СОГЛАСОВАНО
Председатель профсоюза
МДОБУ «Муринский ДСКВ №1»
_____ Г.В. Подгорная
Принято на общем собрании
Протокол № 1 от 09.01.2019 г.

УТВЕРЖДАЮ
Заведующий МДОБУ
«Муринский ДСКВ №1»
_____ М.Н. Арцыбашева
Введено в действие приказом
от 09.01.2019 №08 -ОД

ПОЛОЖЕНИЕ

О порядке обработки и обеспечении защиты персональных данных
Муниципального дошкольного образовательного бюджетного учреждения
«Муринский детский сад комбинированного вида №1».

Мурино
2019 г.

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Федеральным законом 152-ФЗ «О персональных данных» (далее – Федеральный закон), постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», 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 устанавливает единый порядок обработки и защиты персональных данных в организации.

1.2. Настоящее Положение регулирует отношения, связанные с обработкой персональных данных, осуществляемой с использованием средств автоматизации или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации.

1.3. Настоящее Положение не регулирует вопросы обработки персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

1.4. В Положении используются следующие термины и их определения:

1) *персональные данные* - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, фото и другая информация;

2) *информационная система персональных данных (ИСПДн)* - информационная система ИОГВ ЯНАО, представляющая собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

3) *оператор* - орган государственный власти или муниципальный орган юридическое 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;

4) *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;

4) *автоматизированная обработка персональных данных* - обработка персональных данных с помощью средств вычислительной техники;

5) *распространение персональных данных* - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

6) *предоставление персональных данных* - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

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

8) *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;

9) *обезличивание персональных данных* - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

10) *трансграничная передача персональных данных* - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу

2. Основные положения обработки персональных данных

2.1 .Цели и содержание обработки персональных данных в ИСПДн определяются в соответствии с требованиями законодательства РФ.

2.1. Обработка персональных данных осуществляется в соответствии с утвержденной в организации организационно-распорядительной документацией, определяющей правила и процедуры работы с персональными данными.

2.2. Защищаемая информация ИСПДн определяется в соответствии с Перечнем ПДн, подлежащих защите в организации.

2.3. 3.Безопасность персональных данных при их обработке в информационной системе обеспечивает организация (подразделение), осуществляющее обработку персональных данных.

2.4. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона «О персональных данных».

2.5. Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

2.6. Выбор средств защиты информации для системы защиты персональных данных осуществляется уполномоченным лицом оператора по защите ПДн и согласуется с отделом информационной безопасности Департамента образования.

2.7. ИСПДн является информационной системой, обрабатывающей специальные категории персональных данных, если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.

2.8. ИСПДн является информационной системой, обрабатывающей биометрические персональные данные, если в ней обрабатываются 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, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.

2.9. ИСПДн является информационной системой, обрабатывающей общедоступные персональные данные, если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона «О персональных данных».

2.10. ИСПДн является информационной системой, обрабатывающей иные категории персональных данных, если в ней не обрабатываются персональные данные, указанные в абзацах первом - третьем настоящего пункта.

2.11. ИСПДн является информационной системой, обрабатывающей персональные данные сотрудников оператора, если в ней обрабатываются персональные данные только указанных сотрудников. В остальных случаях информационная система персональных данных является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора.

3. Основные положения обработки персональных данных

3.1. В ИСПДн обрабатываются персональные данные сотрудников оператора и иные категории персональных данных субъектов ПДн, проживающих на территории Ленинградской области Всеволожского района.

3.2. Обработка персональных данных в ИСПДн осуществляется в соответствии с требованиями Федерального закона «О персональных данных», нормативных и методических документов уполномоченных федеральных органов исполнительной власти по обеспечению безопасности персональных данных, а также нормативно-правовыми актами МДОБУ «Муринский ДСКВ №1».

3.3. Ответственным осуществляется классификация ИСПДн в соответствии с Приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных» в зависимости от категории обрабатываемых данных и их объема. Результаты классификации оформляются Актом и утверждаются руководителем организации.

3.4. Приказом руководителя назначается сотрудник, ответственный за защиту персональных данных (ответственный за безопасность (ПДн), определяется перечень помещений, в которых разрешена обработка ПДн, и перечень лиц, допущенных к обработке персональных данных.

3.5. Лица, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящим Положением и подписывают обязательство о неразглашение информации, содержащей персональные данные, по форме согласно приложения №2 к настоящему Положению.

3.6. Персональные данные (ПДн) сотрудника – информация, необходимая МДОБУ «Муринский ДСКВ №1» в связи с установлением трудовых отношений и касающаяся конкретного сотрудника.

3.7. Персональные данные работников (субъектов ПДн), МДОБУ «Муринский ДСКВ №1» информация, необходимая в связи с осуществлением и выполнением возложенных на него функций, полномочий и обязанностей.

4. Порядок обработки ПДн сотрудников оператора

4.1. К ПДн сотрудника относятся следующие сведения: опознавательные данные (ФИО, дата и место рождения, трудовая биография сотрудника, факты биографии); личные характеристики сотрудника (гражданство, наличие научных трудов, изобретений и т.д.); сведения о семейном положении; составе семьи; социальном положении; служебном положении; навыках; о финансовом положении; информацию, содержащаяся в трудовой книжке, в страховом свидетельстве государственного пенсионного страхования; информацию об образовании, квалификации; информацию медицинского характера; информацию в документах воинского учета и в других документах, которые содержат данные, необходимые работодателю в связи с трудовыми отношениями.

4.2. Обработка ПДн сотрудника осуществляется в целях соблюдения законов и других нормативно-правовых актов РФ, осуществления и выполнения возложенных на оператора функций, полномочий и обязанностей.

