путем изменения Ответственным за обеспечение безопасности ПДн в ИСПДн и (или) Администратором ИСПДн параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов ИСПДн, запись поверх устаревших хранимых записей событий безопасности.

3.17. Мониторинг (просмотр и анализ) записей регистрации (аудита) должен проводиться для всех событий, подлежащих регистрации в соответствии и с периодичностью, установленной оператором, и обеспечивающей своевременное выявление признаков инцидентов информационной безопасности в ИСПДн.

3.18. В случае выявление признаков инцидентов информационной безопасности в ИСПДн осуществляется планирование и проведение мероприятий по реагированию на

выявленные инциденты безопасности в соответствии с порядком проведения разбирательств по фактам возникновения инцидентов в ИСПДн.

3.19. Получение меток времени, включающих дату и время, используемых при генерации записей регистрации (аудита) событий безопасности в ИСПДн, достигается посредством применения внутренних системных часов ИСПДн.

3.20. Защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

3.21. Доступ к записям аудита и функциям управления механизмами регистрации (аудита) должен предоставляться только уполномоченным должностным лицам:

- ответственному за обеспечение безопасности ПДн в ИСПДн;
- администратору ИСПДн.

4. Порядок выявления инцидентов информационной безопасности и реагирования на них

4.1. За выявление инцидентов информационной безопасности и реагирование на них отвечают:

- ответственный за обеспечение безопасности ПДн в ИСПДн;
- администратор ИСПДн.

4.2. Работники Учреждения, должны сообщать ответственным за выявление инцидентов информационной безопасности о любых инцидентах, в которые входят:

- факты попыток и успешной реализации несанкционированного доступа в ИСПДн, в помещения, в которых осуществляется обработка ПДн, и к хранилищам ПДн;
- факты сбоя или некорректной работы систем обработки ПДн;
- факты сбоя или некорректной работы СЗИ;
- факты разглашения ПДн;
- факты разглашения информации о методах и способах защиты и обработки ПДн.

4.3. Все нештатные ситуации, факты вскрытия и опечатывания технических средств, выполнения профилактических работ, установки и модификации аппаратных и программных средств обработки ПДн в ИСПДн должны быть занесены ответственными за выявление инцидентов информационной безопасности в «Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания технических средств, выполнения профилактических работ, установки и модификации аппаратных и программных средств обработки персональных данных в МБУ ДО РР ДЮЦТ, форма которого установлена в Приложении 1 к настоящему Регламенту или в электронные журналы операционной системы и СЗИ.

4.4. Анализ инцидентов информационной безопасности, в том числе определение источников и причин возникновения инцидентов, осуществляется согласно порядку проведения разбирательств по фактам возникновения инцидентов информационной безопасности в ИСПДн (пункт 5 настоящего Регламента).

4.5. Меры по устранению последствий инцидентов информационной безопасности, планированию и принятию мер по предотвращению повторного возникновения

инцидентов, возлагаются на ответственных за выявление инцидентов информационной безопасности.

5. Порядок проведения разбирательств по фактам возникновения инцидентов информационной безопасности

5.1. Для проведения разбирательств по фактам возникновения инцидентов информационной безопасности приказом Директора Учреждения создаётся комиссия, состоящая не менее чем из трех человек с обязательным включением в её состав:

- ответственного за обеспечение безопасности ПДн в ИСПДн;
- администратора ИСПДн.

5.2. Председатель комиссии организует работу комиссии, решает вопросы взаимодействия комиссии с руководителями и работниками структурных подразделений организации, готовит и ведёт заседания комиссии, подписывает протоколы заседаний. По окончании работы комиссии готовится заключение по результатам проведённого разбирательства, которое передается на рассмотрение Директору Учреждения.

5.3. При проведении разбирательства устанавливаются:

- наличие самого факта совершения инцидента информационной безопасности, служащего основанием для вынесения соответствующего решения;
- время, место и обстоятельства возникновения инцидента, а также оценка его последствий;
- конкретный работник, совершивший инцидент информационной безопасности или повлекший своими действиями возникновения инцидента;
- наличие и степень вины работника, совершившего инцидент информационной безопасности или повлекшего своими действиями возникновения инцидента;
- цели и мотивы, способствовавшие совершению инцидента информационной безопасности.

5.4. В целях проведения разбирательства все работники Учреждения обязаны по первому требованию членов комиссии предъявить для проверки все числящиеся за ними материалы и документы, дать устные или письменные объяснения об известных им фактах по существу заданных им вопросов.

5.5. Работник, совершивший инцидент информационной безопасности или повлекший своими действиями возникновения инцидента, обязан по требованию комиссии представить объяснения в письменной форме не позднее трех рабочих дней с момента получения соответствующего требования. Комиссия вправе поставить перед работником перечень вопросов, на которые работник обязан ответить. В случае отказа работника от письменных объяснений, комиссией составляется акт.

5.6. Работник имеет право, по согласованию с председателем комиссии, знакомиться с материалами разбирательства, касающимися лично его, и давать по поводу них свои комментарии, предоставлять дополнительную информацию и документы. По окончании разбирательства работнику для ознакомления предоставляется итоговый акт с выводами комиссии.

5.7. В случае давления на работника со стороны других лиц (не из состава комиссии) в виде просьб, угроз, шантажа и др., по вопросам, связанным с проведением разбирательства, работник обязан сообщить об этом председателю комиссии.

5.8. До окончания работы комиссии и вынесения решения членам комиссии запрещается разглашать сведения о ходе проведения разбирательства и ставшие известные им обстоятельства.

5.9. В процессе проведения разбирательства комиссией выясняются:

- перечень разглашенных ПДн;
- причины разглашения ПДн;
- лица, виновные в разглашении ПДн;
- размер (экспертную оценку) причиненного ущерба;
- недостатки и нарушения, допущенные работниками при работе с ПДн;
- иные обстоятельства, необходимые для определения причин разглашения ПДн, степени виновности отдельных лиц, возможности применения к ним мер воздействия.

5.10. По завершении разбирательства комиссией составляется заключение. В заключении указываются:

- основание для проведения в разбирательства;
- состав комиссии и время проведения разбирательства;
- сведения о времени, месте и обстоятельствах возникновения инцидента информационной безопасности;
- сведения о работнике, совершившем инцидент информационной безопасности или повлекшем своими действиями возникновения инцидента (должность, фамилия, имя, отчество, год рождения, время работы в Учреждении, а также в занимаемая должность);
- цели и мотивы работника, способствовавшие совершению инцидента информационной безопасности;
- причины и условия возникновения инцидента информационной безопасности;
- данные о характере и размерах причиненного в результате инцидента ущерба;
- предложения о мере ответственности работника, совершившего инцидент информационной безопасности или повлекшего своими действиями возникновения инцидента.

5.11. На основании заключения выносится решение о применении мер ответственности к работнику, совершившему инцидент или повлекшему своими действиями возникновению инцидента, также о возмещении ущерба виновным работником (или его законным представителем), которое доводится до указанного работника в письменной форме под расписку.

5.12. Все материалы разбирательства относятся к информации ограниченного доступа и хранятся в течение 5 лет. Копии заключения и распоряжения по результатам разбирательства приобщаются к личному делу работника, в отношении которого оно проводилось.

6. Ответственность

6.1. Все работники, осуществляющие защиту персональных данных, обязаны ознакомиться с данным Регламентом под подпись.

6.2. Работники несут персональную ответственность за выполнение требований настоящего Регламента.

7. Срок действия и порядок внесения изменений

7.1. Настоящий Регламент вступает в силу с момента его утверждения и действует бессрочно.

7.2. Настоящий Регламент подлежит пересмотру не реже одного раза в три года.

7.3. Изменения и дополнения в настоящий Регламент вносятся приказом директора Учреждения

Приложение 1

к Регламенту реагирования на инциденты информационной безопасности в информационных системах персональных данных МБУ ДО РР ДЮЦТ

ФОРМА

Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания технических средств, выполнения профилактических работ, установки и модификации аппаратных и программных средств обработки персональных данных

в МБУ ДО РР ДЮЦТ

№ п/п	Дата	Краткое описание выполненной работы (нештатной ситуации)	ФИО Ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных, подпись	ФИО Администратора информационной системы, подпись	Примечание
1	2	3	4	5	6

УПРАВЛЕНИЕ ОБРАЗОВАНИЯ И МОЛОДЕЖНОЙ ПОЛИТИКИ
АДМИНИСТРАЦИИ РЫБНОВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА РЯЗАНСКОЙ ОБЛАСТИ
Муниципальное бюджетное учреждение дополнительного образования
«Рыбновский районный
Детско-юношеский Центр туризма»

391110, Рязанская область,
г. Рыбное, Набережный
пер., д.2

тел. (49137) 52-2-60,

ПРИКАЗ

«19» марта 2021 г. № 20

О разрешительной системе доступа

Во исполнение требований Федерального закона Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», приказа 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» и прочих нормативных документов по защите информации, ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие Положение о разрешительной системе доступа в информационных системах персональных данных МБУ ДО РР ДЮЦТ (далее – Положение) (Приложение 1 к настоящему Приказу).

2. Утвердить и ввести в действие Матрицу доступа работников к ресурсам информационных систем персональных данных МБУ ДО РР ДЮЦТ (Приложение 2 к настоящему Приказу).

3. Администратору информационной системы персональных данных МБУ ДО РР ДЮЦТ своевременно осуществлять подготовку предложений по внесению изменений в Матрицу доступа работников к ресурсам информационных систем персональных данных МБУ ДО РР ДЮЦТ.

4. Требования Положения довести до работников, непосредственно осуществляющих обработку и защиту персональных данных в информационных системах МБУ ДО РР ДЮЦТ.

5. Контроль за исполнением приказа оставляю за собой.

Директор С.В.Новиков

Приложение 1

к приказу МБУ ДО РР ДЮЦТ

от «19» марта 2021 г. № 20

ПОЛОЖЕНИЕ
о разрешительной системе доступа в

информационных системах персональных данных
МБУ ДО РР ДЮЦТ

8. Основные термины и определения

Дискреционный метод управления доступом – метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе идентификационной информации субъекта и для каждого объекта доступа – списка, содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа;

Доступ к информации - ознакомление с информацией, ее обработка, в частности копирование, модификация или уничтожение информации;

Матрица доступа – таблица, отображающая правила разграничения доступа;

Объект доступа – единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа;

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа;

Ролевой метод управления доступом – метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа;

Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации;

Субъект доступа – лицо или процесс, действия которого регламентируются правилами разграничения доступа;

Типы доступа – операции, разрешенные к выполнению субъектом доступа при доступе к объектам доступа.

9. Общие положения

2.1. Настоящее Положение о разрешительной системе доступа в информационных системах персональных данных МБУ ДО РР ДЮЦТ (далее – Положение), разработано в соответствии с законодательством Российской Федерации о персональных данных (далее – ПДн) и нормативно-методическими документами исполнительных органов государственной власти по вопросам безопасности ПДн при их обработке в информационных системах персональных данных (далее – ИСПДн).

2.2. Настоящее Положение определяет методы управления доступом, типы доступа и правила разграничения доступа субъектов доступа к объектам доступа в ИСПДн.

2.3. Положение обязательно для исполнения всеми работниками ОГБУДО «ДЭБЦ» (далее – Учреждение), непосредственно осуществляющими защиту ПДн.

10. Субъекты и объекты доступа

3.1. К субъектам доступа ИСПДн, относятся работники, выполняющие свои должностные обязанности (функции) с использованием информации, информационных технологий и технических средств ИСПДн в соответствии с должностными инструкциями и которым в ИСПДн присвоены учетные записи.

3.2. К объектам доступа в ИСПДн, относятся:

- средства вычислительной техники;
- средства связи и передачи данных;
- средства обеспечения бесперебойной работы средств вычислительной техники и средств связи и передачи данных;
- основные конфигурационные файлы операционных систем, средств связи и передачи данных и средств защиты информации (далее – СЗИ);
- средства настройки и управления операционной системой, средств связи и передачи данных и СЗИ;
- прикладное программное обеспечение;
- периферийные устройства;
- машинные носители информации;
- обрабатываемые, хранимые данные.

11. Методы разграничения доступа

4.1. Методы разграничения доступа к ИСПДн реализуются в соответствии с особенностями функционирования ИСПДн и включают комбинацию следующих методов:

- ролевой метод управления доступом;
- дискреционный метод управления доступом.

4.2. Реализация ролевого метода управления доступом в ИСПДн представлена в таблице 1.

