МУНИЦИПАЛЬНОЕ ОБРАЗОВАНИЕ
ГОРОД ОКРУЖНОГО ЗНАЧЕНИЯ НИЖНЕВАРТОВСК

МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ ГОРОДА НИЖНЕВАРТОВСКА «ЦЕНТР ДЕТСКОГО ТВОРЧЕСТВА»

ПРИКАЗ

№ 152 «02» апреля 2015 год

Об утверждении локальных нормативных актов
по обеспечению безопасности персональных данных

В соответствии с приказом муниципального автономного учреждения дополнительного образования города Нижневартовска «Центр детского творчества» от 27 марта 2015 года № 240, в целях обеспечения безопасности персональных данных при их обработке, в том числе в информационных системах персональных данных муниципального автономного учреждения дополнительного образования города Нижневартовска «Центр детского творчества» и в соответствии с требованиями Трудового кодекса Российской Федерации, Федерального Закона Российской Федерации «О персональных данных» от 27 июля 2006 года № 152-ФЗ, Постановления Правительства Российской Федерации «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» от 17 ноября 2007 года № 781 и Постановления Правительства Российской Федерации «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15 сентября 2008 года № 687,

ПРИКАЗЫВАЮ:

1. Утвердить следующие локальные нормативные акты по обеспечению безопасности персональных данных при их обработке:

перечень подлежащих защите персональных данных, в том числе обрабатываемых в информационных системах персональных данных учреждения (приложение 1);

список сотрудников, доступ которых к персональным данным необходим для выполнения должностных обязанностей, в том числе обрабатываемых в информационных системах персональных данных (приложение 2);

политику учреждения по обеспечению безопасности персональных данных (приложение 3);

регламент проведения внутренних проверок соблюдения безопасности персональных данных (приложение 4);

инструкцию по резервному копированию, восстановлению работы технических средств, программного обеспечения, баз данных и система защиты информации в учреждении (приложение 5);

инструкцию по организации антивирусной защиты в учреждении (приложение 6);

инструкцию администратора безопасности информационных систем персональных данных учреждения (приложение 7);

инструкцию пользователя информационных систем персональных данных учреждения (приложение 8);

перечень помещений для хранения и обработки персональных данных с указанием ответственных лиц за эти помещения (приложение 9);

положение о постоянно действующей экспертной комиссии по защите информации (приложение 10);

программу обучения правилам защиты персональных данных, в том числе обрабатываемых в информационных системах персональных данных учреждения (приложение 11);

границы контролируемой зоны учреждением (приложение 12).

2. Лицам, ответственным за обеспечение безопасности персональных данных при их обработке постоянно проводить мониторинг законодательства в области защиты персональных данных.

3. Отделу кадрового администрирования и делопроизводства (А.В. Билоцкой):

ознакомить работников с локальными нормативными актами по обеспечению безопасности персональных данных при их обработке;

при приеме на работу знакомить работника под роспись с локальными нормативными актами по обеспечению безопасности персональных данных при их обработке.

4. Методическому ресурсному центру технологий дополнительного образования (Н.М. Шишкиной) разместить локальные нормативные акты по обеспечению безопасности персональных данных при их обработке на официальном сайте учреждения.

5. Локальные нормативные акты по обеспечению безопасности персональных данных при их обработке вступают в силу с момента утверждения и распространяются на правоотношения, возникшие с 01 апреля 2015 года.

6. Контроль исполнения приказа оставляю за собой.

Директор **А.В. Черногалов**

Приложение № 1
к приказу № 152 от «02» апреля 2015 года
«Об утверждении локальных нормативных актов по обеспечению безопасности персональных данных»

УТВЕРЖДЕНО
Приказом от «02» апреля 2015 года
№ 152

ПЕРЕЧЕНЬ,
ПОДЛЕЖАЩИХ ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ,
В ТОМ ЧИСЛЕ ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ УЧРЕЖДЕНИЯ

№ п/п	Содержание сведений
1.	Фамилия, имя, отчество работников
2.	Дата и место рождения работников
3.	Паспортные данные работников (номер, серия, кем и когда выдан)
4.	Идентификационный номер налогоплательщика (ИНН)
5.	Номер обязательного пенсионного страхования (СНИЛС)
6.	Адрес регистрации / адрес места жительства
7.	Контактный номер телефона (стационарный, мобильный)
8.	Гражданство. Национальность.
9.	Семейное положение.
10.	Сведения о составе семьи (фамилия, имя, отчество; дата рождения; адрес регистрации / проживания; место работы / учебы; контактный номер телефона)
11.	Сведения о воинском учете.
12.	Сведения об образовании, повышении квалификации и переподготовке работника (профессия, специальность, наименование образовательного учреждения, период обучения)
13.	Сведения о трудовой деятельности (серия и номер трудовой книжки; стаж работы; наименование предшествующих работодателей и причины увольнения)
14.	Занимаемая должность, профессия.
15.	Сведения, содержащиеся в трудовом договоре, приказах по личному составу, личной карточке формы Т-2 (оригиналы и копии, указанных документов)
16.	Табельный номер работника.
17.	Материалы, содержащие сведения по аттестации работников, служебным расследованиям
18.	Материалы, содержащие сведения о начисленной заработной плате работника
19.	Личные дела работников
20.	Сведения, содержащие медицинские данные работников (личные медицинские книжки, результаты обследований)
21.	Материалы, содержащие сведения о предоставляемых работнику социальных льготах

22.	Сведения о наличии (отсутствии) судимости (в том числе погашенной и снятой) или о факте уголовного преследования либо о прекращении уголовного преследования
23.	Сведения, содержащиеся в налоговой декларации
24.	Статистические и иные отчеты, направляемые в государственные, региональные и муниципальные органы.
25.	Фамилия, имя, отчество обучающихся и их законных представителей
26.	Дата и место рождения обучающихся и их законных представителей
27.	Паспортные данные / данные свидетельства о рождении обучающихся и их законных представителей (номер, серия, кем и когда выдан)
28.	Адрес регистрации / адрес места жительства обучающихся и их законных представителей
29.	Контактный номер телефона (стационарный, мобильный) обучающихся и их законных представителей
30.	Сведения, содержащие медицинские данные обучающихся (результаты медицинского обследования)
31.	Личные дела обучающихся

Приложение № 2
к приказу № 152 от «02» апреля 2015 года
«Об утверждении локальных нормативных актов по обеспечению безопасности персональных данных»

УТВЕРЖДЕНО
Приказом от «01» апреля 2015 года
№ 152

СПИСОК СОТРУДНИКОВ, ДОСТУП КОТОРЫХ К ПЕРСОНАЛЬНЫМ ДАННЫМ НЕОБХОДИМ ДЛЯ ВЫПОЛНЕНИЯ ДОЛЖНОСТНЫХ ОБЯЗАННОСТЕЙ, В ТОМ ЧИСЛЕ ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

№ п/п	Категория работников (должность)	Состав обрабатываемых ПДн	Обработка с использованием ИСПДн (да,нет)	Без использования ИСПДн (да,нет)
1.	Директор учреждения	Весь перечень ПДн	нет	нет
2.	Заместители директора по УВР, УВР и (КБ)	- анкетные и биографические данные (обучающихся, работников); - сведения о трудовом и общем стаже; - дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям; - адрес места жительства (обучающихся, работников); - домашний и (или) мобильный телефон родителей законных представителей, работников; - копии отчетов, направляемые в органы статистики.	Нет	нет
3.	Главный бухгалтер; Бухгалтер; Экономист.	- анкетные и биографические данные; - сведения о трудовом и общем стаже; - паспортные данные; - сведения о заработной плате сотрудника; - сведения о социальных льготах; - специальность; - занимаемая должность; - адрес места жительства; - домашний телефон (мобильный); - страховое свидетельство государственного пенсионного	Да	да

		страхования; - свидетельство о присвоении ИНН; - содержание трудового договора; - копии отчетов, направляемые в органы статистики.		
4.	Заместитель директора по АХР; Заведующий хозяйством.	- адрес места жительства; - домашний телефон (мобильный); - анкетные и биографические данные; - сведения о трудовом и общем стаже; - паспортные данные; - сведения о заработной плате сотрудника; - сведения о социальных льготах; - специальность; - копии отчетов, направляемые в органы статистики.	Нет	да
5.	Заведующий отдела кадрового администрирования и делопроизводства; Специалист по кадрам; Делопроизводитель; Архивариус.	- анкетные и биографические данные; - образование; - сведения о трудовом и общем стаже; - сведения о составе семьи; - паспортные данные; - сведения о воинском учете; - сведения о социальных льготах; - специальность; - занимаемая должность; - наличие судимостей; - адрес места жительства; - домашний телефон; - место работы или учебы членов семьи и родственников; - страховое свидетельство государственного пенсионного страхования; - свидетельство о присвоении ИНН; - содержание трудового договора; - подлинники и копии приказов по личному составу; - личные дела сотрудников и обучающихся; - трудовые книжки; - дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям; - копии отчетов, направляемые в органы статистики; - результаты медицинского обследования.	да	да
6.	Секретарь руководителя.	- анкетные и биографические данные; - адрес места жительства; - домашний телефон, мобильный; - подлинники и копии приказов по личному составу;	Да	да

		- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям; - копии отчетов, направляемые в органы статистики.		
7.	Секретарь учебной части.	- анкетные и биографические данные (обучающихся); - адрес места жительства (обучающихся); - домашний телефон (или) мобильный (родителей законных представителей); - дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям; - образование; - сведения о трудовом и общем стаже.	Нет	да
8.	Методист.	- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям; - специальность; - занимаемая должность; - анкетные и биографические данные; - образование; - сведения о трудовом и общем стаже; - паспортные данные. - копии отчетов, направляемые в органы статистики.	Да	да
9.	Руководитель ресурсного центра, отдела, службы.	- анкетные и биографические данные; - сведения о трудовом и общем стаже; - адрес места жительства; - домашний телефон или мобильный; - личные дела обучающихся; - сведения о заработной плате сотрудника; - сведения о социальных льготах; - специальность; - занимаемая должность; - дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям; - копии отчетов, направляемые в органы статистики.	Нет	да
10.	Педагог дополнительного образования;	- анкетные и биографические данные (обучающихся);	Нет	да

	Педагог организатор.	- адрес места жительства (обучающихся); - домашний телефон (родителей законных представителей).		
11.	Председатель профсоюзного комитета; Члены ПК.	- анкетные и биографические данные; - паспортные данные; - адрес места жительства; - домашний телефон или мобильный; - занимаемая должность; - сведения о трудовом и общем стаже; - копии отчетов, направляемые в органы статистики.	Нет	да
12.	Уполномоченный по ГО и ЧС.	- анкетные и биографические данные; - паспортные данные; - адрес места жительства; - домашний телефон или мобильный; - занимаемая должность; - место работы или учебы членов семьи и родственников; - сведения о составе семьи.		

Приложение № 3
к приказу № 152 от «01» апреля 2015 года
«Об утверждении локальных нормативных актов
по обеспечению безопасности персональных данных»

УТВЕРЖДЕНО
Приказом от «01» апреля 2015 года
№ 152

ПОЛИТИКА УЧРЕЖДЕНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

1.1. Настоящая Политика оператора в отношении обработки персональных данных (далее - ПДн) (далее - Политика) в МАУДО г. Нижневартовска «Центр детского творчества» (далее - Оператор) характеризуется следующими признаками:

1.2. Разработана в целях обеспечения реализации требований законодательства Российской Федерации в области обработки ПДн субъектов ПДн: Конституции Российской Федерации, Трудового кодекса Российской федерации (глава 14), Федерального закона от 27.07.2006 года № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 15.09.2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановления Правительства Российской Федерации от 01.11.2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных, Федерального законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», Федерального закона от 21.11.1996 № 129-ФЗ «О бухгалтерском учёте», Федерального закона от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации», Закона Российской Федерации от 25.07.2002г.№113-ФЗ «Об альтернативной гражданской службе», Федерального закона Российской Федерации от 29.12.2012г. № 273 «Об образовании в Российской Федерации», Законодательными актами Ханты - Мансийского автономного округа - Югры, распоряжениями администрации города Нижневартовска, приказами Департамента образования и молодежной политики ХМАО-Югры, приказами Департамента образования администрации города Нижневартовска, Уставом МАУДО г. Нижневартовска «Центр детского творчества», Локальными актами учреждения.

1.3. Раскрывает основные категории ПДн, обрабатываемых Оператором, цели, способы и принципы обработки Оператором ПДн, права и обязанности Оператора при обработке ПДн, права субъектов ПДн, а также включает перечень мер, применяемых Оператором в целях обеспечения безопасности ПДн при их обработке.

1.4. Является общедоступным документом, декларирующим

концептуальные основы деятельности Оператора при обработке ПДн.

2. Информация об Операторе

Наименование: Муниципальное автономное учреждение дополнительного образования г. Нижневартовска «Центр детского творчества».

ИНН: 8603006462.

Фактический адрес: 628609, Российская Федерация, Тюменская область, Ханты-Мансийский автономный округ – Югра, город Нижневартовск, улица Ленина, дом 9 «а».

Тел., факс: 8 (3466) 67-24-80.

3. Основные понятия и состав персональных данных

Персональные данные работника - информация, необходимая работодателю в связи с трудовыми отношениями и касающиеся конкретного работника. Под информацией о работниках понимаются сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.

Для целей настоящей Политики используются следующие понятия:

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

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

Субъект - субъект ПДн.

Работник - физическое лицо, состоящее в трудовых отношениях с оператором.

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

Распространение ПДн - действия, направленные на раскрытие ПДн неопределенному кругу лиц.

Автоматизированная обработка ПДн - обработка ПДн с помощью средств вычислительной техники.

Предоставление ПДн - действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.

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

Уничтожение ПДн - действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе

персональных данных (далее - ИСПДн) и (или) в результате которых уничтожаются материальные носители ПДн.

Обезличивание ПДн - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

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

Трансграничная передача ПДн - передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

В состав персональных данных входят:

- анкетные и биографические данные;
- образование;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- место работы или учебы членов семьи и родственников;
- страховое свидетельство государственного пенсионного страхования;
- свидетельство о присвоении ИНН;
- содержание трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела сотрудников и обучающихся;
- трудовые книжки;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики;
- результаты медицинского обследования.

4. Цели обработки ПДн

Оператор обрабатывает ПДн исключительно в целях исполнения положений нормативных актов, указанных в п. 1.2.

5. Категории субъектов ПДн, сроки обработки и хранения

5.1. В ИСПДн Оператора обрабатываются следующие категории ПДн:
Уволенных сотрудников Оператора;
Физических лиц состоящих с оператором в договорных отношениях;
Физических лиц, являющихся обучающимися, родителями (законными представителями) либо ближайшими родственниками обучающихся.

5.2. Сроки обработки и хранения ПДн определены внутренней организационно-распорядительной документацией.

6. Основные принципы обработки, передачи и хранения ПДн

6.1. Под обработкой персональных данных понимается любое действие, совершаемое 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.

6.2. Обработка персональных данных оператором МАУДО г. Нижневартовска «ЦДТ» осуществляется на основании следующих принципов:

1) обработка должна осуществляться на законной и справедливой основе;

2) обработка должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка, несовместимая с целями сбора персональных данных;

3) не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

4) обработке подлежат только те персональные данные, которые отвечают целям обработки;

5) содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Не допускается обработка избыточных данных по отношению к заявленным целям обработки;

6) при обработке должны быть обеспечены точность и достаточность персональных данных, а в необходимых случаях - актуальность по отношению к целям обработки. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных;

7) форма хранения персональных данных должна позволять определять субъекта этих данных. Хранение не должно длиться дольше, чем этого требуют цели обработки, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено действующим законодательством.

6.3. Оператор не производит трансграничную (на территорию

иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу) передачу ПДн.

6.4. Оператором не создаются общедоступные источники ПДн.

7. Основные принципы обработки, передачи и хранения ПДн

7.1 Оператор в своей деятельности обеспечивает соблюдение принципов обработки ПДн, указанных в ст. 5 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

7.2. Оператор не осуществляет обработку биометрических ПДн (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность).

7.3. Оператор не производит трансграничную (на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу) передачу ПДн.

7.4. Оператором не создаются общедоступные источники ПДн.

8. Сведения о третьих лицах, участвующих в обработке ПДн

8.1. В целях соблюдения законодательства Российской Федерации, для достижения целей обработки, а также в интересах и с согласия субъектов ПДн Оператор в ходе своей деятельности предоставляет ПДн следующим организациям:

– Федеральной налоговой службе;
– Пенсионному фонду России;
– Негосударственным пенсионным фондам;
– Страховым компаниям;
– Кредитным организациям;
– Контролирующим органам государственной власти и местного самоуправления;
– Организациям, указанным в нормативно правовых актах пункта 4.1 настоящей Политики.

8.2. Оператор не поручает обработку ПДн другим лицам на основании договора.

8.3. Оператор по организованному защищенному каналу связи подключается к базе данных размещенной на серверных мощностях сторонней организации.

8.4. Подключение осуществляется для выполнения должностных обязанностей, связанных с обработкой ПДн сотрудников Оператора.

8.5. Между оператором и сторонней организацией заключен договор на предоставление серверных мощностей для осуществления обработки ПДн.

8.6. В договоре оговорены все зоны ответственности Сторон, участвующих в процессе обработки ПДн.