4.3. Работодатель получает и обрабатывает ПДн сотрудника только с его письменного согласия (Приложение 1).

4.4. Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных.

4.5. Все ПДн сотрудника работодатель получает непосредственно от самого сотрудника путем анкетирования и сбора официальных документов, необходимых для обеспечения трудовой деятельности сотрудника.

4.6. Работодатель вправе проверять ПДн сотрудников с целью формирования кадрового резерва.

4.7. При приеме на работу, заключении трудового договора, заполнении анкетных данных работодатель не имеет право получать и обобщать информацию о религиозных, политических и других убеждениях сотрудника.

4.8. Работодатель сообщает работнику цели, предположительные источники, способы получения ПДн, характер ПДн и последствия отказа сотрудника дать письменное согласие на их получение.

4.9. Работодатель имеет право передавать ПДн сотрудников в налоговые органы, Пенсионный фонд РФ, Фонд социального страхования РФ, Федеральную инспекцию труда. Использование ПДн сотрудника допустимо только в соответствии с целями, определившими их получение. Передача ПДн сотрудника возможна только с согласия сотрудника, если иное не предусмотрено законодательством РФ.

4.10. Работодатель производит расчет и выплату налогов за сотрудника путем удержания их из заработной платы, работодатель имеет право собирать предусмотренные Налоговым Кодексом РФ сведения о налогоплательщике.

4.11. При обработке ПДн работодатель обязан обеспечить право сотрудников:

- получение полной информации об их ПДн и обработке этих данных;

– свободный бесплатный доступ к своим ПДн, включая право на получение копий любой записи, содержащей ПДн сотрудника, за исключением случаев, предусмотренных федеральным законом;

– требование об исключении или исправлении неверных или неполных ПДн, а также данных, обработанных с нарушением требований действующего законодательства; при отказе работодателя исключить или исправить ПДн сотрудника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия; ПДн оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;

– требование об извещении работодателем всех лиц, которым раннее были сообщены неверные или неполные ПДн сотрудника, обо всех произведенных в них исключениях, исправлениях или дополнениях;

– обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его ПДн.

4.12. Все представленные при оформлении на работу ПДн остаются на хранении у работодателя. За хранение ПДн сотрудников отвечает должностное лицо кадрового подразделения, осуществляющее ведение личных дел сотрудников. Режим хранения ПДн должен исключать возможность их утраты или неправомерного использования.

4.13. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных.

4.14. В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор.

4.15. Передача ПДн сотрудника третьим лицам осуществляется в соответствии с инструкцией, при этом работодатель должен соблюдать следующие требования:

– не сообщать ПДн сотрудника третьей стороне без письменного согласия сотрудника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью сотрудника, а также в случаях, установленных федеральным законом;

– предупредить лиц, получающих ПДн сотрудника, 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;

– передавать ПДн сотрудника представителям сотрудников в порядке, установленном действующим законодательством РФ, и ограничивать эту информацию только теми ПДн сотрудника, которые необходимы для выполнения указанными представителями их функций.

4.16. Обработка персональных данных осуществляется:

- после получения согласия субъекта персональных данных, составленного по форме согласно приложению №1 к настоящему Положению, за исключением случаев, предусмотренных частью 2 статьи 6 Федерального закона;

- после направления уведомления об обработке персональных данных в Роскомнадзор России, за исключением случаев, предусмотренных частью 2 статьи 22 Федерального закона;

- после принятия необходимых мер по защите персональных данных.

4.17. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.

4.18. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

5. Порядок обработки иных категорий персональных данных

5.1. Требования к обработке оператором иных категорий персональных данных идентичны п.4 настоящего Положения.

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

1) подтверждение факта обработки персональных данных;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые ответственным, способы обработки ПДн;

4) 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;

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

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

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

10) иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

5.3. Право субъекта ПДн на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

1) обработка персональных данных, полученных в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

2) обработка персональных данных осуществляется органами, осуществившими задержание субъекта ПДн по подозрению в совершении преступления, либо предъявившими субъекту ПДн обвинение по уголовному делу, либо применившими к субъекту ПДн меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

3) обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

4) доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

5) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

5.4. Ответственный обязан немедленно прекратить по требованию субъекта ПДн обработку его персональных данных.

6. Порядок обработки персональных данных в ИСПДН с использованием средств автоматизации

6.1. Обработка персональных данных с использованием средств автоматизации осуществляется в соответствии с требованиями постановления Правительства Российской Федерации от 1 ноября 2012 г. №1119, нормативных и методических документов уполномоченных федеральных органов исполнительной власти по обеспечению безопасности персональных данных, а так же нормативно-

правовыми МДОБУ «Муринский ДСКВ №1» и организационно-распорядительными документами организации.

6.2. Требования к защите персональных данных в ИСПДн определяются исходя из установленного класса ИСПДн и состава актуальных угроз безопасности персональным данным.

6.3. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

6.4. Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 181 Федерального закона «О персональных данных», и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона «О персональных данных».

6.5. Для обеспечения требуемого уровня защищенности персональных данных при их обработке в ИСПДн необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;

д) назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе;

е) поддержание в актуальном состоянии электронного журнала сообщений, определенного постановлением Правительства РФ от 1 ноября 2012 г. №1119.

6.6. Не допускается обработка персональных данных в ИСПДн с использованием средств автоматизации при отсутствии:

- утвержденной организационно-распорядительной документации о порядке работы и защиты ПДн в организации, включающих акт классификации ИСПДн, инструкции пользователя, ответственного за безопасность, по организации антивирусной защиты, использования средств защиты информации и других нормативных и методических документов;

- настроенных средств защиты от несанкционированного доступа, средств антивирусной защиты, резервного копирования информации и других программных и технических средств в соответствии с требованиями безопасности информации;

- охраны и организации режима допуска к ресурсам ИСПДн и в помещения, предназначенные для обработки персональных данных.