Таблица 1

№ п/п	Роль субъекта доступа	Уровень доступа к объектам доступа
1	Администратор	- обладает полной информацией о конфигурации ИСПДн (структуре ИСПДн, составе, местах установки и параметров программного обеспечения и технических средств); - обладает правами настройки и конфигурирования средств связи передачи данных; - обладает правами настройки и конфигурирования операционных систем и прикладного программного обеспечения.
2	Пользователь	- обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к ИСПДн.

4.3. Реализация дискреционного метода управления доступом достигается путем назначения прав доступа для каждой пары «Роль субъекта доступа» – «Объект доступа» явного и недвусмысленного перечисления допустимых типов доступа в соответствии с Матрицей доступа к информационным ресурсам (далее – Матрица доступа), форма которой установлена в Приложении к настоящему Положению.

12. Типы доступа

5.1. В ИСПДн определены следующие типы доступа субъектов доступа к объектам доступа:

- чтение (R) – субъекту доступа разрешено просматривать содержимое объекта доступа;
- запись (W) – субъекту доступа разрешено просматривать, записывать и создавать новый объект доступа;
- выполнение (E) – субъекту доступа разрешено запускать/выполнять объект доступа;
- печать (P) – субъекту доступа разрешена печать;
- сканирование (S) – субъекту доступа разрешено сканирование;
- полный (F) – субъект доступа имеет полный доступ к объектам доступа.

5.2. Разрешенные к выполнению, субъектами доступа при доступе к объектам доступа в ИСПДн, типы доступа, определены в Матрице доступа.

13. Правила разграничения доступа

6.1. В ИСПДн правила разграничения доступа реализованы совокупностью правил, регламентирующих порядок и условия доступа субъекта к объектам доступа в ИСПДн:

- разделение обязанностей и назначение минимально необходимых прав;
- управление (заведение, активация, блокирование и уничтожение) учетными записями Пользователей ИСПДн;
- управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками в ИСПДн;
- ограничение неуспешных попыток доступа в ИСПДн;
- разрешение (запрет) действий Пользователей ИСПДн, разрешенных до идентификации и аутентификации;
- реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети;
- контроль использования в ИСПДн технологий беспроводного доступа;
- контроль использования в ИСПДн мобильных технических средств;
- управление взаимодействием с ИСПДн организаций (внешние информационные системы).

6.2. Права и обязанности Пользователей зафиксированы в «Инструкции пользователя информационных систем персональных данных МБУ ДО РР ДЮЦТ».

6.3. Права и обязанности Администратора зафиксированы в «Инструкции администратора информационных систем персональных данных МБУ ДО РР ДЮЦТ».

6.4. Права и обязанности Администратора безопасности зафиксированы в «Инструкции ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных МБУ ДО РР ДЮЦТ».

6.5. Управление (заведение, активацию, блокирование и уничтожение) учетными записями Пользователей ИСПДн, осуществляет Администратор ИСПДн.

6.6. Администратор ИСПДн определяет и назначает права доступа субъектов к объектам доступа в ИСПДн в соответствии с исполняемой ролью субъекта в ИСПДн и Матрицей доступа.

6.7. В ИСПДн реализованы следующие функции управления учетными записями Пользователей ИСПДн:

- определение типа учетной записи (пользователь, администратор, системная);
- объединение учетных записей в группы (пользователи, администраторы);
- верификация пользователя при заведении учетной записи пользователя;
- заведение, активация, блокирование и уничтожение учетных записей Пользователей ИСПДн;
- пересмотр и корректировка учетных записей Пользователей ИСПДн;
- порядок заведения и контроля использования временных учетных записей Пользователей ИСПДн;
- оповещение Администратора ИСПДн, осуществляющего управление учетными записями Пользователей ИСПДн, об изменении сведений о Пользователях ИСПДн, их ролях, обязанностях, полномочиях, ограничениях;
- уничтожение временных учетных записей Пользователей ИСПДн, предоставленных для однократного (ограниченного по времени) выполнения задач в ИСПДн;
- предоставление Пользователям ИСПДн прав доступа к объектам доступа ИСПДн, основываясь на задачах, решаемых Пользователями ИСПДн.

6.8. Временная учетная запись может быть заведена для Пользователя ИСПДн на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям ИСПДн с временным доступом к ИСПДн).

6.9. В ИСПДн осуществляется автоматическое блокирование временных учетных записей Пользователей ИСПДн по окончании установленного периода времени для их использования.

6.10. При передаче информации между устройствами, сегментами в рамках ИСПДн, осуществляется управление информационными потоками, включающее:

- фильтрацию информационных потоков в соответствии с правилами управления потоками;
- разрешение передачи информации в ИСПДн только по установленному маршруту;
- изменение (перенаправление) маршрута передачи информации только в установленных случаях;
- запись во временное хранилище информации для анализа и принятия решения о возможности ее дальнейшей передачи в установленных случаях.

6.11. Управление информационными потоками обеспечивает разрешенный маршрут прохождения информации между Пользователями ИСПДн, устройствами, сегментами в рамках ИСПДн, а также при взаимодействии с сетью Интернет (или другими информационно-телекоммуникационными сетями международного информационного

обмена) на основе правил управления информационными потоками, включающих контроль конфигурации ИСПДн, источника и получателя передаваемой информации, структуры передаваемой информации, характеристик информационных потоков и (или) канала связи (без анализа содержания информации).

6.12. Управление информационными потоками блокирует передачу защищаемой информации через сеть Интернет (или другие информационно-телекоммуникационные сети международного информационного обмена) по незащищенным линиям связи, сетевые запросы и трафик, не санкционированно исходящие из ИСПДн и (или) входящие в ИСПДн.

6.13. В ИСПДн установлено и зафиксировано в «Инструкции по парольной защите информации в МБУ ДО РР ДЮЦТ:

- количество неуспешных попыток входа (доступа) ИСПДн за установленный период времени;
- блокирование сеанса доступа Пользователя ИСПДн после установленного времени его бездействия (неактивности).

6.14. В ИСПДн обеспечивается блокирование сеанса доступа Пользователя ИСПДн по запросу.

6.15. Для заблокированного сеанса осуществляется блокирование любых действий по доступу к информации и устройствам отображения, кроме необходимых для разблокирования сеанса.

6.16. Администратору ИСПДн и Ответственному за обеспечение безопасности ПДн в ИСПДн разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования ИПСДн в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

6.17. В ИСПДн в качестве мобильных технических средств рассматриваются съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства).

6.18. Регламентация и контроль использования съемных машинных носителей ПДн, описаны в «Порядке обращения со съемными машинными носителями персональных данных в МБУ ДО РР ДЮЦТ.

6.19. В ИСПДн при взаимодействии с внешними информационными системами, взаимодействие с которыми необходимо для функционирования ИСПДн, предоставление доступа к ИСПДн осуществляется только авторизованным (уполномоченным) Пользователям ИСПДн в соответствии с Матрицей доступа.

14. Ответственность

7.1. Все работники Учреждения, осуществляющие обработку и защиту ПДн обязаны ознакомиться с данным Положением под подпись.

7.2. Работники Учреждения несут персональную ответственность за выполнение требований настоящего Положения.

7.3. Контроль выполнения работниками Учреждения правил разграничения доступа в ИСПДн осуществляется Ответственным за обеспечение безопасности ПДн в ИСПДн.

15. Срок действия и порядок внесения изменений

8.1. Настоящее Положение вступает в силу с момента его утверждения и действует бессрочно.

8.2. Настоящее Положение подлежит пересмотру не реже одного раза в три года.

8.3. Изменения и дополнения в настоящее Положение вносятся приказом директора Учреждения.

Приложение

к Положению о разрешительной системе доступа в информационных системах персональных данных МБУ ДО РР ДЮЦТ

ФОРМА

Матрица доступа работников к ресурсам информационных систем персональных данных
МБУ ДО РР ДЮЦТ

Субъект доступа	Объект доступа								
	Основные конфигурационные файлы операционной системы	Средства настройки и управления операционной системой	Основные конфигурационные файлы средств защиты информации	Средства настройки и управления средств защиты информации	Прикладное программное обеспечение	Периферийные устройства	Съемные машинные носители информации	Обрабатываемые, хранимые данные	Настройки BIOS / UEFI
Администратор									
Пользователь									

Типы доступа:

- чтение (R) – субъекту доступа разрешено просматривать содержимое объекта доступа;
- запись (W) – субъекту доступа разрешено просматривать, записывать и создавать новый объект доступа;
- выполнение (E) - субъекту доступа разрешено запускать/выполнять объект доступа;
- печать (P) – субъекту доступа разрешена печать;
- сканирование (S) – субъекту доступа разрешено сканирование;
- полный (F) – субъект доступа имеет полный доступ к объектам доступа.

Приложение 2

к приказу МБУ ДО РР ДЮЦТ

от «19» марта 2021 г. № 20

Матрица доступа

субъектов к ресурсам информационных систем персональных данных
МБУ ДО РР ДЮЦТ

Субъект доступа	Объект доступа							
	Основные конфигурационные файлы операционной системы	Средства настройки и управления операционной системой	Основные конфигурационные файлы средств защиты информации	Средства настройки и управления средств защиты информации	Прикладное программное обеспечение	Периферийные устройства	Съемные машинные носители информации	Обрабатываем хранимые данные
Администратор	F	F	-	-	F	P/S	-	-
Пользователь	R-E	-	-	-	R-E	P/S	F	F

Типы доступа:

- чтение (R) – субъекту доступа разрешено просматривать содержимое объекта доступа;
- запись (W) – субъекту доступа разрешено просматривать, записывать и создавать новый объект доступа;
- выполнение (E) - субъекту доступа разрешено запускать/выполнять объект доступа;
- печать (P) – субъекту доступа разрешена печать;
- сканирование (S) – субъекту доступа разрешено сканирование;
- полный (F) – субъект доступа имеет полный доступ к объектам доступа.

УПРАВЛЕНИЕ ОБРАЗОВАНИЯ И МОЛОДЕЖНОЙ ПОЛИТИКИ
АДМИНИСТРАЦИИ РЫБНОВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА РЯЗАНСКОЙ ОБЛАСТИ

Муниципальное бюджетное учреждение дополнительного образования
«Рыбновский районный
Детско-юношеский Центр туризма»

391110, Рязанская область,
г. Рыбное, Набережный
пер., д.2

тел. (49137) 52-2-60,

ПРИКАЗ

«19» марта 2021 г. № 21

Об утверждении положения об организации обработки персональных данных без использования средств автоматизации.

Во исполнение требований Федерального закона №152-ФЗ от 27.07.2006 г. «О персональных данных» и «Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» утвержденного постановлением Правительства РФ № 687 от 15.09.2008 г., а также прочих нормативных документов по защите информации,

ПРИКАЗЫВАЮ:

4. Утвердить и ввести в действие Положение об организации обработки персональных данных, обрабатываемых в МБУ ДО РР ДЮЦТ без использования средств автоматизации (далее – Положение) (Приложение 1 к настоящему Приказу).
5. Ответственному за организацию обработки персональных данных ознакомить работников, осуществляющих обработку персональных данных без использования средств автоматизации, с прилагаемым Положением и Перечнем.
6. Контроль за исполнением настоящего Приказа оставляю за собой.

Директор С.В.Новиков

Приложение 1

к приказу МБУ ДО РР ДЮЦТ

от «19» марта 2021 г. № 21

ПОЛОЖЕНИЕ

об организации обработки персональных данных, обрабатываемых в

МБУ ДО РР ДЮЦТ

без использования средств автоматизации

1. Основные термины и определения

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

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

Основные технические средства и системы – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи персональных данных;

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;

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

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

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

2. Общие положения

2.1. Настоящее Положение об организации обработки персональных данных в МБУ ДО РР ДЮЦТ без использования средств автоматизации (далее – Положение), разработано в соответствии с законодательством Российской Федерации о персональных данных (далее – ПДн) и нормативными правовыми актами (методическими документами) федеральных органов исполнительной власти по вопросам безопасности ПДн.

2.2. Настоящее Положение определяет основные принципы обеспечения безопасности ПДн при их обработке без использования средств автоматизации, а также ответственность работников, участвующих в такой обработке.

2.3. Положение обязательно для исполнения всеми работниками МБУ ДО РР ДЮЦТ (далее – Учреждение), непосредственно участвующими в обработке ПДн без использования средств автоматизации.

3. Обеспечение безопасности персональных данных

3.1. ПДн при их неавтоматизированной обработке должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях ПДн, в специальных разделах или на полях форм.

3.2. Не допускается хранение ПДн различных категорий на одном материальном носителе.