9. Меры по обеспечению безопасности ПДн при их обработке

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

– Назначением ответственных за организацию обработки ПДн;

– Осуществлением внутреннего контроля и аудита соответствия обработки ПДн Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, локальным актам;

– Ознакомлением работников Оператора, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе с требованиями к защите ПДн, локальными актами в отношении обработки ПДн, и обучением указанных сотрудников;

– Определением угроз безопасности ПДн при их обработке в ИСПДн;

– Применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн;

– Оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;

– Учетом машинных носителей ПДн;

– Выявлением фактов несанкционированного доступа к ПДн и принятием соответствующих мер;

– Восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– Установлением правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;

– Контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровнем защищенности ИСПДн.

9.2.Обязанности должностных лиц, осуществляющих обработку и защиту ПДн, а также их ответственность, определяются приказами Оператора.

10. Обработка ПДн

10.1. **Общие требования при обработке ПДн.**

В целях обеспечения прав и свобод человека и гражданина при обработке ПДн соблюдаются следующие требования:

10.1.1. Обработка ПДн осуществляется с согласия субъекта ПДн на обработку его ПДн;

10.1.2. Обработка ПДн при отсутствии согласия субъекта на обработку ПДн допускается в следующих случаях:

– необходима для достижения целей, предусмотренных международным

договором Российской Федерации или законом, для осуществления и выполнения, возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

– необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее - исполнение судебного акта);

– необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора,

– по которому субъект ПДн будет являться выгодоприобретателем или поручителем;

– необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно;

– необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;

– необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта ПДн;

– осуществляется в статистических или иных исследовательских целях при условии

–

обязательного обезличивания ПДн за исключением целей, указанных в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных»;

– осуществляется обработка ПДн, доступ неограниченного круга лиц, к которым предоставлен субъектом ПДн либо по его просьбе (далее - ПДн, сделанные общедоступными субъектом ПДн);

– осуществляется обработка ПДн, подлежащих опубликованию или бязательному раскрытию в соответствии с федеральным законом.

10.1.3. Обработка ПДн должна осуществляться на законной и справедливой основе.

10.1.4. Обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн.

10.1.5. Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

10.1.6. Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.

10.1.7. При обработке ПДн должны быть обеспечены точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

10.1.8. Субъекты ПДн не должны отказываться от своих прав на сохранение и защиту ПДн.

10.1.9. Порядок рассмотрения запросов субъектов ПДн или их представителей осуществляется в соответствии с «Инструкцией по обработке запросов субъекта персональных данных или уполномоченного органа по защите прав субъектов персональных данных», утвержденной Оператором.

10.2. **Получение ПДн:**

10.2.1. Все ПДн следует получать непосредственно от субъекта ПДн. Субъект самостоятельно принимает решение о предоставление своих ПДн и дает письменное согласие на их обработку оператором. Типовая форма заявления-согласия субъекта на обработку ПДн представлена в приложении 1 к настоящей Политике.

10.2.2. Если предоставление ПДн является обязательным в соответствии с федеральным законом, оператор обязан разъяснить субъекту ПДн юридические последствия отказа предоставить его ПДн. Типовая форма разъяснений субъекту ПДн юридических последствий отказа предоставить свои ПДн приведена в приложении 6 к настоящей Политике.

10.2.3. В случае недееспособности либо несовершеннолетия субъекта ПДн все ПДн субъекта следует получать от его законных представителей. Законный представитель самостоятельно принимает решение о предоставлении ПДн своего подопечного и дает письменное согласие на их обработку оператором. Типовая форма заявления-согласия на обработку ПДн подопечного представлена в приложении 2 к настоящей Политике.

10.2.4. Письменное согласие не требуется, если обработка ПДн осуществляется в случаях, указанных в пункте 10.1.2 настоящей Политике.

10.2.5. Согласие на обработку ПДн может быть отозвано субъектом ПДн. В случаях, указанных в пункте 10.2.3. настоящей Политики согласие может быть отозвано законным представителем субъекта ПДн. Типовая форма отзыва согласия на обработку ПДн представлена в приложении 3 к настоящей Политике.

10.2.6. В случаях, когда оператор может получить необходимые ПДн субъекта только у третьей стороны, субъект должен быть уведомлен об этом заранее. В уведомлении оператор обязан указать:

- наименование и адрес оператора;
- цель обработки ПДн и ее правовое основание;
- предполагаемые пользователи ПДн;
- права субъекта ПДн;
- источник получения ПДн.

Типовая форма уведомления субъекта о получении его ПДн от третьей стороны представлена в приложении 4 к настоящей Политике.

10.2.7. Запрещается получать и обрабатывать ПДн субъекта о его религиозных и иных убеждениях и частной жизни.

10.2.8. Запрещается получать и обрабатывать ПДн субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

10.2.9. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации оператор вправе получать и обрабатывать данные о частной жизни субъекта

только с его письменного согласия.

10.3. **Хранение ПДн**:

10.3.1. Хранение ПДн субъектов осуществляется структурными подразделениями оператора в соответствии с перечнями ПДн и ИСПДн, утвержденными у Оператора.

10.3.2. Личные дела сотрудников хранятся в бумажном виде в папках, прошитые и пронумерованные по страницам. Личные дела хранятся в специально отведенной секции сейфа (или металлических шкафах), обеспечивающего защиту от несанкционированного доступа.

10.3.3. Подразделения, хранящие ПДн на бумажных носителях, обеспечивают их защиту от несанкционированного доступа и копирования согласно постановлению Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

10.4. **Передача ПДн:**

10.4.1. При передаче ПДн субъекта оператор обязан соблюдать следующие требования:

– не сообщать ПДн субъекта третьей стороне без письменного согласия субъекта или его законного представителя, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, предусмотренных Трудовым Кодексом Российской Федерации или иными федеральными законами. Форма заявления-согласия субъекта на передачу его ПДн третьей стороне см. в приложении 5 настоящей Политики;

– предупредить лиц, получающих ПДн субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие ПДн субъекта, обязаны соблюдать требования конфиденциальности;

– не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения им трудовой функции;

– передавать ПДн субъекта представителям субъектов в порядке, установленном Трудовым Кодексом Российской Федерации, и ограничивать эту информацию только теми ПДн субъекта, которые необходимы для выполнения указанными представителями их функций;

– все сведения о передаче ПДн субъекта регистрируются в Журнале учета передачи ПДн в целях контроля правомерности использования данной информации лицами, ее получившими. В журнале фиксируются сведения о лице, направившем запрос, дата передачи ПДн или дата уведомления об отказе в их предоставлении, а также отмечается, какая именно информация была передана.

10.4.2. Все меры конфиденциальности при сборе, обработке и хранении ПДн субъекта распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

10.4.3. Доступ работников к ПДн разрешен в соответствии со списками, утвержденными приказом от 21.01.2015 № 14 «Об организации работ по обеспечению безопасности персональных данных при их обработке, в том числе в информационных системах персональных данных».

10.4.4. Все сотрудники, имеющие доступ к ПДн субъектов, обязаны подписать обязательство о неразглашении ПДн.

10.4.5. Передача ПДн осуществляется в организации, указанные в пункте 8 настоящей Политики.

10.5. **Уничтожение ПДн:**

10.5.1. ПДн субъектов хранятся не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

10.5.2. Документы, содержащие ПДн, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.

11. Права и обязанности субъектов ПДн и оператора

11.1. Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

- подтверждение факта обработки ПДн оператором;
- правовые основания и цели обработки ПДн;
- 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 или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка поручена или будет поручена такому лицу;

- иные сведения, предусмотренные действующим законодательством Российской Федерации.

11.2. В целях обеспечения защиты ПДн субъекты имеют право:

- требовать от оператора уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;
- требовать предоставления сведений, указанных в пункте 11.1, от оператора в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если

имеются законные основания для раскрытия таких ПДн;

– требовать предоставления сведений, указанных в пункте 11.1, от оператора при обращении либо при получении запроса субъекта ПДн или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПДн в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн оператором, подпись субъекта ПДн или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации;

– требовать исключения или исправления неверных или неполных ПДн, а также данных, обработанных с нарушением законодательства;

– при отказе оператора или уполномоченного им лица исключить или исправить ПДн субъекта - заявить в письменной форме о своем несогласии, представив соответствующее обоснование;

– дополнить ПДн оценочного характера заявлением, выражающим его собственную точку зрения;

– требовать от оператора или уполномоченного им лица уведомления всех лиц, которым ранее были сообщены неверные или неполные ПДн субъекта, обо всех произведенных в них изменениях или исключениях из них;

– обжаловать в суд любые неправомерные действия или бездействие оператора или уполномоченного им лица при обработке и защите ПДн субъекта.

11.3. Субъект ПДн или его законный представитель обязуется предоставлять ПДн, соответствующие действительности.

12. Ответственность за нарушение норм, регулирующих обработку и защиту ПДн

12.1. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, содержащему ПДн, несет персональную ответственность за данное разрешение.