6.7. Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы.

6.8. Решение, порождающее юридические последствия в отношении субъекта ПДн или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной

форме субъекта ПДн или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта ПДн.

6.9. Ответственный обязан разъяснить субъекту ПДн порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом ПДн своих прав и законных интересов.

6.10. Ответственный обязан рассмотреть возражение, в течение тридцати дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

7. Порядок обработки персональных данных ИСПДн без использования средств автоматизации

7.1. Обработка персональных данных без использования средств автоматизации (неавтоматизированная) - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

7.2. Обработка персональных данных без использования средств автоматизации (далее – неавтоматизированная обработка персональных данных) может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, базы банных) на электронных носителях информации.

7.3. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

7.4. При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;

- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;

- дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

7.5. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

7.6. Неавтоматизированная обработка персональных данных в электронном виде осуществляется на внешних электронных носителях информации.

7.7. При отсутствии технологической возможности осуществления неавтоматизированной обработки персональных данных в электронном виде на внешних носителях информации необходимо принимать организационные (охрана помещений) и технические меры (установка сертифицированных средств защиты информации), исключающие возможность несанкционированного доступа к персональным данным лиц, не допущенных к их обработке.

7.8. Электронные носители информации, содержащие персональные данные, учитываются в журнале учета электронных носителей персональных данных, составленном по форме согласно приложению №3 к настоящему Положению.

К каждому электронному носителю оформляется опись файлов, содержащихся на нем, с указанием цели обработки и категории персональных данных.

7.9. При несовместимости целей неавтоматизированной обработки персональных данных, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

7.10. Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

8. Меры, направленные на обеспечение безопасности ПДн

8.1. Ответственный обязан принимать меры, необходимые и достаточные для обеспечения безопасности персональных данных работников МДОБУ «Муринский ДСКВ №1».

8.2. Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством РФ уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

8.3. К мерам обеспечения безопасности персональных данных относятся:

1) назначение ответственным, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;

2) издание ответственным, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 настоящего Федерального закона;

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных настоящему Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам МДОБУ «Муринский ДСКВ №1».

5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом;

6) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

8.4. Ответственный обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных.

8.5. Ответственный обязан представить документы и локальные акты и (или) иным образом подтвердить принятие мер по запросу уполномоченного органа по защите прав субъектов персональных данных.

8.6. Ответственный определяет состав и перечень мер, необходимых и достаточных для обеспечения безопасности персональных данных МДОБУ «Муринский ДСКВ №1».

8.7. Для выполнения работ и оказания услуг по обеспечению безопасности персональных данных могут привлекаться на договорной основе специализированные организации – лицензиаты ФСТЭК России по технической защите конфиденциальной информации.

9. Порядок контроля и ответственность должностных лиц

9.1. Контроль за выполнением настоящих требований организуется и проводится ответственным (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые ответственным (уполномоченным лицом).

9.2. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных в государственных информационных системах персональных данных осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия

техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

9.3. 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.

9.4. Сотрудники организации, допущенные установленным порядком к персональным данным, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение № 1
К Положению о порядке обработки
Персональных данных в ИСПДн

СОГЛАСИЕ
на обработку персональных данных

Я, _____
(Фамилия, Имя, Отчество)
даю согласие МДОБУ «Муринский ДСКВ №1»,
на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно – совершение действий, предусмотренных п. 3 ч.1 ст. 3 Федерального закона от 27.07.2006г. №152 ФЗ «О персональных данных», содержащихся в настоящем заявлении, в целях обеспечения соблюдения трудового законодательства и иных нормативных правовых актов, содействия в трудоустройстве, обучении и продвижения по службе, обеспечения личной безопасности работников, контроля качества выполняемой работы и обеспечения сохранности имущества, а именно:
использовать все нижеперечисленные данные для оформления кадровых документов и выполнения учреждением всех требований трудового законодательства;
использовать мои персональные данные в информационной системе для осуществления расчетов работодателя со мной как работником;
размещать мою фотографию, фамилию, имя и отчество на доске почета, на стендах в помещении учреждения, на внутреннем сайте учреждения.

1. Ф.И.О. _____
2. Дата рождения: _____
3. Документ, удостоверяющий личность _____
(наименование, номер и серия документа,
_____
кем и когда выдан)
4. Адрес регистрации по месту жительства _____
_____
(почтовый адрес)
5. Адрес фактического проживания: _____
(почтовый адрес фактического проживания
_____
контактный телефон)
6. ИНН _____
7. Номер страхового свидетельства пенсионного страхования _____

Об ответственности за достоверность представленных сведений предупрежден(а).

_____ _____ _____
(Ф. И.О. работника) (подпись) (дата)

Приложение №2
к Положению о порядке обработки
персональных данных в ИСПДн

ОБЯЗАТЕЛЬСТВО
о неразглашении информации, содержащей персональные данные

Я,_____,
(Ф.И.О.)
исполняющий (ая) должностные обязанности по замещаемой должности

_____

_____,
(должность, наименование структурного подразделения)

предупрежден (а) о том, что на период исполнения должностных обязанностей в соответствии с должностным регламентом мне будет предоставлен допуск к информации, содержащей персональные данные. Настоящим добровольно принимаю на себя обязательства:

1. Не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.

2. В случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать непосредственному начальнику.

3. Не использовать информацию, содержащую персональные данные, с целью получения выгоды.

4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.

5. В течение года после прекращения права на допуск к информации, содержащей персональные данные, не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

Я предупрежден (а) о том, что в случае нарушения данного обязательства буду привлечен (а) к дисциплинарной ответственности и/или иной ответственности в соответствии с законодательством Российской Федерации.