3.3. Не допускается фиксация на одном бумажном носителе ПДн, цели обработки которых заведомо не совместимы.

3.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее – Типовая форма), должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы должны содержать сведения о цели обработки ПДн, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки ПДн;
- типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на неавтоматизированную обработку ПДн, при необходимости получения письменного согласия на обработку ПДн;
- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПДн, имел возможность ознакомиться со своими ПДн, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн;
- типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых, заведомо не совместимы.

3.5. Должно обеспечиваться раздельное хранение материальных носителей, содержащих ПДн, обработка которых осуществляется в различных целях.

3.6. При несовместимости целей неавтоматизированной обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн, должны быть приняты меры по обеспечению раздельной обработки ПДн, в частности:

- при необходимости использования или распространения определенных ПДн отдельно от находящихся на том же материальном носителе других ПДн, осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, используется (распространяется) копия ПДн;
- при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.

3.7. Необходимо принимать организационные (охрана помещений) и технические меры, исключающие возможность несанкционированного доступа к материальным носителям ПДн.

3.8. Учреждение не передает материальные носители персональных данных любым лицам, без письменного согласия субъектов ПДн, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта ПДн, а также в иных случаях, предусмотренных законодательством Российской Федерации.

3.9. При передаче материальных носителей, содержащих ПДн, третьей стороне должны быть приняты меры, исключающие возможность несанкционированного доступа к ПДн.

3.10. При передаче материальных носителей, содержащих ПДн, третьей стороне должно быть подготовлено сопроводительное письмо, в котором зафиксирован состав передаваемых материальных носителей, с указанием количества страниц для бумажных носителей, с указанием степени конфиденциальности (если необходимо).

3.11. О факте передачи/приема материальных носителей, содержащих ПДн, делаются соответствующие записи в журналах учета исходящей/входящей корреспонденции.

3.12. При приеме материальных носителей, содержащих ПДн, должны быть приняты меры, обеспечивающие их сохранность. При приеме бумажных носителей работа с такими носителями должна быть организована, в соответствии с принципом конфиденциального делопроизводства, действующего в Учреждении.

4. Хранение персональных данных

4.1. При хранении материальных носителей ПДн должны соблюдаться условия, обеспечивающие сохранность ПДн, исключающие несанкционированный к ним доступ.

4.2. Материальные носители ПДн должны храниться в пределах контролируемой зоны.

4.3. Территория контролируемой зоны определяется приказом Директора Учреждения.

4.4. Запрещен вынос или копирование носителей ПДн.

4.5. В нерабочее время и время отсутствия необходимости использования ПДн материальные носители ПДн должны храниться в хранилищах материальных носителей ПДн.

4.6. Перечень хранилищ определяется в «Журнале учета хранилищ носителей персональных данных в МБУ ДО РР ДЮЦТ, форма которого установлена в Приложении 1 к настоящему Положению.

5. Уничтожение персональных данных

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

5.2. Уничтожение носителей ПДн осуществляется в течение 30 дней с момента отзыва субъектом ПДн согласия на обработку ПДн (если более короткий срок не предусмотрен соответствующим договором, стороной которого является Учреждение) или истечения сроков обработки ПДн, в том числе хранения в архивах.

5.3. Уничтожением бумажных носителей ПДн занимается комиссия по организации работ по защите ПДн, создаваемая приказом Директора Учреждения.

5.4. Бумажные носители ПДн (документы, их копии, выписки), уничтожаются путём измельчения на мелкие части, исключающие возможность последующего восстановления информации, или сжигаются.

5.5. По окончании уничтожения бумажных носителей ПДн комиссией составляется «Акт об уничтожении бумажных носителей персональных данных», форма которого установлена в Приложении 2 к настоящему Положению.

5.6. Комиссия составляет и подписывает в двух экземплярах соответствующий «Акт об уничтожении бумажных носителей персональных данных». В течение трех дней после составления акт направляется на утверждение Директору Учреждения. После утверждения один экземпляр акта остается у Ответственного за организацию обработки ПДн, второй экземпляр передается в архив на хранение.

6. Ответственность

6.1. Ответственность за надлежащее и своевременное выполнение функций, предусмотренных настоящим положением, несет Ответственный за организацию обработки ПДн в Учреждении.

6.2. На ответственного за организацию обработки ПДн в Учреждении возлагается персональная ответственность за:

- создание надлежащих условий для использования документов;
- сохранность документов.

16. Срок действия и порядок внесения изменений

7.1. Настоящее Положение вступает в силу с момента его утверждения и действует бессрочно, до замены его новым Положением.

7.2. Изменения и дополнения в настоящее Положение вносятся приказом директора Учреждения.

Приложение 1

к Положению об организации обработки персональных данных в МБУ ДО РР ДЮЦТ без использования средств автоматизации

ФОРМА

Журнал учета хранилищ материальных носителей персональных данных в

МБУ ДО РР ДЮЦТ

№ п/п	Материальный носитель	Категория персональных данных, обрабатываемая на материальном носителе	Место хранения	Перечень лиц, имеющих доступ к материальным носителям персональных данных	Дата начала хранения	Срок хранения	Фамилия, имя, отчество принявшего на хранение, подпись
1	2	3	4	5	6	7	8

Приложение 2
к Положению об организации
обработки персональных данных
в МБУ ДО РР ДЮЦТ без
использования средств
автоматизации

ФОРМА

АКТ

«___» _____ 20__г. № _____

Рязань

Об уничтожении бумажных

носителей персональных данных

Комиссия в составе:

Председатель:

_____ _____

Члены комиссии:

1. _____ _____
2. _____ _____
3. _____ _____

составили настоящий акт о том, что в результате проведенной экспертной оценки подлежат уничтожению следующие документы, срок хранения которых истек (опись прилагается):

№ п/п	Дата окончания срока обработки зафиксированных на носителе персональных данных	Наименование бумажного носителя	Примечание
1	2	3	4

Перечисленные бумажные носители персональных данных уничтожены путем _____ _____.

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

Председатель:

_____ _____ _____

Члены комиссии:

_____ _____ _____

_____ _____ _____

_____ _____ _____

УПРАВЛЕНИЕ ОБРАЗОВАНИЯ И МОЛОДЕЖНОЙ ПОЛИТИКИ

АДМИНИСТРАЦИИ РЫБНОВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА РЯЗАНСКОЙ ОБЛАСТИ

Муниципальное бюджетное учреждение дополнительного образования
«Рыбновский районный

Детско-юношеский Центр туризма»

391110, Рязанская область,
г. Рыбное, Набережный
пер., д.2

тел. (49137) 52-2-60,

ПРИКАЗ

«19» марта 2021 г. № 22

Об утверждении регламента проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

Во исполнение требований Федерального закона №152-ФЗ от 27.07.2006 г. «О персональных данных» и прочих нормативных документов по защите информации,

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие Регламент проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – Регламент) (Приложение к настоящему Приказу).

2. Требования Регламента довести до работников, непосредственно осуществляющих защиту персональных данных.

3. Контроль за исполнением настоящего Приказа оставляю за собой.

Директор С.В.Новиков

Приложение

к приказу МБУ ДО РР ДЮЦТ

от «19» марта 2021 г. № 22

РЕГЛАМЕНТ
проведения внутреннего контроля соответствия обработки персональных данных в МБУ ДО РР ДЮЦТ **требованиям к защите персональных данных**

1. Основные термины и определения

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

Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность. Инцидентами информационной безопасности являются:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по информационной безопасности;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

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;

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

Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. ЗОбщие положения

2.1. Настоящий Регламент проведения внутреннего контроля соответствия обработки персональных данных в МБУ ДО РР ДЮЦТ требованиям к защите

персональных данных (далее – Регламент), разработан в соответствии с законодательством Российской Федерации о персональных данных (далее – ПДн) и нормативными правовыми актами (методическими документами) федеральных органов исполнительной власти по вопросам безопасности ПДн при их обработке в информационных системах персональных данных (далее – ИСПДн).

2.2. Настоящий Регламент определяет порядок проведения внутреннего контроля соответствия обработки ПДн (далее – Внутренний контроль), требованиям к защите ПДн.

2.3. Регламент обязателен для исполнения всеми работниками МБУ ДО РР ДЮЦТ (далее – Учреждение), непосредственно осуществляющими защиту ПДн.

3. Порядок проведения внутреннего контроля

3.2. Для проведения внутреннего контроля в ИСПДн приказом Директора Учреждения создаётся комиссия, состоящая не менее чем из трех человек с обязательным включением в её состав:

- ответственного за обеспечение безопасности ПДн в ИСПДн;
- ответственного за организацию обработки ПДн в Учреждении.

3.3. Председатель комиссии организует работу комиссии, решает вопросы взаимодействия комиссии с руководителями и работниками Учреждения, готовит и ведёт заседания комиссии, подписывает протоколы заседаний. По окончании работы комиссии готовится заключение по результатам внутреннего контроля, которое передается на рассмотрение Директору Учреждения.

3.4. Внутренний контроль проводится в соответствии с «Планом проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных», утвержденным приказом директора Учреждения, форма которого установлена в Приложении 1 к настоящему Регламенту.

3.5. В «Плане проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных» указывается перечень проводимых мероприятий внутреннего контроля и периодичность их проведения.

3.6. Комиссия проводит внутренний контроль непосредственно на месте обработки ПДн, опрашивает работников Учреждения, осуществляющих обработку ПДн, осматривает рабочие места.

3.7. В ходе проведения внутреннего контроля осуществляется:

- контроль выполнения организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн;
- анализ изменения угроз безопасности ПДн в ИСПДн, возникающих в ходе ее эксплуатации;
- проверка параметров настройки и правильности функционирования программного обеспечения и средств защиты информации (далее – СЗИ);
- контроль состава технических средств, программного обеспечения и СЗИ;
- состояние учета СЗИ;
- состояние учета средств шифровальной (криптографической) защиты информации;
- состояние учета съемных машинных носителей ПДн;
- соблюдение правил доступа к ПДн;

- контроль наличия (отсутствия) фактов несанкционированного доступа к ПДн;
- соблюдение пользователями ИСПДн парольной политики;
- соблюдение пользователями ИСПДн антивирусной политики;
- соблюдение пользователями ИСПДн правил работы со съемными машинными носителями ПДн.

3.8. В целях проведения внутреннего контроля все работники Учреждения обязаны по первому требованию членов комиссии предъявить для проверки все числящиеся за ними материалы и документы, дать устные или письменные объяснения по существу заданных им вопросов.

3.9. По завершении внутреннего контроля комиссией составляется «Акт о проведении контроля соответствия обработки персональных данных», форма которого установлена в Приложении 2 к настоящему Регламенту.

3.10. В «Акте о проведении контроля соответствия обработки персональных данных» указываются:

- перечень проведенных мероприятий;
- выявленные нарушения;
- мероприятия по устранению нарушений;
- решения по результатам внутреннего контроля;
- сроки устранения нарушений.

3.11. Периодичность проведения внутреннего контроля составляет не реже 1 раза в год.

3.12. Предложения о создании комиссии и о плановом/внеплановом проведении внутреннего контроля представляются Директору Учреждения Ответственным за организацию обработки ПДн и Ответственным за обеспечение безопасности ПДн в ИСПДн.

4. Ответственность

4.1. Ответственный за организацию обработки ПДн в Учреждении несет ответственность за организацию проведения внутреннего контроля соответствия обработки ПДн в Учреждении требованиям к защите ПДн.

5. Срок действия и порядок внесения изменений

5.1. Настоящий Регламент вступает в силу с момента его утверждения и действует бессрочно, до замены новым Регламентом.

5.2. Настоящий Регламент подлежит пересмотру не реже одного раза в три года.

5.3. Изменения и дополнения в настоящий Регламент вносятся приказом директора Учреждения.