12.2. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым Кодексом Российской Федерации и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

Приложение № 1
к Политике учреждения
по обеспечению безопасности персональных данных

Типовая форма
заявления-согласия субъекта на обработку его персональных данных

Я, _____

проживающий (- ая) по адресу_____

паспорт серии _____ , номер_____ выданный _____

« __» _____ года, в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», даю согласие МАУДО г. Нижневартовска «Центр детского творчества», расположенной по адресу 628609, Тюменская область, Ханты-Мансийский автономный округ-Югра, г. Нижневартовск, ул. Ленина, д. 9 «а», на обработку моих персональных данных, а именно:

(указать состав персональных данных (Ф.И.О, паспортные данные, адрес ...)

Обработка вышеуказанных персональных данных будет осуществляться путем:_____

(Перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных)

Для обработки в целях:

Я утверждаю, что ознакомлен с документами организации, устанавливающими порядок обработки персональных данных, а также с моими правами и обязанностями в этой области.

Мне разъяснены юридические последствия отказа предоставить мои персональные данные Оператору.

Согласие вступает в силу со дня его подписания и действует в течение_____. Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

_____

«_____» _____20____г. _____

подпись

Приложение № 2
к Политике учреждения
по обеспечению безопасности персональных данных

Типовая форма
заявления-согласия субъекта на обработку
персональных данных законного представителя

Я, _____
проживающий (-ая) по адресу_____
паспорт серии _____ , номер _____ , выданный_____

« __ » _____ года, в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», даю согласие МАУДО г. Нижневартовска «Центр детского творчества», расположенной по адресу 628609, Тюменская область, Ханты-Мансийский автономный округ-Югра, г. Нижневартовск, ул. Ленина, д. 9 «а» персональных данных моего/ей сына (дочери, подопечного):

(Ф.И.О. сына, дочери, подопечного)

а именно:

(указать состав персональных данных (Ф.И.О, паспортные данные, адрес ...)

Обработка вышеуказанных персональных данных будет осуществляться путем:

(Перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных)

Для обработки в целях:

Я утверждаю, что ознакомлен с документами организации, устанавливающими порядок обработки персональных данных, а также с моими правами и обязанностями в этой области.

Мне разъяснены юридические последствия отказа предоставить персональные данные Оператору.

Согласие вступает в силу со дня его подписания и действует в течение_____. Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

«_____» _____20____г. _____

подпись

Приложение № 3
к Политике учреждения
по обеспечению безопасности персональных данных

наименование оператора

адрес оператора

Ф.И.О. субъекта персональных данных

адрес регистрации субъекта персональных данных

наименование, серия и номер основного документа, удостоверяющего личность

дата выдачи указанного документа

наименование органа, выдавшего документ

Типовая форма
отзыва согласия на обработку персональных данных

Прошу прекратить обработку моих персональных данных в связи с _____
_____
_____
(указать причину)

«_____» _____20____г. _____
подпись

Приложение № 4
к Политике учреждения
по обеспечению безопасности персональных данных

Типовая форма
уведомления субъекта о начале обработки его персональных данных, полученных у третьей стороны.

_____,
(фамилия, имя, отчество,

адрес субъекта персональных данных)

МАУДО г. Нижневартовска «Центр детского творчества», расположенная по адресу 628609, Тюменская область, Ханты-Мансийский автономный округ-Югра, г. Нижневартовск, ул. Ленина, д. 9 «а», уведомляет Вас о начале обработки Ваших персональных данных с целью

(цель обработки персональных данных)

на основании положений _____.
Персональные данные, а именно _____,
получены от _____.

К Вашим персональным данным имеют доступ следующие категории сотрудников

Согласно Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» Вы имеете право:

- на получение сведений о МАУДО г. Нижневартовска «Центр детского творчества» (далее - Оператор), как операторе персональных данных, месте его нахождения, о наличии оператора Ваших персональных данных;
- на ознакомление с Вашими персональными данными, если это не влечет за собой нарушения конституционных права и свободы других лиц;
- требовать от оператора уточнения Ваших персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите Ваших прав;
- получать при обращении информацию, касающуюся обработки Ваших персональных данных, в том числе содержащую:
- подтверждение факта обработки, а также цель такой обработки;
- способы обработки, применяемые оператором;
- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки Ваших персональных данных, в том числе сроки их хранения.
- в случаях возникновения оснований считать, что оператор осуществляет обработку Ваших персональных данных с нарушением требований Федерального закона или иным образом нарушает Ваши права и свободы, обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке;
- на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

«_____» _____20____г. _____
подпись

Приложение № 5
к Политике учреждения
по обеспечению безопасности персональных данных

Типовая форма
заявления-согласия субъекта на передачу его персональных данных третьей стороне

Я, _____,
проживающий(-ая) по адресу по
паспорт серия _____, номер_____выданный « ___» _____ года, в соответствии со ст. 12 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», даю согласие на передачу моих персональных данных МАУДО г. Нижневартовска «Центр детского творчества», расположенной по адресу 628609, Тюменская область, Ханты-Мансийский автономный округ-Югра, г. Нижневартовск, ул. Ленина, д. 9 «а», а именно:

(указать состав персональных данных (Ф.И.О, паспортные данные, адрес …)

Обработка вышеуказанных персональных данных будет осуществляться путем: *(Перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных)*
для обработки в целях:

следующим лицам:

(указать Ф.И.О. физического лица или наименование организации и адрес, которым сообщаются данные)

Я также утверждаю, что ознакомлен с документами организации, устанавливающими порядок обработки персональных данных, а также с моими правами и обязанностями в этой области.

Согласие вступает в силу со дня его подписания и действует в течение _____. Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

«_____» _____20____г. _____
подпись

Приложение № 6
к Политике учреждения
по обеспечению безопасности персональных данных

Разъяснение
юридических последствий отказа предоставить свои персональные данные,
субъектом в связи с _____

Мне, _____

разъяснены юридические последствия отказа предоставить свои персональные данные МАУДО г. Нижневартовска «Центр детского творчества».

В соответствии с _____ субъект персональных данных обязан представить определенный перечень информации о себе.

Без представления субъектом персональных данных обязательных для, субъекту не может

«_____» _____20____г. _____

подпись

Приложение № 4
к приказу № 252 от «01» апреля 2015 года
«Об утверждении локальных нормативных актов по обеспечению безопасности персональных данных»

УТВЕРЖДЕНО
Приказом от «1» апреля 2015 года
№ 252

РЕГЛАМЕНТ
проведения внутренних проверок соблюдения безопасности персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Регламент осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в муниципальном автономном учреждении дополнительного образования города Нижневартовска «Центр детского творчества» (далее – Регламент) разработан с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».
1.2. Настоящие Регламент определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в муниципальном автономном учреждении дополнительного образования города Нижневартовска «Центр детского творчества» (далее – учреждение) и действуют постоянно.
1.3. Исполнение данного Регламента обязательно для всех работников учреждения, осуществляющих обработку персональных данных (далее – ПДн), как без использования средств автоматизации, так и в информационных системах обработки персональных данных (далее – ИСПДн).

2. ПОРЯДОК ПРОВЕДЕНИЯ ВНУТРЕННИХ ПРОВЕРОК

2.1. Внутренний контроль соответствия обработки персональных данных установленным требованиям в учреждении организуется на основе проведения периодических проверок условий обработки ПДн в соответствии с планом, утверждаемым директором учреждения.
2.2. Проверки осуществляются администратором ИСПДн либо действующей в учреждении экспертной комиссией по защите информации.
2.3. Внутренние проверки могут проводиться по необходимости в соответствии с отдельным поручением директора учреждения
2.4. Проверки осуществляются непосредственно на местах обработки персональных данных путем опроса либо, при необходимости, путем

осмотра рабочих мест работников учреждения, допущенных к обработке персональных данных.
2.5. Результаты каждой проверки оформляются протоколом проведения внутренней проверки.
2.6. При выявлении в ходе проверки нарушений в протоколе делается запись о мероприятиях, необходимых для устранения нарушений, сроках исполнения и ответственных лицах.
2.7. Протоколы проверок хранятся в отделе кадров. Протоколы уничтожаются комиссией после окончания года, в течение которого проводились проверки.
2.8. Администратор ИСПДн либо председатель комиссии обязаны информировать директора учреждения по результатам всех проверок, в результате которых были выявлены нарушения, а также о мерах, которые необходимо принять для их устранения.