_____ _____
(фамилия, инициалы) (подпись)

«_____»_____ ____г.

Приложение №3
к Положению о порядке обработки
персональных данных в ИСПДн

Начат «___» _____ ____ г.
Окончен «___» _____ ____ г.
На _____ листах

ЖУРНАЛ
учета электронных носителей персональных данных

Учетный номер	Дата постановки на учет	Вид электронного носителя, место его хранения (размещения)	Ответственный за использование и хранение		
			Ф.И.О.	подпись	дата
1	2	3	4	5	6

Начат «___» _____ ____ г.
Окончен «___» _____ ____ г.
На _____ листах

ЖУРНАЛ
учета обращений субъектов персональных данных о выполнении их законных прав, при обработке персональных данных в ИСПДН

№	ФИО	Дата	Цель
			Информирование
			Прекращение обработки
			Уточнение ПДн

Приложение №4
к Положению о порядке обработки
персональных данных в ИСПДн

Матрица доступа

пользователей к защищаемым информационным ресурсам ИСПДн
(форма)

Наименование информационных ресурсов, используемых в ИСПДн (логические диски, каталоги, программы, устройства и т.п.)	Тип доступа	Пользователи ИСПДн					
		Администратор	Группа 1	Группа 2	Группа 3	…	Группа N
C:\Каталог 1	чтение						
	запись						
	выполнение						
C:\Каталог 2	чтение						
	запись						
	выполнение						
USB-flash накопители	чтение						
	запись						
	выполнение						
CD/DVD-RW	чтение						
	запись						
	выполнение						
Принтер	печать						
Программные средства	инсталляция, изменение						
ОС, СЗИ	настройки						

«УТВЕРЖДАЮ»
Заведующий МДОБУ
«Муринский ДСКВ № 1»
М.Н. Арцыбашева
Приказ от 27.10.2021 №02-ОД

ИНСТРУКЦИЯ
по порядку сбора, учета и хранения персональных данных

1. Общие положения

1.1.Настоящая Инструкция МДОБУ «Муринский ДСКВ №1» (далее – МДОБУ) по порядку учета, хранения и уничтожения персональных данных (далее – Инструкция) разработана в соответствии с Федеральным законом Российской Федерации от 27.07.2006 N 152-ФЗ «О персональных данных» (далее – Федеральный закон), иными нормативно-правовыми актами по защите персональных данных, действующими на территории Российской Федерации и применяется в МДОБУ.

1.2. Инструкция устанавливает порядок учета, хранения, и уничтожения персональных данных сотрудников МДОБУ.

1.3.Инструкция предназначена для работников МДОБУ , имеющих доступ к персональным данным сотрудников (далее – ПДн).

1.4. В настоящей Инструкции используются следующие понятия:

1) **персональные данные (ПДн)** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая для выполнения основных видов деятельности МБОДУ;

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;

3) **конфиденциальность персональных данных** – обязательное для соблюдения лицом, получившим доступ к персональным данным, требование не допускать их распространения без согласия субъекта персональных данных или иного законного основания;

4) **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;

5) **обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

6) **информационная система персональных данных (ИСПДн)**– совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

7) **информация** – сведения (сообщения, данные) независимо от формы их представления;

8) **носитель информации (материальный носитель)** – любой материальный объект бумажный и электронный, способный достаточно длительное время сохранять (нести) в своей структуре занесённую в/на него информацию.

2. Порядок сбора и учета персональных данных

2.1. Получение персональных данных в МБОДУ возможно следующими способами:

1) Субъект ПДн дает письменное согласие на обработку своих персональных данных (кроме случаев, указанных в Федеральном законе, «Согласия на обработку персональных данных») Субъект ПДн предоставляет работнику МБОДУ достоверные сведения о себе. Работник МДОБУ проверяет достоверность сведений, сверяя данные, предоставленные субъектом ПДн, с имеющимися документами, удостоверяющими личность субъекта ПДн.

2) МДОБУ получает персональные данные установленным порядком от организаций, собирающих их непосредственно с субъектов ПДн.

3. Порядок хранения персональных данных

3.1. Материальные носители, содержащие персональные данные регистрируются в специальных журналах МДОБУ.

3.2. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним. Материальные носители с персональными данными должны храниться в запирающихся на ключ помещениях, металлических шкафах, сейфах, иных шкафах, имеющих запираемые блок-секции.

4. Порядок обработки персональных данных

4.1. В МДОБУ обработка персональных данных осуществляется с использованием средств автоматизации и без использования таковых.

4.2. При обработке персональных данных с использованием средств автоматизации должны соблюдаться следующие условия:

1) экран видеомонитора необходимо располагать в помещении во время работы так, чтобы исключалась возможность ознакомления посторонними лицами с отображаемой на нем информацией;

2) вход в ИСПДн должен осуществляется по имени пользователя и паролю;

3) при выходе из помещения в течение рабочего дня необходимо выключать или блокировать ИСПДн;

4) обязательно использование антивирусного приложения в ИСПДн;

5) хранение и копирование персональных данных возможно только на учтенные в соответствующем журнале материальные носители

5. Порядок передачи персональных данных

5.1. Передача персональных данных третьим лицам осуществляется в соответствии с Федеральным законом и в целях выполнения основных видов деятельности МДОБУ.

5.2. Передача носителей с персональными данными возможна только курьерской доставкой или заказным письмом с описью вложения.

5.3. Передача персональных данных по открытым телекоммуникационным сетям общего пользования возможна только при использовании сертифицированных ФСБ РФ средств шифрования.

6. Порядок уничтожения или обезличивания персональных данных

6.1.После достижения цели обработки персональных данных они должны быть уничтожены в течение 30 дней с даты достижения цели обработки персональных данных.