Приложение 1

к Регламенту проведения внутреннего контроля соответствия обработки персональных данных в МБУ ДО РР ДЮЦТ требованиям к защите персональных данных

ФОРМА

План проведения внутреннего контроля

соответствия обработки персональных данных

в МБУ ДО РР ДЮЦТ

№ п/п	Мероприятие	Регулярность проведения
1.	Анализ актуальности локальных нормативных актов (внутренних документов) по вопросам обеспечения безопасности персональных данных: – Проверка соответствия локальных нормативных актов (внутренних документов) по вопросам обеспечения безопасности персональных данных действующему законодательству РФ по защите персональных данных; – Учет в локальных нормативных актах (внутренних документах) по вопросам обеспечения безопасности персональных данных изменений в деятельности ОГБУДО «ДЭБЦ» по обработке и защите персональных данных.	1 раз в три года или по мере обновления законодательства РФ
2.	Проверка ознакомления работников с положениями законодательства РФ по защите персональных данных, документами, определяющими политику ОГБУДО «ДЭБЦ» в отношении обработки персональных данных и организационно-распорядительными документами по вопросам персональных данных.	1 раз в год
3.	Проверка выполнения работниками – пользователями информационных систем персональных данных инструкций по эксплуатации информационных систем персональных данных, положения о разрешительной системе доступа.	1 раз в год
4.	Проверка актуальности прав разграничения доступа пользователей информационных систем персональных данных, необходимых для выполнения должностных обязанностей.	1 раз в год

№ п/п	Мероприятие	Регулярность проведения
5.	Проверка актуальности определенных угроз безопасности персональных данных для информационных систем персональных данных.	1 раз в год
6.	Проверка полноты реализованных технических мер по обеспечению безопасности персональных данных в информационных системах персональных данных с учетом структурно-функциональных характеристик информационных системах персональных данных, информационных технологий, особенностей функционирования информационных системах персональных данных.	1 раз в год
7.	Проверка наличия сертифицированных средств защиты информации, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.	1 раз в год
8.	Проверка правил обращения со съемными машинными носителями персональных данных.	1 раз в год
9.	Проверка актуальности информации, содержащейся в Уведомлении об обработке персональных данных, предоставленной в Роскомнадзор.	1 раз в год
10.	Выявление уязвимостей в информационных системах персональных данных в т.ч. в системе защиты с использованием средства инструментального анализа защищенности.	1 раз в год
11.		

Приложение 2

к Регламенту проведения внутреннего контроля соответствия обработки персональных данных в МБУ ДО РР ДЮЦТ требованиям к защите персональных данных

ФОРМА

АКТ

«___» _____ 20__ г. № _____

Рязань

О проведении контроля соответствия обработки

персональных данных

Комиссия в составе:

Председатель:

_____ _____

Члены комиссии:

1. _____ _____
2. _____ _____
3. _____ _____

составила настоящий акт о том, что комиссией были проведены мероприятия по контролю соответствия обработки персональных данных в МБУ ДО РР ДЮЦТ требованиям к защите персональных данных. Результат проведенного внутреннего контроля отражен в Таблице 1.

Таблица 1

№ п/п	Мероприятие	Выявленные недостатки	Мероприятия по устранению недостатков	Срок проведения мероприятий	Ответственное лицо

№ п/п	Мероприятие	Выявленные недостатки	Мероприятия по устранению недостатков	Срок проведения мероприятий	Ответственное лицо

Внутренний контроль проводился в соответствии с «Регламентом проведения внутреннего контроля соответствия обработки персональных данных в МБУ ДО РР ДЮЦТ требованиям к защите персональных данных».

Председатель:

_____ _____ _____

Члены комиссии:

_____ _____ _____

_____ _____ _____

_____ _____ _____

УПРАВЛЕНИЕ ОБРАЗОВАНИЯ И МОЛОДЕЖНОЙ ПОЛИТИКИ

АДМИНИСТРАЦИИ РЫБНОВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА РЯЗАНСКОЙ ОБЛАСТИ

Муниципальное бюджетное учреждение дополнительного образования
«Рыбновский районный

Детско-юношеский Центр туризма»

391110, Рязанская область,
г. Рыбное, Набережный
пер., д.2

тел. (49137) 52-2-60,

ПРИКАЗ

«19» марта 2021 г. № 23

Об утверждении положения об обеспечении безопасности персональных данных

Во исполнение требований Федерального закона №152-ФЗ от 27 июля 2006 г. «О персональных данных», приказа 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» и прочих нормативных документов по защите информации,

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие Положение об обеспечении безопасности персональных данных, обрабатываемых в информационных системах персональных данных МБУ ДО РР ДЮЦТ (далее – Положение) (Приложение к настоящему приказу).
2. Ответственному за обеспечение безопасности персональных данных в информационных системах обеспечить выполнение требований Положения.
3. Требования Положения довести до работников, непосредственно осуществляющих защиту персональных данных в информационных системах персональных данных.
4. Контроль за исполнением настоящего Приказа оставляю за собой.

Директор Новиков С.В.

Приложение

к приказу МБУ ДО РР ДЮЦТ

от «19» марта 2021 г. № 23

ПОЛОЖЕНИЕ

об обеспечении безопасности персональных данных,

обрабатываемых в информационных системах персональных данных

МБУ ДО РР ДЮЦТ

17. Термины и определения

9.1. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

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

9.3. 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.

9.4. Основные технические средства и системы – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи персональных данных.

9.5. 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.

9.6. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);

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

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

9.9. Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

18. Общие положения

2.1. Настоящее Положение об обеспечении безопасности персональных данных, обрабатываемых в информационных системах персональных данных МБУ ДО РР ДЮЦТ (далее – Положение), разработано в соответствии с законодательством Российской Федерации о персональных данных (далее – ПДн) и нормативными правовыми актами (методическими документами) федеральных органов исполнительной власти по вопросам безопасности ПДн при их обработке в информационных системах персональных данных (далее – ИСПДн).

2.2. Настоящее Положение определяет состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн.

2.3. Положение обязательно для исполнения всеми работниками МБУ ДО РР ДЮЦТ (далее – Учреждение), непосредственно осуществляющими защиту ПДн, обрабатываемых в ИСПДн.

19. Цели и задачи обеспечения безопасности персональных данных

3.1. Основной целью обеспечения безопасности ПДн, при их обработке в ИСПДн, является защита ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

3.2. Задачей, которую необходимо решить для достижения поставленной цели, является обеспечение безопасности ПДн при их обработке в ИСПДн с помощью системы защиты персональных данных (далее – СЗПДн), нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006г. №152-ФЗ «О персональных данных».

3.3. СЗПДн включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности ПДн и информационных технологий, используемых в ИСПДн.

20. Основные принципы построения системы защиты информации

4.1. СЗПДн основывается на следующих принципах:

- системности;
- комплексности;
- непрерывности защиты;
- разумной достаточности;
- гибкости;
- простоты применения средств защиты информации (далее – СЗИ).

4.2. Принцип системности – предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн.

4.3. Принцип комплексности – предполагает, что СЗПДн должна включать совокупность объектов защиты, сил и средств, принимаемых мер, проводимых мероприятий и действий по обеспечению безопасности ПДн от возможных угроз всеми доступными законными средствами, методами и мероприятиями.

4.4. Принцип непрерывности защиты – это процесс обеспечения безопасности ПДн, осуществляемый руководством, ответственным за обеспечение безопасности ПДн в ИСПДн и работниками всех уровней. Это не только и не столько процедура или политика,

которая осуществляется в определенный отрезок времени или совокупность СЗИ, сколько процесс, который должен постоянно идти на всех уровнях внутри Учреждения, и каждый работник должен принимать участие в этом процессе.

4.5. Принцип разумной достаточности – предполагает соответствие уровня затрат на обеспечение безопасности ПДн ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения.

4.6. Принцип гибкости – СЗПДн должна быть способна реагировать на изменения внешней среды и условий осуществления своей деятельности.

4.7. Принцип простоты применения СЗИ – механизмы защиты должны быть интуитивно понятны и просты в применении. Применение СЗИ не должно быть связано со знанием каких-либо языков или требовать дополнительных затрат на её применение, а также не должно требовать выполнения рутинных малопонятных операций.

21. Основные мероприятия по обеспечению безопасности персональных данных

5.1. Для обеспечения защиты ПДн, обрабатываемых в ИСПДн, проводятся следующие мероприятия:

- определение ответственных лиц за обеспечение защиты ПДн;
- определение актуальных угроз безопасности ПДн;
- определение уровня защищенности ПДн;
- реализация правил разграничения доступа и введение ограничений на действия пользователей ИСПДн;
- ограничение доступа в помещения, где размещены основные технические средства и системы, позволяющие осуществлять обработку ПДн;
- учет и хранение съемных машинных носителей ПДн;
- организация резервирования и восстановления работоспособности программного обеспечения, баз данных ПДн и СЗИ;
- организация парольной защиты;
- организация антивирусной защиты;
- организация обновления программного обеспечения и СЗИ;
- использование СЗИ;
- использование средств шифровальной (криптографической) защиты информации (далее – СКЗИ);
- оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию СЗПДн;
- обнаружение фактов несанкционированного доступа к ПДн и принятие мер;
- контроль за принимаемыми мерами по обеспечению безопасности ПДн;
- планирование мероприятий по защите ПДн в ИСПДн;
- управление (администрирование) СЗПДн;
- управление конфигурацией ИСПДн и СЗПДн;
- реагирование на инциденты;
- информирование и обучение персонала ИСПДн.

5.2. Определение ответственных лиц за обеспечение безопасности ПДн

5.2.1. За вопросы обеспечения безопасности ПДн, обрабатываемых в ИСПДн, отвечают:

- Директор.
- Ответственный за организацию обработки ПДн – работник, отвечающий за организацию и состояние процесса обработки ПДн.
- Ответственный за обеспечение безопасности ПДн в ИСПДн – работник, отвечающий за правильность использования и нормальное функционирование установленной СЗПДн.
- Администратор ИСПДн – работник, отвечающий за правильность использования и бесперебойное, стабильное функционирование установленных систем обработки ПДн.

5.3. Определение актуальных угроз безопасности ПДн в ИСПДн

5.3.1. Актуальные угрозы безопасности ПДн, обрабатываемых в ИСПДн, определяются по результатам оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, анализа возможных уязвимостей ИСПДн, возможных способов реализации угроз безопасности ПДн и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

5.3.2. Для определения угроз безопасности ПДн и разработки «Модели угроз безопасности персональных данных» применяются методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. №1085.

5.4. Определение уровня защищенности ПДн

5.4.1. Уровень защищенности ПДн, обрабатываемых в ИСПДн, определяется в соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и оформляется в виде «Акта об определения уровня защищенности персональных данных».

5.5. Реализация правил разграничения доступа и введение ограничений на действия пользователей ИСПДн

5.5.1. Реализация правил разграничения доступа, к ПДн, обрабатываемым в ИСПДн, осуществляется в соответствии с «Положением о разрешительной системе доступа в информационных системах персональных данных МБУ ДО РР ДЮЦТ, утвержденным приказом директора МБУ ДО РР ДЮЦТ.

5.5.2. Основные технические средства и системы ИСПДн располагаются в помещениях, находящихся в пределах границы контролируемой зоны, определенной приказом директора МБУ ДО РР ДЮЦТ, с максимальным удалением от её границ.

5.5.3. Доступ в помещения, в которых ведется обработка ПДн, осуществляется в соответствии с «Правилами доступа работников в помещения, в которых ведется обработка персональных данных в МБУ ДО РР ДЮЦТ, утвержденными приказом директора МБУ ДО РР ДЮЦТ.

5.6. Учет и хранение съемных машинных носителей ПДн

5.6.1. Работа со съемными машинными носителями ПДн в ИСПДн осуществляется в соответствии с «Порядком обращения со съемными машинными носителями персональных данных в МБУ ДО РР ДЮЦТ, утвержденным приказом директора МБУ ДО РР ДЮЦТ.

5.7. Организация резервирования и восстановления работоспособности программного обеспечения, баз данных ПДн и СЗИ.

5.7.1. Организация резервирования и восстановления работоспособности программного обеспечения, баз данных ПДн и СЗИ в ИСПДн осуществляется в соответствии с «Инструкцией по организации резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных МБУ ДО РР ДЮЦТ, утвержденной приказом директора МБУ ДО РР ДЮЦТ.

5.8. Организация парольной защиты

5.8.1. Организация парольной защиты в ИСПДн осуществляется в соответствии с «Инструкцией по парольной защите информации в МБУ ДО РР ДЮЦТ, утвержденной приказом директора МБУ ДО РР ДЮЦТ.

5.9. Организация антивирусной защиты

5.9.1. Организация антивирусной защиты в ИСПДн осуществляется в соответствии с «Инструкцией по организации антивирусной защиты в МБУ ДО РР ДЮЦТ, утвержденной приказом директора МБУ ДО РР ДЮЦТ.

5.10. Организация обновления программного обеспечения и СЗИ

5.10.1. Организация обновления программного обеспечения и СЗИ в ИСПДн осуществляется в соответствии с «Инструкцией ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных МБУ ДО РР ДЮЦТ и «Инструкцией администратора информационных систем персональных данных МБУ ДО РР ДЮЦТ, утвержденные приказом директора МБУ ДО РР ДЮЦТ.