3. СОДЕРЖАНИЕ ПРОВЕРОК ВНУТРЕННЕГО КОНТРОЛЯ

3.1. В процессе проверки соответствия обработки персональных данных без использования средств автоматизации требованиям к защите персональных данных должно быть установлено:
- порядок и условия хранения бумажных носителей, содержащих персональные данные работников и обучающихся учреждения;
- соблюдение правил доступа к бумажным носителям с персональными данными;
- условия доступа в помещения, где обрабатываются и хранятся бумажные носители с персональными данными;
- наличие или отсутствие фактов несанкционированного доступа к персональным данным и необходимость принятия дополнительных мер по обеспечению безопасности ПДн.
3.2. При проведении проверки соответствия обработки персональных данных в ИСПДн учреждения требованиям к защите персональных данных должно быть установлено:
- соответствие используемых пользователями ИСПДн полномочий параметрам (матрице) доступа, установленной в соответствии с Положением о разграничении прав доступа к обрабатываемым персональным данным в ИСПДн учреждения;
- соблюдение пользователями ИСПДн парольной политики, установленной в соответствии с инструкцией по формированию, распределению и применению паролей в ИСПДн учреждения;
- соблюдение пользователями ИСПДн антивирусной политики в соответствии с требованиями инструкции по организации антивирусной защиты в учреждении;
- соблюдение пользователями ИСПДн правил работы со съемными носителями персональных данных, установленных инструкцией о порядке учета и хранения в учреждении съемных носителей конфиденциальной информации;

- соблюдение порядка доступа в помещения учреждения, где расположены элементы ИСПДн;
- соблюдение порядка резервирования баз данных и хранения резервных копий, установленного инструкцией о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в ИСПДн учреждения;
- своевременность проведения мероприятий по обезличиванию персональных данных в соответствии с политикой учреждения в отношении обработки персональных данных;
- знание пользователями ИСПДн своих действий во внештатных ситуациях.
- наличие или отсутствие фактов несанкционированного доступа к ИСПДн и необходимость принятия дополнительных мер по обеспечению безопасности ПДн.
- необходимость мероприятий по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

Приложение № 1
к Регламенту проведения внутренних
проверок соблюдения безопасности персональных данных

План
проведения внутренних проверок условий обработки персональных данных в МАУДО г. Нижневартовска «Центр детского творчества»
в 2015 году

№ п/п	Тема проверки	Срок проведения	Исполнитель
1.	Соблюдение работниками учреждения, ответственных за обработку персональных данных правил обработки персональных данных.	Не реже одного раза в квартал	Члены постоянно действующей экспертной комиссии по защите информации - (ПДЭК по ЗИ)
2.	Соблюдение ответственным работником учреждения, за регистрацию запросов субъектов персональных данных или их представителей, правил рассмотрения обращений.	Не реже одного раза в пол года	Члены ПДЭК по ЗИ
3.	Соблюдение работниками учреждения, ответственных за обработку персональных данных, правил порядка доступа в помещения, в которых ведется обработка персональных данных.	Не реже одного раза в квартал	Члены ПДЭК по ЗИ
4.	Соблюдение работниками учреждения, работающими в информационных системах, парольной и антивирусной политики, использования ими средств защиты информации.	Не реже одного раза в квартал	Члены ПДЭК по ЗИ

Приложение № 2
к Регламенту проведения внутренних
проверок соблюдения безопасности персональных данных

Протокол
проведения внутренней проверки условий обработки персональных данных

Настоящий Протокол составлен в том, что __._____.20__
ответственным за организацию обработки персональных данных ПДЭК по ЗИ проведена проверка

_____

тема проверки

Проверка осуществлялась в соответствии с требованиями

_____

_____

название документа

В ходе проверки проверено:

_____

_____

_____

_____

_____

_____

_____

Выявленные нарушения:

_____

_____

_____

_____

_____

_____

_____

Меры по устранению нарушений:

_____

_____

_____

_____

_____

_____

_____

Срок устранения нарушений: _____

Должность ответственного _____

Председатель комиссии_____
Члены комиссии:
Должность _____
Должность _____
Должность _____

Должность, Ф.И.О., роспись
руководителя проверяемого
структурного подразделения _____

Приложение № 5
к приказу № 152 от «02» апреля 2015 года
«Об утверждении локальных нормативных актов по обеспечению безопасности персональных данных»

УТВЕРЖДЕНО
Приказом от «02» апреля 2015 года
№ 152

ИНСТРУКЦИЯ ПО РЕЗЕРВНОМУ КОПИРОВАНИЮ, ВОССТАНОВЛЕНИЮ РАБОТЫ ТЕХНИЧЕСКИХ СРЕДСТВ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, БАЗ ДАННЫХ И СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ В УЧРЕЖДЕНИИ

1. Назначение и область действия

Порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ определяет действия (далее – Инструкция), связанные с функционированием ИСПДн МАУДО г. Нижневартовска «ЦДТ», меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

Целью настоящего документа является превентивная защита элементов ИСПДн от предотвращения потери защищаемой информации.

Задачей данной Инструкции является:

- определение мер защиты от потери информации;
- определение действий восстановления в случае потери информации.

Действие настоящей Инструкции распространяется на всех пользователей (наименование оператора), имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже одного раза в два года.

Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается Администратор ИСПДн _____.

Ответственным сотрудником за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, назначается Администратор безопасности _____.

2.Порядок реагирования на инцидент.

В настоящем документе под Инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а так же потерей защищаемой информации.

Происшествие, вызывающее инцидент, может произойти:

- в результате непреднамеренных действий пользователей;
- в результате преднамеренных действий пользователей и третьих лиц;
- в результате нарушения правил эксплуатации технических средств ИСПДн;
- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники (наименование оператора) (Администратор безопасности, Администратор и Оператор ИСПДн), предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с

вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

3.1 Технические меры.

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов, такие как:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

Все критичные помещения (наименование оператора) (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
- дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т. д.);
- резервные линии электропитания в пределах комплекса зданий;
- аварийные электрогенераторы.

Системы обеспечения отказоустойчивости:

- кластеризация;
- технология RAID.

Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации. Могут использоваться следующие методы кластеризации: для наиболее критичных компонентов ИСПДн должны использоваться территориально удаленные системы кластеров.

Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск и т.п.).

3.2 Организационные меры

Резервное копирование и хранение данных должно осуществлять на периодической основе:

- для обрабатываемых персональных данных – не реже раза в неделю;
- для технологической информации – не реже раза в месяц;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

Данные о проведение процедуры резервного копирования, должны отражаться в специально созданном журнале учета.
Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.
Носители должны храниться в несгораемом шкафу или помещении оборудованном системой пожаротушения.
Носители должны храниться не менее года, для возможности восстановления данных.

Приложение 6
к приказу № 152 от «02» апреля 2015 года
«Об утверждении локальных нормативных актов по обеспечению безопасности персональных данных»

УТВЕРЖДЕНО
Приказом от «02» апреля 2015 года
№ 152

Инструкция по организации антивирусной защиты

1. Общие положения

1.1. Настоящая инструкция предназначена для организации порядка проведения антивирусного контроля в муниципальном автономном учреждении дополнительного образования города Нижневартовска «Центр детского творчества» (далее МАУДО г. Нижневартовска «ЦДТ») и предотвращения возникновения фактов заражения программного обеспечения компьютериыми вирусами, а также фильтрации доступа пользователей МАУДО г. Нижневартовска «ЦДТ» к непродуктивным Интернет-ресурсам и контроля их электронной переписки.

1.2. Директором учреждения назначается лицо, ответственное за организацию антивирусной защиты в МАУДО г. Нижневартовска «ЦДТ».

1.3. В учреждении может использоваться только лицензионное антивирусное программное обеспечение либо свободно-распространяемое программное обеспечение.

1.4. Установка, настройка и регулярное обновление антивирусных средств осуществляется только ответственным за организацию антивирусной защиты в МАУДО г. Нижневартовска «ЦДТ».

1.5. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, почтовые сообщения), получаемая и передаваемая по телекоммуникационным каналам связи, а также информация, находящаяся на съемных носителях (магнитных дисках, лентах, CD- ROM, DVD. flash-накопителях и т.п.).

1.6. Контроль информации на съёмных носителях производится непосредственно перед её использованием.

1.7. Файлы, помещаемые в электронный архив или на сервер, должны в обязательном порядке проходить антивирусный контроль.

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

1.9. Факт выполнения антивирусной проверки должен регистрироваться в специальном журнале за подписью лица, ответственного за организацию антивирусной защиты.

2. Мероприятия, направленные на решение задач по антивирусной защите

2.1. Установка только лицензированного программного обеспечения либо

бесплатного антивирусного программного обеспечения.

2.2. Регулярное обновление и профилактические проверки (обновление ежедневное; профилактические проверки: 1 раз в неделю во вторник с 12.00).

2.3. Непрерывный контроль над всеми возможными путями проникновения вредоносных программ, мониторинг антивирусной безопасности и обнаружение деструктивной активности вредоносных программ на всех объектах информационно коммуникационной системы (далее ИКС) МАУДО г. Нижневартовска «ЦДТ».

2.4. Проведение профилактических мероприятий по предотвращению и ограничению вирусных эпидемий, включающих загрузку и развертывание специальных правил нейтрализации (отражению, изоляции и ликвидации) вредоносных программ на основе рекомендаций по контролю атак, подготавливаемых разработчиком средств защиты от вредоносных программ и другими специализированными экспертными антивирусными службами до того, как будут выпущены файлы исправлений, признаков и антивирусных сигнатур.