6.2.Материальные носители персональных данных уничтожаются комиссией с составлением «Акта об уничтожении материальных носителей персональных данных…» .

6.3. При использовании персональных данных после достижения цели их обработки в статистических или иных исследовательских целях необходимо их обезличивание.

«УТВЕРЖДАЮ»
Заведующий МДОБУ
«Мурминский ДСКВ № 1»
_____ М.Н. Арешбашева
Приказ «09» 01 2018 № 08 -ОД

ИНСТРУКЦИЯ
по порядку учета, хранения и уничтожения съемных носителей персональных данных

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Федеральным законом № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации», ГОСТ Р ИСО/МЭК 17799-2005 «Практические правила управления информационной безопасностью» и другими нормативными правовыми актами, и устанавливает порядок использования носителей информации, предоставляемых органом исполнительной власти (далее наименование ОИВ) для использования в ИС.

1.2. Действие настоящего Положения распространяется на сотрудников органа исполнительной власти, подрядчиков и третью сторону.

2. Основные термины, сокращения и определения

1. Администратор ИС – технический специалист, обеспечивает ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации ПО и оборудования вычислительной техники.

2. АРМ – автоматизированное рабочее место пользователя (ПК с прикладным ПО) для выполнения определенной производственной задачи.

3. ИБ – информационная безопасность – комплекс организационно- технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.

4. ИС – информационная система – система, обеспечивающая хранение, обработку, преобразование и передачу информации с использованием компьютерной и другой техники.

5. Носитель информации – любой материальный объект, используемый для хранения и передачи электронной информации.

6. Паспорт ПК – документ, содержащий полный перечень оборудования и программного обеспечения АРМ.

7. ПК – персональный компьютер.

8. ПО – Программное обеспечение вычислительной техники.

9. ПО вредоносное – ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.

10. ПО коммерческое – ПО сторонних производителей (правообладателей). Предоставляется в пользование на возмездной (платной) основе.

11. Пользователь – работник Организации, использующий мобильные устройства и носители информации для выполнения своих служебных обязанностей.

3. Порядок использования носителей информации

3.1. Под использованием носителей информации в ИС органа исполнительной власти понимается их подключение к инфраструктуре ИС с целью обработки, приема/передачи информации между ИС и носителями информации.
3.2. В ИС допускается использование только учтенных носителей информации, которые являются собственностью органа исполнительной власти и подвергаются регулярной ревизии и контролю.
3.3. К предоставленным органам исполнительной власти носителям конфиденциальной информации предъявляются те же требования ИБ, что и для стационарных АРМ (целесообразность дополнительных мер обеспечения ИБ определяется администраторами ИС).
3.4. Носители конфиденциальной информации предоставляются сотрудникам органа исполнительной власти по инициативе Руководителей структурных подразделений в случаях:

- необходимости выполнения вновь принятым работником своих должностных обязанностей;
- возникновения у сотрудника органа исполнительной власти производственной необходимости.

3.5. Процесс предоставления сотрудникам органа исполнительной власти носителей конфиденциальной информации состоит из следующих этапов:

4. Порядок учета, хранения и обращения со съемными носителями конфиденциальной информации (персональных данных), твердыми копиями и их утилизации.

4.1. Все находящиеся на хранении и в обращении съемные носители с конфиденциальной информацией (персональными данными) в органе исполнительной власти подлежат учёту.
4.2. Каждый съемный носитель с записанными на нем конфиденциальной информацией (персональными данными) должен иметь этикетку, на которой указывается его уникальный учетный номер.
4.3. Учет и выдачу съемных носителей конфиденциальной информации (персональных данных) осуществляют сотрудники структурных подразделений, на которых возложены функции хранения носителей персональных данных. Факт выдачи съемного носителя фиксируется в журнале учета съемных носителей конфиденциальной информации.
4.4. Сотрудники органа исполнительной власти получают учтенный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

5. При использовании сотрудниками носителей конфиденциальной информации необходимо:

5.1. Соблюдать требования настоящего Положения.
5.2. Использовать носители информации исключительно для выполнения своих служебных обязанностей.
5.3. Ставить в известность администраторов ИС о любых фактах нарушения требований настоящего Положения.
5.4. Бережно относится к носителям конфиденциальной информации.

5.5. Обеспечивать физическую безопасность носителей информации всеми разумными способами.

5.6. Извещать администраторов ИС о фактах утраты (кражи) носителей конфиденциальной информации.

6. При использовании носителей конфиденциальной информации запрещено:

6.1. Использовать носители конфиденциальной информации в личных целях.

6.2. Передавать носители конфиденциальной информации другим лицам (за исключением администраторов ИС).

6.3. Хранить съемные носители с конфиденциальной информацией (персональными данными) вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

6.4 Выносить съемные носители с конфиденциальной информацией (персональными данными) из служебных помещений для работы с ними на дому и т. д.

6.5 Любое взаимодействие (обработка, прием/передача информации) инициированное сотрудником органа исполнительной власти между ИС и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев оговоренных с администраторами ИС заранее). Администратор ИС оставляет за собой право блокировать или ограничивать использование носителей информации.

6.6. Информация об использовании сотрудником органа исполнительной власти носителей информации в ИС протоколируется и, при необходимости, может быть предоставлена Руководителям структурных подразделений, а также Руководителю органа исполнительной власти.

6.7. В случае выявления фактов несанкционированного и/или нецелевого использовании носителей конфиденциальной информации инициализируется служебная проверка, проводимая комиссией, состав которой определяется Руководителем органа исполнительной власти.

6.8. По факту выясненных обстоятельств составляется акт расследования инцидента и передается Руководителю структурного подразделения для принятия мер согласно локальным нормативным актам Организации и действующему законодательству.