5.11. Применение СЗИ

5.11.1. Для обеспечения защиты ПДн, обрабатываемых в ИСПДн, применяются СЗИ, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации, в соответствии со статьей 5 Федерального закона от 27 декабря 2002 г. №184-ФЗ «О техническом регулировании».

5.11.2. Установка и настройка СЗИ в ИСПДн проводится в соответствии с эксплуатационной документацией на СЗПДн и документацией на СЗИ.

5.12. Использование СКЗИ

5.12.1. Для обеспечения защиты ПДн, обрабатываемых в ИСПДн, при их передаче по открытым каналам связи, применяются СКЗИ. Обращение с СКЗИ, эксплуатируемыми в ИСПДн, осуществляется в соответствии с «Инструкцией по обращению со средствами криптографической защиты информации в МБУ ДО РР ДЮЦТ, утвержденной приказом директора МБУ ДО РР ДЮЦТ.

5.13. Оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию СЗПДн

5.13.1. На этапах внедрения СЗПДн проводится оценка эффективности принимаемых мер по обеспечению безопасности ПДн, которая включает в себя:

- предварительные испытания СЗПДн;
- опытную эксплуатацию СЗПДн;
- анализ уязвимостей ИСПДн и принятие мер по их устранению;
- приемочные испытания СЗПДн.

5.14. Обнаружение фактов несанкционированного доступа к ПДн и принятие мер

5.14.1. Ответственному за обеспечение безопасности ПДн в ИСПДн или администратору ИСПДн должны сообщаться любые инциденты информационной безопасности, в которые входят:

- факты попыток и успешной реализации несанкционированного доступа в ИСПДн;
- факты попыток и успешной реализации несанкционированного доступа в помещения, в которых ведется обработка ПДн;
- факты сбоя или некорректной работы систем обработки ПДн;
- факты сбоя или некорректной работы СЗИ;
- факты разглашения ПДн, обрабатываемых в ИСПДн;
- факты разглашения информации о методах и способах защиты и обработки ПДн в ИСПДн.

5.14.2. Разбор инцидентов информационной безопасности проводится в соответствии с «Регламентом реагирования на инциденты информационной безопасности в информационных системах персональных данных МБУ ДО РР ДЮЦТ, утвержденным приказом директора МБУ ДО РР ДЮЦТ.

5.15. Контроль за принимаемыми мерами по обеспечению безопасности ПДн

5.15.1. Контроль за принимаемыми мерами по обеспечению безопасности ПДн осуществляется в соответствии с «Регламентом проведения внутреннего контроля соответствия обработки персональных данных в МБУ ДО РР ДЮЦТ, утвержденным приказом директора МБУ ДО РР ДЮЦТ.

22. Ответственность

6.1. Все работники, допущенные в установленном порядке к работе с ПДн, несут административную, материальную, уголовную ответственность в соответствии с действующим законодательством Российской Федерации за необеспечение сохранности и несоблюдение правил работы с ПДн.

6.2. Ответственность за доведение требований настоящего Положения до работников МБУ ДО РР ДЮЦТ и обеспечение мероприятий по их реализации несет ответственный за обеспечение безопасности ПДн в ИСПДн.

УПРАВЛЕНИЕ ОБРАЗОВАНИЯ И МОЛОДЕЖНОЙ ПОЛИТИКИ

АДМИНИСТРАЦИИ РЫБНОВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА РЯЗАНСКОЙ ОБЛАСТИ

Муниципальное бюджетное учреждение дополнительного образования

«Рыбновский районный

Детско-юношеский Центр туризма»

391110, Рязанская область,
г. Рыбное, Набережный
пер., д.2

тел. (49137) 52-2-60,

ПРИКАЗ

«19» марта 2021 г. № 24

Об утверждении положения об организации обработки персональных данных

Во исполнение требований Федерального закона №152-ФЗ от 27.07.2006 г. «О персональных данных», а также прочих нормативных документов по защите информации,

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие Положение об организации обработки персональных данных в МБУ ДО РР ДЮЦТ (далее – Положение) (Приложение 1 к настоящему Приказу).
2. Утвердить и ввести в действие Правила рассмотрения запросов субъектов персональных данных, чьи персональные данные обрабатываются в МБУ ДО РР ДЮЦТ (далее – Правила) (Приложение 2 к настоящему Приказу).
3. Ответственному за организацию обработки персональных данных в МБУ ДО РР ДЮЦТ ознакомить работников, осуществляющих обработку персональных данных с Положением.
4. Ответственному за организацию обработки персональных данных в МБУ ДО РР ДЮЦТ руководствоваться Правилами при обращении субъектов персональных данных в МБУ ДО РР ДЮЦТ.
5. Контроль за исполнением настоящего приказа оставляю за собой.

Директор С.В.Новиков

Приложение 1

к приказу МБУ ДО РР ДЮЦТ

от «19» марта 2021 г. № 24

ПОЛОЖЕНИЕ

об организации обработки персональных данных

в МБУ ДО РР ДЮЦТ

Основные термины и определения

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Биометрические персональные данные – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются для установления личности субъекта персональных данных.

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

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

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их раскрытие третьим лицам или их распространение без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

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

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

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

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.

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

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

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

Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни.

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

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

Общие положения

- Настоящее Положение об организации обработки персональных данных в МБУ ДО РР ДЮЦТ (далее – Положение), определяет цели, содержание, порядок и политику обработки персональных данных, меры, направленные на защиту персональных данных, а также процедуры выявления и предотвращения нарушений законодательства Российской Федерации в области персональных данных МБУ ДО РР ДЮЦТ юридический адрес: 391110, Рязанская область, г.Рыбное, ул. Набережный переулок, д.2 (далее – Оператор).
- Положение обязательно для исполнения всеми работниками Оператора, непосредственно участвующими в обработке персональных данных.
- Все работники Оператора, имеющие доступ к персональным данным, должны подписать «Обязательство о неразглашении информации ограниченного доступа», форма которого установлена в Приложении 1 к данному Положению
- Настоящее Положение разработано в соответствии с Федеральным законом от 27 июля 2006 г. N 152-ФЗ «О персональных данных», Федеральным законом от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- Оператор обрабатывает персональные данные в исполнение и в соответствии со следующими нормативными и правовыми актами:
  - ст. ст. 23-24 Конституции Российской Федерации;
  - ст. ст. 86-90 Трудовым кодексом Российской Федерации;
  - Налоговым кодексом Российской Федерации;
  - Гражданским кодексом Российской Федерации;
  - Федеральным законом от 15.12.2001 № 167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации»;

- Федеральным законом от 06.12.2011 №402-ФЗ «О бухгалтерском учете»;
- Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
- Федеральным законом от 28.12.2013 № 426-ФЗ «О специальной оценке условий труда»;
- ст. 15 и ст. 36.19 Федерального закона от 07.05.1998 № 75-ФЗ «О негосударственных пенсионных фондах»;
- Федеральным законом от 29.12.2006 № 255-ФЗ «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством»;
- ст. 8 Федерального закона от 31.05.1996 № 61-ФЗ «Об обороне»;
- ст. 9 Федерального закона от 26.02.1997 № 31-ФЗ «О мобилизационной подготовке и мобилизации в Российской Федерации»;
- постановлением Правительства Российской Федерации от 27.11.2006 № 719 «Об утверждении Положения о воинском учете»;
- Федеральным законом от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;
- Лицензией на осуществление образовательной деятельности № 13-2316 от 15.07.2015;
- Уставом Оператора.

- Настоящее Положение не распространяется на следующие случаи:
  - осуществляется хранение, комплектование, учет и использование архивных документов, содержащих персональные данные, в соответствии с законодательством об архивном деле в Российской Федерации;
  - осуществляется обработка персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

Условия и порядок обработки персональных данных работников

- Персональные данные работников Оператора, бывших работников Оператора и физических лиц, работающих на основании договора гражданско-правового характера с Оператором, обрабатываются в целях:
  - ведения кадрового, бухгалтерского и воинского учета;
  - обеспечения пропускного режима, сохранности имущества Оператора, обеспечение личной безопасности;
  - исполнения Оператором функции работодателя, оформления трудовых отношений и обеспечения установленных законодательством Российской Федерации условий труда;
  - заключения и исполнения договора, стороной которого является субъект персональных данных.

- В целях, указанных в пункте 3.1 настоящего Положения обрабатываются следующие категории персональных данных:
  - фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);
  - пол;

- дата и место рождения;
- информация о гражданстве;
- вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;
- адрес места жительства (адрес регистрации, фактического проживания);
- номер контактного телефона и адрес электронной почты;
- СНИЛС;
- ИНН;
- сведения о свидетельствах государственной регистрации актов гражданского состояния;
- семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших);
- сведения о трудовой деятельности и занимаемая должность;
- сведения о предыдущих местах работы;
- сведения о социальном положении;
- сведения о воинском учете и реквизиты документов воинского учета;
- сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании);
- информация о владении иностранными языками, степень владения;
- фотография;
- информация, содержащаяся в трудовом договоре, дополнительных соглашениях к нему;
- сведения о профессиональной переподготовке и (или) повышении квалификации;
- сведения о наградах;
- информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания;
- сведения о доходах;
- номер банковской карты;
- сведения о деловых и иных личных качествах, носящих оценочный характер.

- Обработка персональных данных осуществляется с помощью средств автоматизации и без применения таких средств и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.
- Обработка персональных данных осуществляется только после получения письменного «Согласия на обработку персональных данных», форма которого, установлена в Приложении 2 к настоящему Положению.
- Получение персональных данных осуществляется непосредственно от субъекта персональных данных путем:
  - получения оригиналов необходимых документов (заявление, трудовая книжка и иные документы, предоставляемые в отдел кадров);
  - копирования оригиналов документов;

- внесения сведений в учетные формы (на бумажных и электронных носителях);
- формирования персональных данных в ходе кадровой работы;
- внесения персональных данных в информационные системы.

- В случае возникновения необходимости получения персональных данных у третьей стороны, следует известить об этом субъекта персональных данных, получить его письменное согласие и сообщить ему о целях, предполагаемых источниках и способах получения персональных данных.
- В случаях, когда предоставление персональных данных является обязательным в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», субъекту персональных данных разъясняются юридические последствия отказа предоставить его персональные данные. Форма «Разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные» представлена в Приложении 3 к данному Положению.
- Запрещается получать, обрабатывать персональные данные, не предусмотренные пунктом 3.2 настоящего Положения, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.
- Обработка биометрических персональных данных (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность, и которые используются для установления личности субъекта персональных данных) Оператором не осуществляется.
- Передача (распространение, предоставление) персональных данных осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.
- Трансграничная передача персональных данных работников Оператора и бывших работников и физических лиц, работающих на основании договора гражданско-правового характера, не осуществляется.
- Право доступа к персональным данным работников Оператора и бывших работников и физических лиц, работающих на основании договора гражданско-правового характера в электронной форме и на бумажных носителях, имеют лица, занимающие следующие должности:
  - руководитель Оператора;
  - методист Оператора.

- Срок хранения персональных данных работников Оператора и бывших работников Оператора в электронной форме и на бумажных носителях составляет 5 лет после расторжения трудового договора и после передаются в архив в порядке, предусмотренном законодательством Российской Федерации, где хранятся в течение 75 лет.
- Срок хранения персональных данных физических лиц, работающих на основании договора гражданско-правового характера с Оператором, электронной форме и на бумажных носителях составляет 5 лет после завершения работ по договору или после его расторжения.

Условия и порядок обработки персональных данных кандидатов на замещение вакантных должностей

- В целях, указанных в пункте 4.1 настоящего Положения обрабатываются следующие категории персональных данных:
  - фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);
  - пол;

- дата и место рождения;
- информация о гражданстве;
- номер контактного телефона и адрес электронной почты;
- сведения о трудовой деятельности и занимаемая должность;
- сведения о предыдущих местах работы;
- сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, квалификация, специальность по документу об образовании);
- информация о владении иностранными языками, степень владения;
- фотография;
- сведения о профессиональной переподготовке и (или) повышении квалификации;
- сведения о деловых и иных личных качествах, носящих оценочный характер.