2.5. Внешние носители информации неизвестного происхождения следует проверять на наличие вирусов до их использования

2.6. Необходимо строго придерживаться установленных процедур по уведомлению о случаях поражения автоматизированной информационной среды компьютерными вирусами и принятию мер по ликвидации последствий от их проникновения.

2.7. Обеспечение бесперебойной работы МАУДО г. Нижневартовска «ЦДТ» для случаев вирусного заражения, в том числе резервного копирования всех необходимых данных и программ и их восстановления.

3. Требования к проведению мероприятий по антивирусной защите

3.1. Ежедневно в начале работы при загрузке компьютера (для серверов ЛВС - при перезагрузке) в автоматическом режиме должно выполняться обновление антивирусных баз и серверов и проводиться антивирусный контроль всех дисков и файлов персонального компьютера и съёмных носителей.

3.2. Периодические проверки компьютеров должны проводиться не реже одного раза в неделю.

3.3. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:

- непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети) должна быть выполнена антивирусная проверка на серверах и персональных компьютерах учреждения;
- при возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.);
- при отправке и получении электронной почты оператор электронной почты обязан проверить электронные письма и их вложения на наличие вирусов.

4. Действия сотрудников при обнаружении компьютерного вируса

4.1. В случае обнаружения зараженных компьютерными вирусами файлов или электронных писем пользователи обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение антивирусной защиты в МАУДО г. Нижневартовска «ЦДТ»;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

4.2.При возникновении подозрения на наличие компьютерного вируса ответственный за организацию антивирусной защиты должен провести внеочередной антивирусный контроль.

5.Ответственность

5.1.Ответственность за организацию антивирусной защиты и выполнение положений данной инструкции возлагается на лицо, назначенное директором МАУДО г. Нижневартовска «ЦДТ».

5.2.Ответственность за проведение мероприятий антивирусного контроля в МАУДО г. Нижневартовска «ЦДТ» возлагается на ответственного за организацию антивирусной защиты.

5.3.Ответственность за соблюдение требований настоящей Инструкции при работе на персональных рабочих станциях возлагается на пользователей данных станций или педагога, отвечающего за работу компьютерного класса.

5.4Периодический контроль за состоянием антивирусной защиты в МАУДО г. Нижневартовска «ЦДТ» осуществляется директором учреждения и фиксируется Актом проверки (не реже 1 раз в квартал).

Приложение № 7
к приказу № 252 от «02» апреля 2015 года
«Об утверждении локальных нормативных актов по обеспечению безопасности персональных данных»

УТВЕРЖДЕНО
Приказом от «02» апреля 2015 года
№ 252

ИНСТРУКЦИЯ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ УЧРЕЖДЕНИЯ

1. Общие положения

1.1. Администратор информационных систем персональных данных (ИСПДн) (далее – Администратор) назначается приказом руководителя *МАУДО г. Нижневартовска «ЦДТ»*, на основании Положения о разграничении прав доступа к обрабатываемым персональным данным.

1.2. Администратор подчиняется директору МАУДО г. Нижневартовска «ЦДТ».

1.3. Администратор в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами ФСТЭК России и регламентирующими документами *МАУДО г. Нижневартовска «ЦДТ»*.

1.4. Администратор отвечает за обеспечение устойчивой работоспособности элементов ИСПДн и средств защиты при обработке персональных данных.

1.5. Методическое руководство работой Администратора осуществляется ответственным за обеспечение защиты персональных данных.

2. Должностные обязанности

обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:

- программного обеспечения автоматизированных рабочих мест (АРМ) и серверов (операционные системы, прикладное и специальное программное обеспечение (ПО));
- аппаратных средств;
- аппаратных и программных средств защиты.

2.3. Обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети.

2.4. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.

2.5. Обеспечивать функционирование и поддерживать работоспособность средств защиты.

2.6. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.7. Проводить периодический контроль принятых мер по защите, в пределах возложенных на него функций.

2.8. Хранить, осуществлять прием и выдачу персональных паролей пользователей,

осуществлять контроль за правильностью использования персонального пароля ИСПДн. Оператором

2.9. Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации.

2.10. Информировать ответственного за обеспечение защиты персональных данных о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

2.11. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

2.12. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт. Техническое обслуживание и ремонт средств вычислительной техники, предназначенных для обработки персональных данных, проводятся организациями, имеющими соответствующие лицензии. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации. Вышедшие из строя элементы и блоки средств вычислительной техники заменяются на элементы и блоки, прошедшие специальные исследования и специальную проверку.

2.13. Присутствовать при выполнении технического обслуживания элементов ИСПДн, сторонними физическими людьми и организациями.

2.14. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

3. *Права и ответственность Администратора ИСПДн*

3.1 Администратор ИСПДн имеет право в отведенное ему время решать поставленные задачи в соответствии с полиомочиями доступа к ресурсам ИСПДн, в том числе производить установку и настройку элементов ИСПДн, контролировать и поддерживать работоспособность ИСПДн и выполнять прочие действия в рамках должностных обязанностей.

3.2 Администраторы ИСПДн, виновные в несоблюдении Настоящей инструкции расцениваются как нарушители Федерального закона РФ 27.07.2006 г. N 152-ФЗ "О персональных данных" и несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Приложение № 8
к приказу № 152 от «02» апреля 2015 года
«Об утверждении локальных нормативных актов по обеспечению безопасности персональных данных»

УТВЕРЖДЕНО
Приказом от «02» апреля 2015 года
№ 152

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ УЧРЕЖДЕНИЯ

1. **Общие положения**

1.1. Пользователь информационных систем персональных данных (ИСПДн) (далее – Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.
1.2. Пользователем является каждый сотрудник МАУДО г. Нижневартовска «ЦДТ», участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.
1.3. Пользователь несет персональную ответственность за свои действия.
1.4. Пользователь в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами ФСТЭК России и регламентирующими документами МАУДО г. Нижневартовска «ЦДТ».
1.5. Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных данных.

2. **Должностные обязанности пользователя**:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.
2.2. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в Положении о разграничении прав доступа к обрабатываемым персональным данным.
2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.
2.4. Соблюдать требования парольной политики.
2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других.
2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).
2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью МАУДО г. Нижневартовска «ЦДТ», а так же для получений консультаций по вопросам информационной безопасности, необходимо обратиться в МАУДО г. Нижневартовска

«ЦДТ», по электронной почте: CDT.NV@yandex.ru или по внутреннему телефону 67-24-80.
2.8. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору ИСПДн по внутреннему телефону 67-24-80.
2.9. Пользователям запрещается:

- разглашать защищаемую информацию третьим лицам;
- копировать защищаемую информацию на внешние носители без разрешения своего руководителя;
- самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
- не санкционированно открывать общий доступ к папкам на своей рабочей станции;
- запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;
- отключать (блокировать) средства защиты информации;
- обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн;
- сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;
- привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.

2.10. При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш .и выбрать опцию <Блокировка>.
2.11. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в пределах возложенных на него функций.

3. Организация парольной защиты

3.1 Личные пароли доступа к элементам ИСПДн выдаются пользователям Администратором информационной безопасности, Администратором ИСПДн или создаются самостоятельно.
3.2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.
3.3. Правила формирования пароля:
- пароль не может содержать имя учетной записи пользователя или какую-либо его часть;
- пароль должен состоять не менее чем из 8 символов;
- в пароле должны присутствовать символы трех категорий из числа следующих четырех: прописные буквы английского алфавита от A до Z;
строчные буквы английского алфавита от a до z; десятичные цифры (от 0 до 9);
символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %);
- запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе;
- запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
- запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);
- запрещается выбирать пароли, которые уже использовались ранее.
3.4. Правила ввода пароля:
- ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан;
- во время ввода паролей необходимо исключить возможность его подсматривания

посторонними лицами или техническими средствами (видеокамеры и др.).
3.5. Правила хранение пароля:
- запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;
-запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.
3.6. Лица, использующие паролирование, обязаны:
- четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию;
- своевременно сообщать Администратору информационной безопасности об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

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

4.1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее - Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.
4.2. При работе в Сети запрещается:
- осуществлять работу при отключенных средствах защиты (антивирус и других);
- передавать по Сети защищаемую информацию без использования средств шифрования;
- запрещается скачивать из Сети программное обеспечение и другие файлы;
- запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты, содержащие нелегально распространяемое ПО и другие);
- запрещается нецелевое использование подключения к Сети.