6.9. Информация, хранящаяся на носителях конфиденциальной информации, подлежит обязательной проверке на отсутствие вредоносного ПО.

6.10. При отправке или передаче конфиденциальной информации (персональных данных) адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка конфиденциальной информации (персональных данных) адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования.

6.11. Вынос съемных носителей конфиденциальной информации (персональных данных) для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения.

6.12. В случае утраты или уничтожения съемных носителей конфиденциальной информации (персональных данных) либо разглашении содержащихся в них сведений немедленно ставится в известность начальник соответствующего структурного подразделения. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета съемных носителей конфиденциальной информации (персональных данных).

6.13. Съемные носители конфиденциальной информации (персональных данных), пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется «уполномоченной комиссией». По результатам уничтожения носителей составляется акт по прилагаемой форме

6.14. В случае увольнения или перевода работника в другое структурное подразделение, предоставленные носители конфиденциальной информации изымаются.

7. Ответственность

7.1. Работники, нарушившие требования настоящего Положения, несут ответственность в соответствии с действующим законодательством и локальными нормативными актами органа исполнительной власти.

Форма акта

УТВЕРЖДАЮ

_____

«_____»_____20___ г.

АКТ

уничтожения съемных носителей персональных данных

Комиссия в составе: _____

_____

_____

_____

_____

наделенная полномочиями приказа № _____ от _____ 20____г. провела отбор съемных носителей конфиденциальной информации (персональных данных), не подлежащих дальнейшему хранению:

№	дата	Учетный номер съемного носителя	примечание

Всего съёмных носителей _____ (цифрами и прописью)

На съемных носителях уничтожена конфиденциальная информация путем стирания ее на устройстве гарантированного уничтожения информации (механического уничтожения, сжигания и т. П.)

Перечисленные съемные носители уничтожены

_____

Путем (разрезания, демонтажа и т.п.)

_____

Председатель комиссии: _____ _____ (дата, подпись)

Члены комиссии: _____ _____

_____ _____

_____ _____

_____ _____

«УТВЕРЖДАЮ»
Заведующий МДОБУ
«Муринский ДСКВ № 1»
_____ М.Г. Арцыбашева
Приказ «11» 01 2019 №08 -ОД

ИНСТРУКЦИЯ

по эксплуатации средств защиты информации (СИЗ)

1. Информационная система персональных данных (далее - ИСПДн) МДОБУ «Муринский ДСКВ №1» (далее – МДОБУ) предназначена для разработки, хранения, печати информации, содержащей персональные данные, при этом информация может поступать из других информационных систем на гибких магнитных дисках, компакт дисках (CD, DVD) или flesh-накопителях. ИСПДн представляет собой локальную вычислительную сеть, в которой обрабатываются персональные данные работников МДОБУ. Хранение базы персональных данных осуществляется на сервере. Доступ к базе персональных данных осуществляется с рабочих мест пользователей по каналу, защищенному системой криптографической защиты. Также используется сертифицированный распределенный межсетевой экран. На сервере введено разграничение доступа к персональным данным пользователей. Возможно подключение рабочих станций пользователей к сетям связи общего доступа. На рабочие станции и сервер установлены сертифицированные по требованиям ФСТЭК России системы защиты информации от несанкционированного доступа.

2. Обязанности по сопровождению и настройке средств защиты возлагаются на ответственного за эксплуатацию СЗИ.

3. Ответственный за эксплуатацию СЗИ должен:

3.1 Осуществлять оперативные действия по конфигурированию установленных средств и механизмов защиты и их поддержке в работоспособном состоянии в соответствии с утвержденным положением и инструкциями, включая:

– определение состава и настроек антивирусного программного обеспечения;

– определение параметров и субъектов для процедур резервного копирования;

– определение категорий пользователей и назначение им прав;

– настройку политики контроля событий безопасности на серверах и рабочих станциях, входящих в состав ИСПДн;

– конфигурирование средств межсетевого экрана (МЭ) и коммуникационного оборудования.

– оценку эффективности реализованных механизмов защиты.

3.2 Подготавливать предложения для включения в планы и программы работ мероприятий по принятию организационных и инженерно-технических мер защиты ИСПДн.

3.3 Выполнять комплекс работ, связанных с контролем и защитой информации, на основе разработанных программ и методик.

3.4 Организовывать работы по сбору, анализу и систематизации сведений об объектах ИСПДн и о подлежащей защите информации ограниченного доступа, циркулирующей в ИСПДн.

3.5 Контролировать защищенность всех пользовательских рабочих мест ИСПДН.

3.6 Вести журналы регистрации событий информационной безопасности и мер, которые были приняты для устранения попыток НСД.

4. Особенности настройки и конфигурирования системы защиты информации от несанкционированного доступа «Dallas Lock 8.0» приведены в документах «Описание применения» и «Руководство оператора», «Руководство по эксплуатации».

5. Особенности настройки и конфигурирования Программный комплекс «ViPNet Клиент КС2, версия 3.1»,, приведены в документе «ViPNet Контроль приложений, руководство пользователя», «ViPNet Деловая почта, руководство пользователя», «ViPNet Client Монитор, руководство пользователя»

6. Обязанности пользователя ИСПДн:

6.1 Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке машинных носителей информации, а также руководящих и организационно-распорядительных документов на ИСПДн.

6.2 Пользователи перед началом обработки в ИСПДн файлов, хранящихся на съемных носителях информации, должны осуществить проверку файлов на наличие компьютерных вирусов.

6.3 Соблюдать установленный режим разграничения доступа к информационным ресурсам: получать у ответственного за информационную безопасность (ответственному за ИБ) пароль, надежно его запоминать и хранить в тайне.