- Обработка персональных данных осуществляется с помощью средств автоматизации и без применения таких средств и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, блокирование, удаление, уничтожение персональных данных.
- Обработка персональных данных осуществляется только после получения письменного «Согласия на обработку персональных данных», форма которого, установлена в Приложении 2 к настоящему Положению, кроме получения персональных данных из общедоступных источников.
- Получение персональных данных может осуществляться следующими способами:
  - непосредственно от кандидата по электронной почте;
  - копирование резюме кандидата из общедоступных источников персональных данных (в том числе сайты по поиску работы);
  - от кадровых агентств.
- Запрещается получать, обрабатывать персональные данные, не предусмотренные пунктом 4.2 настоящего Положения, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни и состояния здоровья.
- Обработка биометрических персональных данных (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность, и которые используются Оператором для установления личности субъекта персональных данных) Оператором не осуществляется.

Условия и порядок обработки персональных данных посетителей сайта Оператора

- Персональные данные посетителей сайта Оператора (https://p62.навигатор.дети) (далее – Сайт), обрабатываются в целях:
  - оценки и анализа работы Сайта;
  - регистрации и авторизации посетителей на Сайте;
  - информирования посетителей Сайта об акциях, скидках и специальных предложениях посредством электронных и СМС-рассылок.
- В целях, указанных в пункте 5.1 настоящего Положения обрабатываются следующие категории персональных данных:
  - фамилия, имя;
  - номер мобильного телефона;

– адрес электронной почты.

- Обработка персональных данных осуществляется с помощью средств автоматизации и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.
- Получение персональных данных и получение согласия на обработку персональных данных осуществляется непосредственно от субъекта персональных данных при:

– регистрации в личном кабинете на Сайте;

– отправке формы обратной связи;

– отправке запроса обратной связи.

- Отдельно для оценки и анализа работы Сайта обрабатываются следующие данные: файлы cookie, сведения о действиях посетителя Сайта, сведения об оборудовании пользователя, IP-адрес, дата и время сессии, в том числе с использованием метрических программ Яндекс.Метрика, Google Analytics.
- В случае отказа от обработки персональных данных, указанных в предыдущем пункте метрическими программами посетитель Сайта должен прекратить использование Сайта или отключить использование файлов cookie в настройках браузера.
- Запрещается получать, обрабатывать персональные данные, не предусмотренные пунктом 5.2 настоящего Положения, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни и состояния здоровья.
- Обработка биометрических персональных данных (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность, и которые используются Оператором для установления личности субъекта персональных данных) Оператором не осуществляется.
- Передача персональных данных посетителей Сайта третьим лицам не осуществляется.
- Трансграничная передача персональных данных посетителей Сайта не осуществляется.
- Право доступа к персональным данным посетителей Сайта в электронной форме имеют лица, занимающие следующие должности:

– руководитель Оператора.

- Персональные данные посетителей Сайта в электронной форме хранятся в течение всего периода использования Сайта.

Условия и порядок обработки персональных данных детей и родителей

- Персональные данные детей и родителей, обрабатываются в целях обработки заявок на обучение и учет обучающихся.
- В целях, указанных в пункте 6.1 настоящего Положения обрабатываются следующие категории персональных данных:

– фамилия, имя, отчество ребенка;

– фамилия, имя, отчество родителей;

– дата рождения;

– СНИЛС;

– Номер сертификата персонифицированного финансирования дополнительного образования ребенка;

- Email;
- телефон;
- муниципалитет.

- Обработка персональных данных осуществляется с помощью средств автоматизации и без применения таких средств и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, блокирование, удаление, уничтожение персональных данных.
- Обработка персональных данных осуществляется только после получения согласия родителя.
- Получение персональных данных осуществляется непосредственно от субъекта персональных данных путем:
  - регистрации в личном кабинете на Сайте;
  - заполнение заявки на обучение ребенка;
  - внесения персональных данных в информационные системы.
- Запрещается получать, обрабатывать персональные данные, не предусмотренные пунктом 6.2 настоящего Положения, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни и состояния здоровья.
- Обработка биометрических персональных данных (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность, и которые используются Оператором для установления личности субъекта персональных данных) Оператором не осуществляется
- Трансграничная передача персональных данных детей и родителей не осуществляется.
- Право доступа к персональным данным детей и родителей в электронной форме и на бумажных носителях, имеют лица, занимающие следующие должности:
  - руководитель Оператора;
  - методист;
  - педагоги-организаторы;
  - педагоги дополнительного образования.
- Персональные данные детей и родителей хранятся в электронной форме и на бумажных носителях в течение 3 лет.

Информационные системы персональных данных

- Обработка персональных данных осуществляется в следующих информационных системах:

№ п/п	Наименование информационной системы	Назначение и описание	Субъекты персональных данных	Категория персональных данных
1			Работники	ИНЫЕ
2			Кандидаты на вакантную должность	ИНЫЕ
3			Посетители сайта	ИНЫЕ
4			Дети и родители	ИНЫЕ

Меры обеспечения безопасности персональных данных

- Оператор предпринимает необходимые организационные и технические меры для обеспечения безопасности персональных данных от случайного или несанкционированного доступа, уничтожения, изменения, блокирования доступа и других несанкционированных действий.
- Для обеспечения защиты персональных данных, обрабатываемых в информационных системах персональных данных Оператора проводятся следующие мероприятия:

Назначение ответственных лиц за организацию обработки и обеспечение защиты персональных данных;

Ограничение состава работников Оператора, имеющих доступ к персональным данным;

Определение уровня защищенности персональных данных при обработке в информационных системах персональных данных;

Установление правил разграничения доступа к персональным данным, обрабатываемым в информационных системах персональных данных и обеспечение регистрации и учета всех действий, совершаемых с персональными данными;

Ограничение доступа в помещения, где размещены основные технические средства и системы информационных систем персональных данных и осуществляется неавтоматизированная обработка персональных данных;

Ведение учета машинных носителей персональных данных;

Организация резервирования и восстановления работоспособности информационных систем персональных данных и персональных данных модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

Установление требований к сложности паролей для доступа к информационным системам персональных данных;

Применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации;

Осуществление антивирусного контроля, предотвращение внедрения в корпоративную сеть вредоносных программ (программ-вирусов) и программных закладок;

Организация своевременного обновления программного обеспечения, используемого в информационных системах персональных данных и средств защиты информации;

Проведение регулярной оценки эффективности принимаемых мер по обеспечению безопасности персональных данных;

Обнаружение фактов несанкционированного доступа к персональным данным и принятие мер по установлению причин и устранению возможных последствий;

Контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровней защищенности информационных систем персональных данных.

Порядок поручения обработки персональных данных

- Оператор может поручать обработку персональных данных другому лицу только с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора (контракта), (далее – Поручение оператора).
- В Поручении оператора должны быть определены:

– перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных;
– цели обработки персональных данных;
– обязанность указанного лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке;
– требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона №152-ФЗ от 27 июля 2006 г. «О персональных данных»;
– ответственность указанного лица перед Оператором.

- Лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом №152-ФЗ от 27 июля 2006 г. «О персональных данных». При этом обязанность получать согласие субъекта персональных данных на обработку его персональных данных остается за Оператором.
- Ответственность перед субъектом персональных данных за действия или бездействия лица, осуществляющего обработку персональных данных по поручению Оператора, несет Оператор. Лицо, осуществляющее обработку персональных данных по поручению Оператора, несет ответственность перед Оператором.
- Форма договора о поручении обработки персональных данных представлена в Приложении 4 к данному Положению.

Включение персональных данных в общедоступные источники

- В целях информационного обеспечения деятельности Оператора могут создаваться общедоступные источники персональных данных (в том числе справочники, электронные базы данных, страницы сайта в информационно-телекоммуникационной сети «Интернет» и др.).
- В общедоступные источники персональных данных могут включаться только те персональные данные, которые указаны субъектом персональных данных в письменном согласии на обработку персональных данных.
- Сведения о субъекте персональных данных исключаются в любое время из общедоступных источников по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

Правила обезличивания персональных данных и работы с обезличенными персональными данными

- Обезличивание персональных данных, содержащихся на машинных носителях, производится путем замены персональных данных, позволяющих определить их

принадлежность конкретному субъекту персональных данных, на уникальный внутренний идентификатор.

- Обезличивание персональных данных, содержащихся на бумажных носителях, производится путем стирания (вымарывания) персональных данных, позволяющих определить их принадлежность конкретному субъекту персональных данных.
- Работники Оператора не должны нарушать целостность, доступность обезличенных данных.
- Обработка обезличенных персональных данных может осуществляться с использованием средств автоматизации или без использования таких средств.
- При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение правил хранения бумажных носителей и порядка доступа в помещения, где они хранятся, в целях исключения несанкционированного доступа к обезличенным персональных данных, а также исключения возможности их несанкционированного уничтожения, изменения, блокирования, копирования, распространения и других неправомерных действий.
- При обработке обезличенных персональных данных с использованием средств автоматизации необходимо дополнительно соблюдать правила по парольной защите, идентификации пользователей, правил работы со съемными носителями (в случае их использования), правил резервного копирования.

Порядок уничтожения персональных данных

- Оператор прекращает обработку персональных данных и уничтожает носители персональных данных и удаляет их из информационных систем персональных данных в случаях:
  - достижения целей обработки персональных данных или максимальных сроков хранения – в течение 30 дней;
  - утраты необходимости в достижении целей обработки персональных данных – в течение 30 дней;
  - предоставление субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки – в течение 7 дней;
  - невозможности обеспечения правомерности обработки персональных данных – в течение 10 дней;
  - отзыва субъектом персональных данных согласия на обработку его персональных данных – в течение 30 дней;
  - истечения сроков исковой давности для правоотношений, в рамках которых осуществляется либо осуществлялась обработка персональных данных.
- В соответствии со статьей 21, частью 5 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» Оператор не прекращает обработку персональных данных и не уничтожает их в следующих случаях:
  - если иное предусмотрено договором, стороной которого, является субъект персональных данных;
  - если Оператор вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных законодательством Российской Федерации;
  - если не истекли сроки обработки персональных данных субъекта персональных данных, установленные законодательством Российской Федерации.

- Уничтожением бумажных носителей персональных данных занимается комиссия по организации работ по защите персональных данных, создаваемая приказом.
- Персональные данные уничтожаются путем механического нарушения целостности носителя персональных, не позволяющего произвести считывание или восстановление персональных данных, или удалением с электронных носителей методами и средствами гарантированного удаления информации.
- По окончании уничтожения носителей персональных данных комиссией составляется «Акт об уничтожении бумажных носителей персональных данных».

Рассмотрение запросов субъектов персональных данных или их представителей

- Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных Оператором, в том числе содержащей:
  - подтверждение факта обработки его персональных данных Оператором;
  - правовые основания и цели обработки персональных данных;
  - применяемые Оператором способы обработки персональных данных;
  - наименование и место нахождения Оператора, сведения о лицах (за исключением 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 Оператором;
  - порядок осуществления субъектом персональных данных прав, предусмотренных законодательством Российской Федерации в области персональных данных;
  - информацию об осуществленной или о предполагаемой трансграничной передаче персональных данных;
  - наименование организации или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такой организации или лицу;
  - иные сведения, предусмотренные законодательством Российской Федерации в области персональных данных.
- 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 законодательства Российской Федерации в области 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 ПДн имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

Ответственность

- Все работники Оператора, допущенные в установленном порядке к работе с персональными данными, несут административную, материальную, уголовную ответственность в соответствии с действующим законодательством Российской Федерации за обеспечение сохранности и соблюдение правил работы с персональными данными.
- Ответственность за доведение требований настоящего Положения до работников и обеспечение мероприятий по их реализации несет ответственный за организацию обработки персональных данных.
- Предоставление персональных данных посторонним лицам, в том числе, работникам, не имеющим права их обрабатывать, распространение (публикация) персональных данных, утрата носителей персональных данных, а также иные нарушения обязанностей по обработке персональных данных, установленных настоящим Положением и иными локальными нормативными актами, влечет наложение дисциплинарного взыскания, замечания, выговора или увольнения.
- Работники, имеющие доступ к персональным данным и совершившие указанный в предыдущем пункте дисциплинарный проступок, несут полную материальную ответственность в случае причинения их действиями ущерба (п. 7 ст. 243 Трудового кодекса Российской Федерации).
- Работники, имеющие доступ к персональных данных, виновные в незаконном сборе или передаче персональных данных, а также осуществившие неправомерный доступ к охраняемой законом компьютерной информации, несут уголовную ответственность в соответствии со ст. 137 и ст. 272 Уголовного кодекса Российской Федерации.