5. Права и ответственность пользователей ИСПДн

5.1 Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн.
5.2 Пользователи, виновные в несоблюдении Настоящей инструкции расцениваются как нарушители Федерального закона РФ 27.07.2006 г. N 152-ФЗ "О персональных данных" и несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность

Приложение № 9
к приказу № 152 от «02» апреля 2015 года
«Об утверждении локальных нормативных актов по обеспечению безопасности персональных данных»

УТВЕРЖДЕНО
Приказом от «02» апреля 2015 года
№ 152

ПЕРЕЧЕНЬ ПОМЕЩЕНИЙ ДЛЯ ХРАНЕНИЯ И ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ С УКАЗАНИЕМ ОТВЕТСТВЕННЫХ ЛИЦ ЗА ЭТИ ПОМЕЩЕНИЯ

№ п/п	Номер кабинета	Фамилия Имя Отчество. Должность ответственного лица
1	112	Здутова Галина Николаевна, главный бухгалтер
2	115	Алмасова Наталья Сергеевна, бухгалтер Бондаренко Ольга Васильевна, бухгалтер Шарафутдинова Анжелика Анатольевна, экономист
3	204	Билоцкая Анна Владимировна, заведующий отделом кадрового администрирования и делопроизводства Попова Татьяна Сергеевна, делопроизводитель
4	214	Баева Елена Николаевна, бухгалтер

Приложение № 10
к приказу № 252 от «02» апреля 2015 года
«Об утверждении локальных нормативных актов по обеспечению безопасности персональных данных»

УТВЕРЖДЕНО
Приказом от «02» апреля 2015 года
№ 252

ПОЛОЖЕНИЕ
о постоянно действующей экспертной комиссии
по защите информации

1. Общие положения

1.1. Постоянно действующая экспертная комиссия по защите информации (далее – ПДЭК по ЗИ) организует и координирует действия структурных подразделений муниципального автономного учреждения дополнительного образования города Нижневартовска «Центр детского творчества» (далее учреждение) в вопросах защиты информации.
1.2. В своей деятельности ПДЭК по ЗИ руководствуется законодательством Российской Федерации, постановлениями Правительства Российской Федерации, нормативно-методическими документами по вопросам безопасности и защиты информации, и настоящим Положением.
1.3. Состав ПДЭК по ЗИ определяется приказом директора учреждения.
1.4. Обязанности между членами комиссии распределяет председатель комиссии.
1.5. ПДЭК по ЗИ осуществляет свою деятельность во взаимодействии с другими структурными подразделениями учреждения.
1.6. Деятельность ПДЭК по ЗИ осуществляется на основе годового плана работы, утверждаемого директором учреждения.

2. Задачи и функции

2.1. Основными задачами ПДЭК по ЗИ являются:
- своевременное выявление и устранение угроз безопасности информации;
- создание условий и механизма оперативного реагирования на угрозы безопасности;
- эффективное пресечение посягательств на информационные ресурсы на основе правовых, организационных, инженерно-технических, программных средств обеспечения безопасности информации;
- создание условий для максимально возможного возмещения ущерба и локализации негативных последствий, возникших в результате неправомерных действий физических лиц или случайных событий, ослабления последствий нарушения безопасности информации.
2.2. С целью достижения наиболее эффективного результата в решении поставленных задач ПДЭК по ЗИ осуществляет следующие функции:
- своевременное выявление и устранение угроз безопасности информации;
- составляет «Перечень информационных ресурсов учреждения, подлежащих защите»;
- организует разработку, внедрение и эксплуатацию системы защиты информации, составляющую конфиденциальные сведения, обрабатываемые с использованием технических средств;
- проводит категорирование объектов информатизации и классификацию защищенности автоматизированных систем;

- ведет учет и анализ попыток несанкционированного доступа к защищаемой информации;
- проводит служебные расследования по фактам нарушения установленной системы доступа к защищаемой информации;
- дает экспертную оценку организационно-распорядительной документации по вопросам защиты информации;
- рассматривает возможность передачи конфиденциальной информации учреждения по запросам сторонних организаций;
- принимает решения о возможности использования в учреждении технических, программных, программно-аппаратных и криптографических средств защиты информации;
- осуществляет контроль полноты и своевременности выполнения мероприятий по защите информации и принятых решений ПДЭК по ЗИ в структурных подразделениях учреждения;
- ведет постоянную работу по совершенствованию системы защиты информации;
- осуществляет планирование своей деятельности;
- комиссия собирается на заседание по мере необходимости или по факту нарушения установленной системы доступа к защищаемой информации;

3. Права комиссии

3.1. ПДЭК по ЗИ имеет право:
- проводить проверки соблюдения режима защиты информации в структурных подразделениях учреждения;
- вносить предложения директору учреждения по совершенствованию существующей защиты информации;
- привлекать по согласованию с директором учреждения к работе по созданию и совершенствованию системы защиты информации других специалистов;
- проводить служебные расследования по факту утечки информации или грубых нарушений режима защиты информации;
- требовать от работников учреждения письменных объяснений при проведении служебных расследований;
- вносить предложения директору учреждения об отстранении от выполнения служебных обязанностей работников учреждения, систематически нарушающих требования по защите информации;
- давать работникам учреждения обязательные для выполнения указания по защите конфиденциальной информации, определяемые существующим в Российской Федерации законодательством.

3.2. Членам комиссии запрещается:
- доводить до работников учреждения систему защиты информации в полном объеме;
- при выходе из состава комиссии запрещается раскрывать объем работы и конкретные направления деятельности комиссии, разглашать информацию, ставшую известной в ходе работы в составе ПДЭК по ЗИ.

Приложение № 1
к Положению о постоянно действующей
экспертной комиссии по защите информации

План работы ПДЭК по ЗИ
на 2015 год

№ п/п	Мероприятия и рассматриваемые вопросы	Ответственные лица	Сроки исполнения	Отметка о выполнении
1.	Ознакомиться с Положением о ПДЭК по ЗИ.	председатель и члены комиссии		
2.	Распределить обязанности между членами комиссии, выбрать секретаря комиссии.	председатель комиссии и члены комиссии		
3.	Провести категорирование объектов информатизации и классификацию защищенности автоматизированных систем.	члены комиссии		
4.	Разработать и утвердить программу «Обучение сотрудников правилам защиты информации»			
5.	Проводить проверки соблюдения режима защиты информации в структурных подразделениях учреждения.			

Приложение № 11
к приказу № 252 от «02» апреля 2015 года
«Об утверждении локальных нормативных актов по обеспечению безопасности персональных данных»

УТВЕРЖДЕНО
Приказом от «02» апреля 2015 года № 252

ПРОГРАММА ОБУЧЕНИЯ ПРАВИЛАМ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ, В ТОМ ЧИСЛЕ ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ УЧРЕЖДЕНИЯ

Сегодня в образовательных организациях активно внедряются современные средства автоматизации учебных процессов, с помощью которых выполняется обработка персональных данных. Защита персональных данных включает целый ряд мер технического, организационного и правового характера.

Помочь образовательным учреждениям решить эту задачу призван данный курс лекций. Программа курса разработана с учетом новейших изменений в законодательстве об образовании, связанных, в том числе, с сайтами образовательных учреждений.

Роскомнадзор активизировал действия по контролю за соблюдением законодательства о защите персональных данных во многих регионах РФ.

Напоминаем, что, в соответствии с частью 2.1 статьи 25 закона №152-ФЗ, операторы, осуществляющие обработку персональных данных, обязаны предоставлять в региональные Управления Роскомнадзора сведения о выполнении требований по защите персональных данных, и о назначении лиц, ответственных за организацию обработки персональных данных. Невыполнение требований Закона может привести к дисциплинарной, административной и даже уголовной ответственности. Уже сложившаяся судебная практика показывает, что за нарушение законодательства о персональных данных могут быть взысканы весьма существенные штрафы.

Содержание курса:

1. Что такое "персональные данные" и почему проблема их сохранности актуальна для образовательных организаций?

- Как защита персональных данных регулируется законодательством?
- Что такое «персональные данные»
- Кто такие субъект и оператор персональных данных
- Что подразумевается под обработкой персональных данных
- Об информационной открытости образовательной организации
- Уведомление об обработке персональных данных
- Реестр операторов персональных данных
- Методические рекомендации Минздравсоцразвития и письма Рособразования
- Особенность проектов по защите персональных данных в ОУ

2. Какие документы необходимо подготовить в образовательной организации в первую очередь.

- Лицо, ответственное за организацию обработки персональных данных в

образовательной организации
- Обязанности оператора персональных данных
- Политика в отношении обработки персональных данных
- Определение перечней лиц, допущенных к обработке персональных данных и мест их хранения
- Хранение персональных данных
- Документы, регулирующие использование криптосредств.
- Система ведения журналов успеваемости учащихся в электронном виде.
- Защита персональных данных при их обработке в информационных системах
- Разъяснения о Требования к защите персональных данных при их обработке в информационных системах ПДн (Постановление Правительства РФ №1119)
- Уровни защищенности и требования к их обеспечению

3. Как на практике защитить персональные данные

- Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных:
- Выбор мер по обеспечению безопасности персональных данных.
- Соотношение мер и уровней защищенности

4.Проведение проверок: кто, что и как будет проверять

- Мероприятия Роскомнадзора
- Права должных лиц Роскомнадзора
- Что проверяет Роскомнадзор
- Итоги проверки

5.Типичные нарушения законодательства о персональных данных в образовательных учреждениях.