6.4 Немедленно докладывать ответственному ИБ обо всех фактах и попытках НСД к обрабатываемой на ОВТ информации или об ее исчезновении (искажении).

6.5 Пользователям ОВТ запрещается:

6.5.1 записывать и хранить информацию на неучтенных носителях информации;

6.5.2 оставлять во время работы магнитные носителях информации без присмотра, передавать их другим лицам и выносить за пределы помещения, в котором разрешена обработка информации;

6.5.3 отключать (блокировать) средства защиты информации, предусмотренные организационно-распорядительными документами на ИСПДн;

6.5.4 обрабатывать информацию с выключенным или нефункционирующими устройствами защиты информации;

6.5.5 самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

6.5.6 сообщать (или передавать) посторонним лицам личные атрибуты доступа к ресурсам ОВТ;

6.5.7 работать в ИСПДн при обнаружении каких-либо неисправностей;

6.5.8 вводить в ОТСС персональные данные под диктовку или с микрофона;

6.5.9 привлекать посторонних лиц для производства ремонта ОТСС без согласования со специалистом по защите информации.

7. Все изменения конфигурации технических и программных средств ИСПДн МДОБУ, а также внесение необходимых изменений в настройки средств защиты от несанкционированного доступа (НСД) и средств контроля целостности файлов, должны производиться под контролем администратора безопасности информации и ответственного за эксплуатацию СЗИ .

7.1 Основанием для внесения изменений в программное обеспечение и состав технических средств является служебная записка (заявка). В заявке указываются следующие виды изменений в составе технических и программных средств:

– добавление устройства (узла, блока);

– замена устройства (узла, блока);

– изъятие устройства (узла, блока);

– установка (развертывание) программных средств, необходимых для решения определенной задачи, добавление возможности, решения новой задачи;

– обновление (замена) программных средств;

– удаление программных средств.

7.2 Ответственный за безопасность информации СЗПДн ИСПДн МДОБУ рассматривает заявку, определяет возможность внесения изменений и вносит изменения в состав аппаратных средств и программного обеспечения.

7.3 Установка или обновление прикладного программного обеспечения в СЗПДн ИСПДн должны проводиться в соответствии с технологией проведения модификаций программных комплексов. Установка и обновление общего программного обеспечения (ПО) (системного, тестового и т.п.) производится с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.), а прикладного ПО - с

эталонных копий программных средств. После установки программного средства осуществляется проверка его функционирования и составляется акт ввода в эксплуатацию.

7.4 Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность и на отсутствие опасных функций (программ, вирусов).

7.5 После установки (обновления) ПО администратор безопасности информации должен провести настройку СЗИ и проверить работоспособность ПО.

7.6 В случае обнаружения не декларированных (не описанных в документации) возможностей программного средства пользователи АРМ немедленно докладывают администратору безопасности информации. Дальнейшее использование программного средства до получения специальных указаний прекращается.

7.7 Изъятие рабочей станции (пользовательского АРМ) и ее передача на склад (в ремонт или для решения иных задач) осуществляется только после того, как администратор безопасности информации снимет с данной рабочей станции средства защиты и примет необходимые меры для удаления (затирания) защищаемой информации, хранимой на дисках. Факт уничтожения данных, находившихся на дисках рабочей станции, оформляется актом. Акт подписывается ответственный за безопасность информации и утверждается руководителем структурного подразделения, в чьём ведении находится АРМ.

7.8 Допуск новых пользователей к решению задач с использованием вновь развернутого программного обеспечения (либо изменение полномочий доступа пользователей) осуществляется согласно установленного порядка составления списка лиц и инструкции по учету лиц, допущенных к работе с персональными данными в СЗПДн ИСПДн МДОБУ. Оригиналы заявок, на основании которых проводились изменения в составе технических или программных средств с отметками о внесении изменений в состав аппаратно-программных средств, должны храниться у администратора безопасности информации СЗПДн ИСПДн МДОБУ. Оригиналы заявок могут использоваться:

– для восстановления конфигурации СЗПДн ИСПДн МДОБУ после аварий;

– для проверки правильности установки и настройки средств защиты;

– для контроля правомерности установки технических или программных средств с целью разбора конфликтных ситуаций.

8. Перед проведением работ по внесению изменений в состав технических и программных средств СЗПДн ИСПДн МДОБУ необходимо согласовать возможность таких изменений с органом, проводившим работы по аттестации. В случае

положительного решения представители органа по аттестации осуществляют надзор за всеми приводящимися работами и делают необходимые отметки в Аттестате соответствия СЗПДн ИСПДн МДОБУ требованиям по безопасности информации.

9. Проведение работ по изменению состава технических и программных средств СЗПДн ИСПДн МДОБУ без согласования с органом по аттестации прекращает действие выданного Аттестата соответствия.

«УТВЕРЖДАЮ»
Заведующий МДОБУ
«Муринский ДСКВ № 1»
М.Н.Арныбашева
Приказ от «20» 12 2013 № 08 -ОД

ИНСТРУКЦИЯ
по организации антивирусной защиты.

Общие положения

1. В образовательном учреждении руководителем должно быть назначено лицо, ответственное за безопасность информационной системы персональных данных и эксплуатацию средств защиты (антивирусной). В противном случае вся ответственность за обеспечение антивирусной защиты ложится на руководителя образовательного учреждения.
2. В образовательном учреждении может использоваться только лицензионное антивирусное программное обеспечение.

   Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).
4. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.
5. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

Требования к проведению мероприятий по антивирусной защите

1. Ежедневно в начале работы при загрузке компьютера (для серверов ЛВС - при перезапуске) в автоматическом режиме должно выполняться обновление антивирусных баз и проводиться антивирусный контроль всех дисков и файлов персонального компьютера.
2. 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 образовательного 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.).
3. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи обязаны:

   - приостановить работу;

   - немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение информационной безопасности в образовательном учреждении;

   - совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

   - провести лечение или уничтожение зараженных файлов;

- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, ответственный за антивирусную защиту обязан направить зараженный вирусом файл на внешнем носителе в организацию, с которой заключен договор на антивирусную поддержку для дальнейшего исследования.