Приложение 1
к Положению об организации
обработки персональных данных
в МБУ ДО РР ДЮЦТ

ФОРМА

ОБЯЗАТЕЛЬСТВО

о неразглашении информации ограниченного доступа

Я,

_____

,

(Фамилия, Имя, Отчество)

заключив трудовой договор (контракт) № _____ от «__» _____ _____ года на работу в МБУ ДО РР ДЮЦТ, зарегистрированному по адресу: 391110, Рязанская обл., г.Рыбное, Набережный переулок, д.2 в качестве

_____

,

(наименование должности)

предупрежден(а), что на период исполнения должностных обязанностей, в соответствии с должностной инструкцией и/или локальными нормативными актами (внутренними документами) МБУ ДО РР ДЮЦТ мне будет предоставлен допуск к информации ограниченного доступа, в том числе и к персональным данным. Настоящим добровольно принимаю на себя следующие обязательства:

1. Не разглашать, не раскрывать и не передавать третьим лицам сведения, составляющие информацию ограниченного доступа, в том числе относящуюся к персональным данным, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.
2. В случае попытки третьих лиц получить от меня сведения, составляющие информацию ограниченного доступа, в том числе, касающуюся персональных данных, незамедлительно сообщить об этом непосредственному руководителю в устной или письменной форме.
3. Не использовать сведения, составляющие информацию ограниченного доступа, в том числе, касающуюся персональных данных, с целью получения личной выгоды (в любой форме).
4. Выполнять требования локальных нормативных актов (внутренних документов) МБУ ДО РР ДЮЦТ, регламентирующих вопросы защиты сведений, составляющих информацию ограниченного доступа, в том числе, касающуюся персональных данных.
5. После прекращения права на доступ к сведениям, составляющим информацию ограниченного доступа, не разглашать и не передавать третьим лицам известные мне сведения, составляющие информацию ограниченного доступа.

6. Передать при прекращении или расторжении трудового договора (контракта) непосредственному руководителю все имеющиеся в моем пользовании носители со сведениями, составляющими информацию ограниченного доступа, в том числе, касающуюся персональных данных.

7. Я предупрежден(а), что в случае нарушения настоящего Обязательства, буду нести дисциплинарную ответственность в соответствии с Трудовым кодексом Российской Федерации вплоть до увольнения с работы, а также предусмотренную в соответствии с законодательством Российской Федерации административную и уголовную ответственность.

«___» _____ 20__г. _____

_____

(подпись) (Ф.И.О.)

Приложение 2
к Положению об организации
обработки персональных данных
в МБУ ДО РР ДЮЦТ

БЛАНК

Согласие на обработку персональных данных

Я, _____

(Фамилия, Имя, Отчество Субъекта персональных данных)

_____серия _____№_____ выдан «___» ____ 20__г._____

(вид основного документа, удостоверяющий личность)

_____

,

(сведения о дате выдачи указанного документа и выдавшем его органе)

проживающий по адресу: _____

_____

.

В лице представителя субъекта персональных данных (заполняется в случае получения согласия от представителя субъекта персональных данных)

_____

(Фамилия, Имя, Отчество представителя)

_____серия _____№_____ выдан «___» ____ 20__г._____

(вид основного документа, удостоверяющий личность)

_____

,

(сведения о дате выдачи указанного документа и выдавшем его органе)

проживающий по адресу: _____

_____,

действующий от имени субъекта персональных данных на основании

_____

_____

(реквизиты доверенности или иного документа, подтверждающего полномочия представителя)

своей волей и в своем интересе **даю согласие** МБУ ДО РР ДЮЦТ (далее – Оператор), зарегистрированному по адресу: 391110, Рязанская обл., г.Рыбное, Набережны переулок, д.2 **на обработку своих персональных данных** как с использованием средств автоматизации, так и без использования таких средств включая сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение **следующих категорий**:

_____

.

(перечень персональных данных)

Вышеуказанные персональные данные могут обрабатываться только с целью _____

_____

(перечень целей обработки)

Даю согласие на передачу своих персональных данных: _____

_____

(указать полное наименование юридического лица; фамилия, имя, отчество и адрес физического лица; передачу которым дается согласие)

Настоящее согласие на обработку персональных данных действует с момента его представления Оператору до «__» _____ 20___ г. или на период действия _____ и может быть отозвано мной в любое время путем подачи Оператору заявления в простой письменной форме. В этом случае Оператор прекращает обработку персональных данных Субъекта и уничтожает их в течение 30 (тридцати) дней с момента получения Оператором заявления.

В соответствии со статьей 21, частью 5 Федерального закона от 27 июля 2006г. №152-ФЗ «О персональных данных» Оператор не прекращает обработку персональных данных Субъекта и не уничтожает их в следующих случаях: иное предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является Субъект; Оператор вправе осуществлять обработку персональных данных без согласия Субъекта на основаниях, предусмотренных федеральными законами; не истекли сроки обработки персональных данных Субъекта, установленные федеральными законами РФ и иными нормативными актами.

«___» _____ 20__г. _____ _____

(подпись) (Ф.И.О.)

Приложение 3
к Положению об организации
обработки персональных данных
в МБУ ДО РР ДЮЦТ

ФОРМА

Разъяснение субъекту персональных данных

юридических последствий отказа предоставить свои персональные данные

Мне, _____

(Фамилия, Имя, Отчество Субъекта персональных данных)

в соответствии с частью 2 статьи 18 Федерального закона от 27.07. 2006 № 152-ФЗ «О персональных данных» разъяснены юридические последствия отказа предоставить персональные данные МБУ ДО РР ДЮЦТ в целях _____

_____

_____

_____

.

(цели обработки персональных данных)

Мне, как субъекту персональных данных, разъяснено что: _____

_____

_____

_____

_____

.

(юридические последствия отказа)

«___» _____ 20__г. _____ _____

(подпись) (Ф.И.О.)

Приложение 4
к Положению об организации
обработки персональных данных
в МБУ ДО РР ДЮЦТ

ФОРМА

Договор поручения

на обработку персональных данных

Рязань «___»_____ 20__ г.

Муниципальное бюджетное учреждение дополнительного образования «Рыбновский районный Детско-юношеский Центр туризма», в дальнейшем именуемое «Доверитель», в лице _____, действующего на основании _____, с одной стороны, и _____, в дальнейшем именуемое «Поверенный», в лице _____, действующего на основании _____, с другой стороны, вместе именуемые «Стороны», заключили настоящий договор о нижеследующем:

1. Термины и определения:

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

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;

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;

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

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

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

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

2. Предмет договора

2.1. Доверитель, являясь оператором персональных данных, в соответствии с п. 3 ст. 6 Федерального закона от 27.07.2006 года № 152-ФЗ «О персональных данных» поручает, а Поверенный обязуются осуществлять обработку персональных данных.

2.2. Состав персональных данных, подлежащих обработке, включает:

- *(наименование субъектов персональных данных),*
- *(перечень персональных данных, относящихся к субъекту),*

2.3. Обработка персональных данных осуществляется в целях:

- *(перечень целей обработки персональных данных),*

3. Порядок взаимодействия сторон

3.1. Основанием для осуществления Поверенным обработки персональных данных субъектов персональных данных, осуществляемую в интересах Доверителя, является настоящий Договор.

3.2. Доверитель обязуется получить от субъектов персональных данных, перечисленных в п 2.2, до передачи их персональных данных письменное согласие, включающее указание наименования и адрес регистрации Поверенного, перечня персональных данных, обработка которых поручается Поверенному, и проинформировать субъектов персональных данных о целях поручения обработки персональных данных Поверенному.

Поверенный не обязан получать согласия субъектов персональных данных, указанных в п.2.2. настоящего Договора, на обработку их персональных данных.

3.3. Перечень действий (операций) с персональными данными, которые будут совершаться Поверенным в рамках данного Доверителем поручения, требования к защите обрабатываемых персональных данных: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение).

3.4. По дополнительному письменному поручению Доверителя, законному требованию субъекта персональных данных и/или по требованию органов государственного регулирования по защите прав субъектов персональных данных, с обязательным письменным уведомлением Доверителя, Поверенный может выполнять следующие действия с персональными данными: извлечение (выгрузка), блокирование удаление и уничтожение персональных данных.

3.5. Уполномоченными представителями каждой из Сторон, обеспечивающими непосредственное взаимодействие их по вопросам обработки указанных в п.2.2. настоящего Договора персональных данных, включая прием и передачу документов и сведений, содержащих персональные данные, являются:

- со стороны Доверителя: *(фамилия, имя, отчество, должность, номер телефона, адрес электронной почты)*;
- со стороны Поверенного: *(фамилия, имя, отчество, должность, номер телефона, адрес электронной почты)*.

4. Права и обязанности сторон

4.1. Доверитель обязуется:

4.1.1. Обеспечить сбор согласий субъектов персональных данных на поручение Доверителем обработки их персональных данных Поверенным.

4.1.2. По запросу уполномоченного органа по защите прав субъектов персональных данных, предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», допускающих обработку персональных данных без наличия согласия субъекта.

4.1.3. В случае отзыва субъектом персональных данных согласия на обработку персональных данных и отсутствия оснований, указанных в пунктах 2 – 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», допускающих обработку персональных данных без наличия согласия субъекта, направлять Поверенному письменное поручение на проведение работ по удалению, либо обезличиванию персональных данных субъекта.

4.1.4. При поступлении запроса от субъекта персональных данных на предоставление сведений, указанных в части 7 статьи 14 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», либо требований субъекта об утонении его персональных данных, их блокировании или уничтожения в случае, если персональные

данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, направлять Поверенному письменное поручение на предоставление информации, либо совершение конкретных действий с персональными данными субъекта.

4.2. Поверенный обязуется:

4.2.1. Соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» и другими нормативными актами, регламентирующие порядок обработки персональных данных.

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

4.2.3. Обеспечивать доступ работников Поверенного к персональным данным, обрабатываемым по поручению Доверителя, после подписания ими Обязательства о неразглашении персональных данных, изучения требований Доверителя по порядку обработки и защиты персональных данных, локальных нормативных актов, регламентирующих порядок организации и обеспечения защиты персональных данных и прохождения инструктажа по порядку обращения с персональными данным.

4.2.4. Определить угрозы безопасности персональных данных при их обработке в информационных системах персональных данных.

4.2.5. Применять прошедшие в установленном порядке процедуру оценки соответствия средств защиты информации, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

4.2.6. Проводить периодическую оценку эффективности принимаемых мер по обеспечению безопасности персональных данных и контроль уровня защищенности информационных систем персональных данных.

4.2.7. Вести учет машинных носителей персональных данных, если такие применяются.

4.2.8. Обеспечить восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

4.2.9. Не раскрывать третьим лицам персональные данные без согласия субъектов персональных данных, за исключением случаев, предусмотренных законодательством.

Не считается раскрытием персональных данных третьим лицам сообщение Поверенным таких данных в государственный орган (должностному лицу), орган (должностному лицу), осуществляющий (осуществляющему) государственный контроль (надзор), государственный финансовый контроль, организацию, уполномоченную в соответствии с федеральными законами на осуществление государственного надзора (должностному лицу), орган (должностному лицу), осуществляющий (осуществляющему)

муниципальный контроль, муниципальный финансовый контроль, сведений (информации), представление которых предусмотрено законом и необходимо для осуществления этим органом (должностным лицом) его законной деятельности.

Не считается раскрытием персональных данных третьим лицам предоставление Поверенным доступа к таким данным своим работникам и иным лицам, связанным обязательствами о неразглашении персональных данных, если таким лицам доступ к персональным данным необходим для целей исполнения принятых ими на себя обязательств перед Поверенным.

5. Ответственность сторон

5.1. Доверитель как оператор персональных данных несет полную ответственность перед субъектом персональных данных за действия, осуществляемые Поверенным при обработке персональных данных субъекта.

5.2. Поверенный несет полную ответственность перед Доверителем за действия, производимые при обработке персональных данных субъектов, осуществляемой по поручению Доверителя.

5.3. Поверенный несет ответственность за действия (бездействие) своих сотрудников, получивших доступ к обрабатываемым персональным данным, повлекшие разглашение персональных данных.

5.4. Стороны несут ответственность за несоблюдение условий договора, а также за разглашение или незаконное использование персональных данных в соответствии с действующим законодательством Российской Федерации.

6. Заключительные положения

6.1. Настоящий договор вступает в силу с момента подписания и не имеет ограниченного срока действия.

6.2. Каждая из Сторон вправе в одностороннем порядке отказаться от исполнения настоящего договора, предупредив об этом другую Сторону не менее чем за 30 (Тридцать) календарных дней. По истечении срока предупреждения настоящий договор считается расторгнутым.