- Непредставление уведомления об обработке персональных данных
- Непредставление информационного письма о внесении изменений в сведения об операторе в реестре операторов, осуществляющих обработку персональных данных.
- Привлечение к обработке персональных данных третьих лиц
- Особенности обработки персональных данных, осуществляемой без использования средств автоматизации
- Последствия несоблюдения требований

Приложение № 12
к приказу № 152 от «02» апреля 2015 года
«Об утверждении локальных нормативных актов по обеспечению безопасности персональных данных»

УТВЕРЖДЕНО
Приказом от «01» апреля 2015 года
№ 152

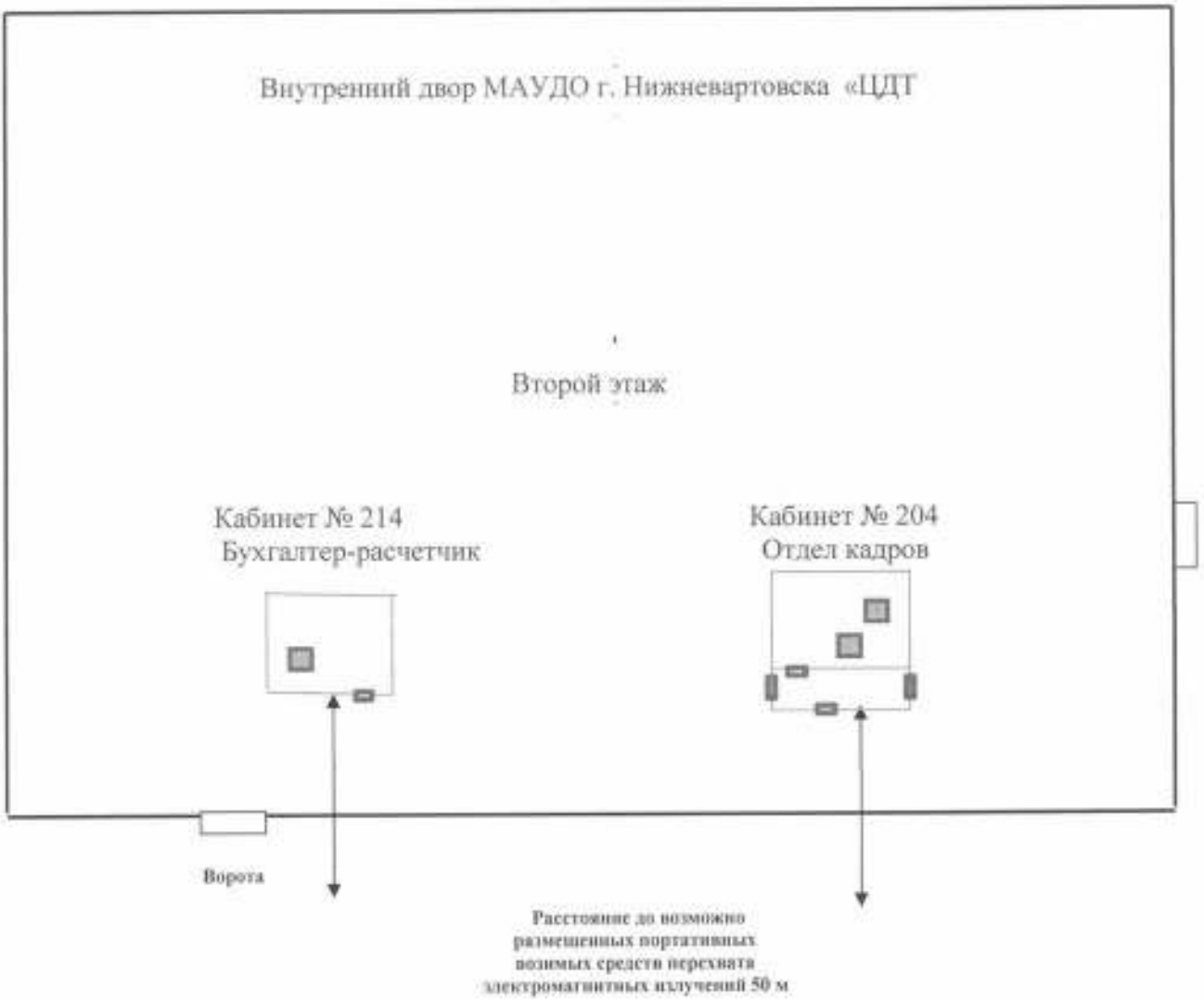
ГРАНИЦЫ КОНРОЛИРУЕМОЙ ЗОНЫ УЧРЕЖДЕНИЕМ

Условные обозначения:

- компьютер

- двери

ГРАНИЦЫ КОНРОЛИРУЕМОЙ ЗОНЫ УЧРЕЖДЕНИЕМ

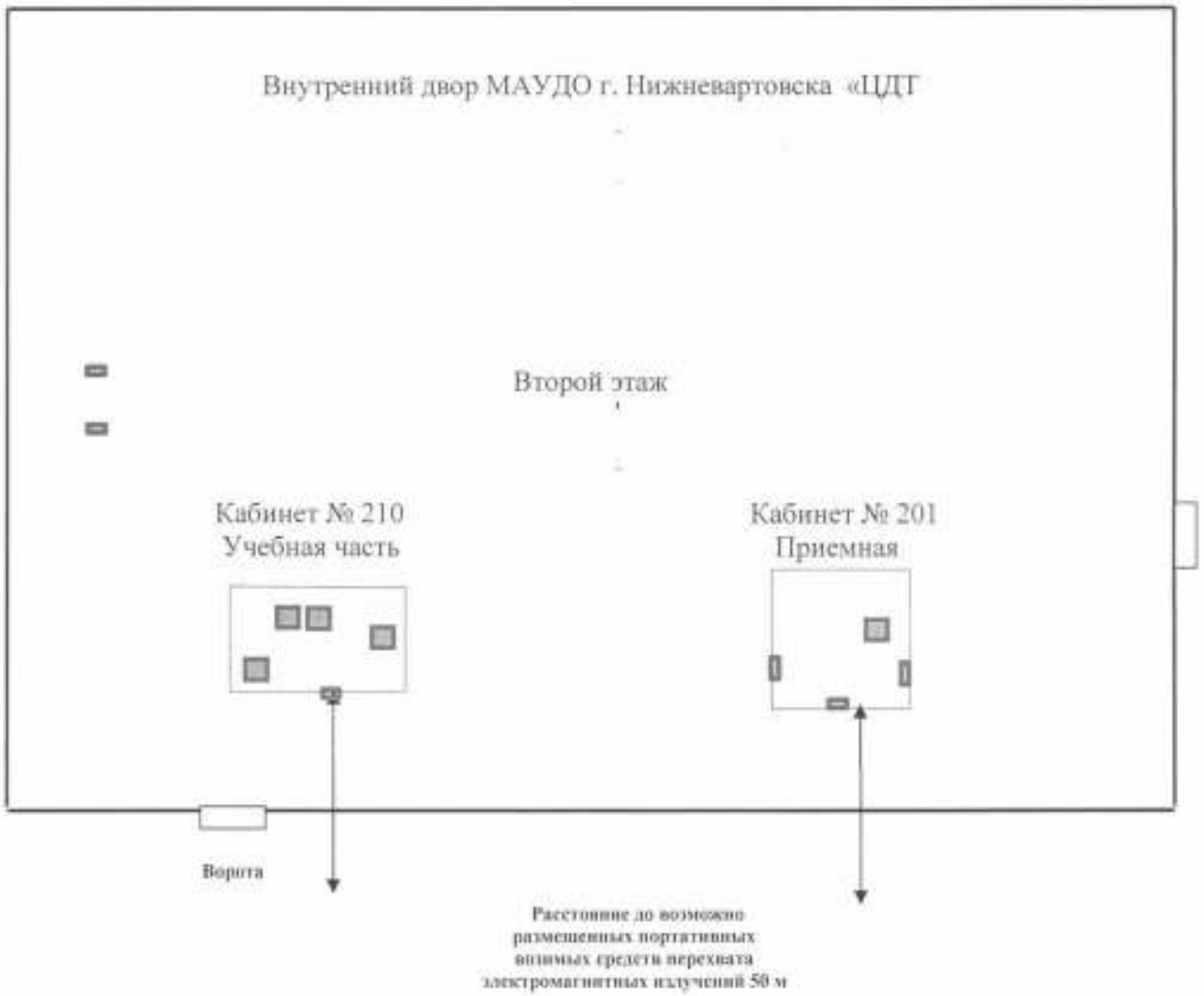


Условные обозначения:

- компьютер

- двери

ГРАНИЦЫ КОНРОЛИРУЕМОЙ ЗОНЫ УЧРЕЖДЕНИЕМ



Условные обозначения:

- компьютер

- двери