6.3. До истечения срока предупреждения, Поверенный обязан передать обрабатываемые персональные данные Доверителю, либо с письменного разрешения Доверителя, уничтожить хранящиеся персональные данные, за исключением случаев, когда уничтожение персональных данных, не может быть произведено в соответствии с действующим законодательством Российской Федерации и/или нормативными актами, регулирующими деятельность Сторон.

6.4. Обязательства по неразглашению персональных данных сохраняются в период действия настоящего договора, а также после выполнения условий по настоящему договору, либо после его расторжения.

6.5. Все вопросы, разногласия или требования, возникающие из настоящего договора или в связи с ним, подлежат урегулированию Сторонами путем переговоров. При отсутствии согласия спор между Сторонами подлежит рассмотрению в суде.

6.6. Ни одна из Сторон не вправе уступать свои права и обязанности по настоящему договору третьим лицам без письменного согласия на то другой Стороны.

6.7. Настоящий договор составлен и подписан в двух экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой Стороны.

7. Реквизиты и подписи сторон

ДОВЕРИТЕЛЬ	ПОВЕРЕННЫЙ
ИНН КПП	ИНН КПП
_____ / _____	_____ / _____
М.П.	М.П.

Приложение 2

к приказу МБУ ДО РР ДЮЦТ

от «19» марта 2021 г. № 24

ПРАВИЛА

рассмотрения запросов субъектов персональных данных,

чьи персональные данные обрабатываются

в МБУ ДО РР ДЮЦТ

23. Общие положения

1.1. Настоящие Правила рассмотрения запросов субъектов персональных данных или их представителей (далее – Правила) определяют порядок учета, рассмотрения и реагирования на запросы субъектов персональных данных (далее – ПДн), чьи ПДн обрабатываются в МБУ ДО РР ДЮЦТ (далее – Оператор) или их представителей.

1.2. Настоящие Правила разработаны в соответствии с действующим законодательством Российской Федерации в области обработки и защиты ПДн.

1.3. Правила обязательны для исполнения всеми работниками Оператора, организующими процедуры учета и обработки обращений субъектов и их законных представителей или непосредственно участвующие в процедурах учета и обработки обращений субъектов и их законных представителей.

1.4. Нарушение Правил влечёт материальную, дисциплинарную, гражданскую, административную и уголовную ответственность в соответствии с нормами действующего законодательства Российской Федерации.

24. Взаимодействие Оператора с субъектами персональных данных

2.1. Ответственным работником Оператора за взаимодействие с субъектами ПДн назначается Ответственный за организацию обработки ПДн.

2.2. Субъекты, ПДн которых обрабатываются Оператором, имеют право:

а) Получать доступ к своим ПДн.

б) Требовать от Оператора уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

в) Получать от Оператора следующую информацию:

- подтверждение факта обработки ПДн Оператором;
- правовые основания обработки ПДн Оператором;
- цели и применяемые Оператором способы обработки ПДн;
- наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Оператором или на основании федерального закона;

- обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки ПДн, в том числе сроки их хранения;
- порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»;
- информацию об осуществленной, осуществляемой или о предполагаемой трансграничной ПДн;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Оператора, если обработка поручена или будет поручена такому лицу.

г) Возражать Оператору относительно принятия на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъектов ПДн или иным образом затрагивающих их права и законные интересы.

д) Обжаловать в уполномоченном органе по защите прав субъектов ПДн или в судебном порядке неправомерные действия или бездействия Оператора при обработке и защите его ПДн.

2.3. Субъекты, ПДн которых обрабатываются Оператором, обязаны предоставлять Оператору достоверные сведения о себе и своевременно информировать об изменении своих ПДн. Оператор имеет право проверять достоверность сведений, предоставленных субъектом, сверяя данные, предоставленные субъектом, с имеющимися у Оператора документами.

2.4. Запросы субъекта или его представителя, поступающие Оператору, фиксируются ответственным за организацию обработки ПДн в «Журнале регистрации обращений субъектов персональных данных, чьи персональные данные обрабатываются в МБУ ДО РР ДЮЦТ, форма которого определена в Приложении к настоящим Правилам).

2.5. В случае поступления запроса в письменной форме субъекта ПДн или его представителя о предоставлении сведений, указанных в подпункте в) пункта 2.2 настоящих Правил, ответственный за организацию обработки ПДн подготавливает, согласно запросу субъекта или его представителя необходимый ответ в письменной форме. В случае требования предоставления иных, непредусмотренных законодательством сведений, ответственный за организацию обработки ПДн подготавливает мотивированный ответ в письменной форме, содержащий ссылку на положение части 8 статьи 14 Федерального закона 27.07.2006 №152-ФЗ «О персональных данных» или иного федерального закона, являющегося основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта ПДн или его представителя либо с даты получения запроса субъекта ПДн или его представителя.

2.6. Необходимые сведения о субъекте ПДн, которые должны присутствовать в подаваемом запросе:

- Фамилия, имя и отчество субъекта ПДн;
- Номер основного документа, удостоверяющего личность субъекта ПДн или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта ПДн или его законного представителя.

Запрос может содержать дополнительные сведения о субъекте ПДн.

2.7. Неправильная форма запроса или отсутствие документов, удостоверяющих личность субъекта ПДн или его законного представителя, может являться основанием для отказа принять запрос.

2.8. Документы, содержащие ПДн субъекта, могут быть отправлены через организацию федеральной почтовой связи. При этом должна быть обеспечена их конфиденциальность. Документы, содержащие ПДн, вкладываются в конверт, к нему прилагается сопроводительное письмо. На конверте делается надпись о том, что содержимое конверта является конфиденциальной информацией, и за незаконное ее разглашение законодательством предусмотрена ответственность. Далее, конверт с сопроводительным письмом вкладывается в другой конверт, на который наносятся только реквизиты, предусмотренные почтовыми правилами для заказных почтовых отправлений.

2.9. Ответственный за организацию обработки ПДн обязан обеспечить текущее хранение нижеуказанных документов в течение трех лет, а по истечении указанного срока – передать документы на архивное хранение:

- запросы субъекта ПДн или его представителя;
- копии документов, являющихся основанием для уточнения или отказа в уточнении обрабатываемых ПДн;
- копии документов, являющихся основанием для прекращения неправомерной обработки ПДн или отказа в прекращении обработки ПДн;
- копии документов, являющихся основанием для отказа в прекращении обработки ПДн;
- уведомления субъекта ПДн или его представителя об уточнении или об отказе уточнения обрабатываемых ПДн;
- уведомления субъекта ПДн или его представителя о прекращении неправомерной обработки ПДн или отказе в прекращении обработки ПДн;
- уведомления субъекта персональных данных или его представителя о прекращении обработки персональных данных или отказе в прекращении обработки персональных данных;
- иные документы и копии иных документов, непосредственно связанные с выполнением Оператором своих обязанностей по рассмотрению запросов субъекта ПДн или его представителя.

25. Обработка запросов об уточнении неполных, устаревших, неточных персональных данных

3.1. В случае запроса субъекта ПДн или его представителя об уточнении Оператором обработки неполных, устаревших, неточных ПДн ответственный за организацию обработки обязан:

а) Зафиксировать наличие запроса субъекта ПДн или его представителя об уточнении обработки неполных, устаревших, неточных ПДн в «Журнале регистрации обращений субъектов персональных данных, чьи персональные данные обрабатываются в МБУ ДО РР ДЮЦТ.

б) Осуществить блокирование указанных ПДн с момента получения запроса на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта ПДн или третьих лиц.

в) Осуществить проверку фактов, изложенных в запросе, и подтверждающих факты документов, предоставляемых субъектом ПДн или его представителем. По результатам проверки может быть получено подтверждение или неподтверждение фактов, изложенных в запросе.

3.2. В случае подтверждения фактов, изложенных в запросе, ответственный за организацию обработки ПДн обязан:

а) Произвести/обеспечить уточнение указанных ПДн на основании представленных сведений в течение семи рабочих дней со дня представления таких сведений.

б) Осуществить снятие блокирования указанных ПДн.

в) В письменной форме уведомить субъекта ПДн или его представителя об устранении допущенных нарушений.

3.3. В случае не подтверждения фактов, изложенных в запросе, ответственный за организацию обработки ПДн обязан:

а) Осуществить снятие блокирования указанных ПДн.

б) В письменной форме уведомить субъекта ПДн или его представителя об отказе в уточнении ПДн.

26. Обработка запросов о прекращении неправомерной обработки персональных данных

4.1. В случае запроса субъекта ПДн или его представителя о прекращении неправомерной обработки Оператором ПДн ответственный за организацию обработки ПДн обязан:

а) Зафиксировать наличие запроса субъекта ПДн или его представителя о прекращении неправомерной обработки ПДн в «Журнале регистрации обращений субъектов персональных данных, чьи персональные данные обрабатываются МБУ ДО РР ДЮЦТ».

б) Осуществить блокирование указанных ПДн с момента получения запроса на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта ПДн или третьих лиц.

в) Осуществить проверку фактов, изложенных в запросе, и подтверждающих факты документов, предоставляемых субъектом ПДн или его представителем. По результатам проверки может быть получено подтверждение или не подтверждение фактов, изложенных в запросе.

4.2. В случае подтверждения факта неправомерной обработки ПДн ответственный за организацию обработки ПДн обязан:

а) Произвести/обеспечить прекращение неправомерной обработки ПДн в срок, не превышающий трех рабочих дней со дня выявления неправомерной обработки ПДн.

б) Если обеспечить правомерность обработки ПДн невозможно, то уничтожить такие ПДн или обеспечить их уничтожение в срок, не превышающий десяти рабочих дней со дня выявления неправомерной обработки ПДн.

в) В письменной форме уведомить субъекта ПДн или его представителя о прекращении неправомерной обработки ПДн.

4.3. В случае не подтверждения факта неправомерной обработки ПДн ответственный за организацию обработки ПДн обязан:

а) Осуществить снятие блокирования указанных ПДн.

б) В письменной форме уведомить субъекта ПДн или его представителя об отказе в прекращении обработки ПДн в срок, не превышающий тридцати дней от даты поступления запроса субъекта ПДн или его представителя о прекращении неправомерной обработки ПДн.

27. Обработка отзывов согласий на обработку персональных данных

5.1. В случае отзыва субъектом ПДн или его представителем согласия на обработку его ПДн Оператором, ответственный за организацию обработки ПДн обязан:

а) Зафиксировать наличие отзыва субъектом ПДн или его представителем согласия на обработку его ПДн в «Журнале регистрации обращений субъектов персональных данных, чьи персональные данные обрабатываются в МБУ ДО РР ДЮЦТ».

б) Организовать принятие решения о прекращении обработки ПДн субъекта (если отсутствуют иные правовые основания для обработки, установленные законодательством РФ).

в) Организовать уничтожение ПДн, согласие на обработку которых было отозвано субъектом ПДн (если отсутствуют иные правовые основания для обработки, установленные законодательством РФ).

г) В письменной форме уведомить субъекта ПДн или его представителя о результатах рассмотрения отзыва согласия на обработку ПДн (в случае наличия соответствующих оснований – об отказе в прекращении обработки ПДн; при этом обязательна ссылка на положения части 2 статьи 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»).

28. Предоставление персональных данных субъектов их представителям, членам их семей и родственникам

6.1. Представителю субъекта (в том числе адвокату) ПДн передаются в порядке, установленном действующим законодательством. Информация передается при наличии одного из документов:

- нотариально удостоверенной доверенности представителя субъекта ПДн.
- письменного заявления субъекта ПДн, написанного в присутствии ответственного за организацию обработки ПДн (если заявление написано субъектом не в присутствии ответственного за организацию обработки ПДн, то оно должно быть нотариально заверено).

6.2. ПДн субъекта могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого субъекта ПДн, за исключением случаев, когда передача ПДн субъекта без его согласия допускается действующим законодательством РФ.

Приложение

к правилам рассмотрения запросов субъектов персональных данных, чьи персональные данные обрабатываются

в МБУ ДО РР ДЮЦТ

ФОРМА

Журнал регистрации обращений субъектов персональных данных, чьи персональные данные обрабатываются

в МБУ ДО РР ДЮЦТ

№ п/п	Дата поступления обращения/ запроса	Сведения о запрашивающем лице (фамилия, имя, отчество, адрес)	Краткое содержание обращения / запроса	Цель запроса	Отметка о предоставлении информации или об отказе в ее предоставлении	Дата предоставления информации / отказа в предоставлении информации	Подпись ответственного за организацию обработки персональных данных	Примечание
1	2	3	4	5	6	7	8	9