Ответственность

Ответственность за организацию антивирусной защиты возлагается на руководителя образовательного учреждения или лицо им назначенное.

Ответственность за проведение мероприятий антивирусного контроля и соблюдение требований настоящей Инструкции возлагается на ответственного за обеспечение антивирусной защиты.

Периодический контроль за состоянием антивирусной защиты в образовательном учреждении осуществляется руководителем.

«УТВЕРЖДАЮ»
Заведующий МДОБУ
_____ М.Н. Арабашева
Приказ от «10» 12 2016 №08 -ОД

ИНСТРУКЦИЯ
по организации парольной защиты ИСПДн

1 Общие положения

1.1. **Первичный пароль** - комбинация символов (буквы, цифры, знаки препинания, специальные символы), устанавливаемые ответственным при создании новой учетной записи.

1.1.1. Установку и сохранность первичного пароля производит ответственный за создание новой учетной записи.

1.1.2. Первичный пароль может содержать несложную комбинацию символов, либо повторяющиеся символы.

1.1.3. При создании первичного пароля, ответственный обязан установить опцию, требующую смену пароля при первом входе в систему, а также уведомить владельца учетной записи о необходимости произвести смену пароля.

1.1.4. Первичный пароль так же используется при сбросе забытого пароля на учетную запись. В любом случае, при использовании первичного пароля все требования настоящего документа сохраняются.

1.2. **Основной пароль** – комбинация символов (буквы, цифры, знаки препинания, специальные символы), известная только сотруднику организации, используемая для подтверждения подлинности владельца учетной записи.

1.3. Установку основного пароля производит пользователь при первом входе в систему с новой учетной записью.

1.4. При выборе пароля необходимо руководствоваться инструкцией «Требованиями к паролям»

1.5. Пользователь несет персональную ответственность за сохранение в тайне основного пароля. Запрещается сообщать пароль другим лицам, записывать его, а также пересылать открытым текстом в электронных сообщениях.

1.6. Пользователь обязан не реже одного раза в месяц производить смену основного пароля соблюдая требования настоящего документа.

1.7. В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно сообщить об этом в отдел автоматизированных информационных систем (далее АИС) и изменить основной пароль.

1.8. Восстановление забытого основного пароля пользователя осуществляется ответственным, путем изменения (сброса) основного пароля пользователя на первичный пароль на основании письменной либо электронной заявки пользователя.

1.9. Устная заявка пользователя на изменение пароля не является основанием для проведения таких изменений.

1.10. Для предотвращения угадывания паролей ответственный обязан настроить механизм блокировки учетной записи при трехкратном неправильном вводе пароля.

1.11. Разблокирование учетной записи пользователя осуществляется ответственным на основании заявки владельца учетной записи (возможен вариант автоматического разблокирования через продолжительный промежуток времени).

1.12. **Административный пароль** - комбинация символов (буквы, цифры, знаки препинания, специальные символы), известная системному администратору, используемая при настройке служебных учетных записей, учетных записей служб и сервисов, а также специальных учетных записей.

1.13. При выборе административного пароля необходимо руководствоваться инструкцией «Требованиями к паролям».

1.14. Ответственный работник несет персональную ответственность за сохранение в тайне административного пароля. Запрещается сообщать пароль другим лицам, записывать его, а также пересылать открытым текстом в электронных сообщениях.

1.15. Ответственный работник обязан не реже одного раза в месяц производить смену административного пароля, соблюдая требования настоящего документа.

1.16. В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно сообщить об этом руководителю и изменить административный пароль.

1.17. Копии административных паролей должны храниться в опечатанном конверте в сейфе.

«УТВЕРЖДАЮ»
Заведующий МДОБУ
«Муринский ДСКВ № 1»
М.Н. Арцыбашева
Приказ от «13» 08 2015 №82 ОД

ИНСТРУКЦИЯ
по обеспечению безопасности персональных данных.

1 Общие положения

1.1. Сотрудники, допущенные к обработке персональных данных (ПДн) назначаются приказом руководителя.

1.2. Ответственные за обеспечение безопасности ПДн подчиняется непосредственно руководителю МДОБУ «Муринский ДСКВ №1» (далее – МДОБУ)

1.3. Ответственные за обеспечение безопасности ПДн в своей работе руководствуются настоящей инструкцией, Политикой информационной безопасности, руководящими и нормативными документами ФСТЭК России и регламентирующими документами МДОБУ.

1.4. Ответственные за обеспечение безопасности ПДн отвечают за поддержание необходимого уровня безопасности объектов защиты.

1.5. Ответственные за обеспечение безопасности ПДн являются ответственными должностными лицами МДОБУ уполномоченными на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты ИСПДн и ее ресурсов на этапах эксплуатации и модернизации и осуществляющими контроль над соблюдением положений ОРД.

1.6. Ответственнык за обеспечение безопасности ПДн должны иметь специальное рабочее место, размещенное в здании МДОБУ так, чтобы исключить несанкционированный доступ к нему посторонних лиц и других пользователей.

1.7. Рабочее место ответственных за обеспечение безопасности ПДн должно быть оборудовано средствами физической защиты (личный сейф, железный шкаф или другое), подключением к ИСПДн, а так же средствами контроля технических средств защиты.

1.8. Требования ответственных за обеспечение безопасности ПДн, связанные с выполнением ими своих должностных обязанностей, обязательны для исполнения всеми пользователями ИСПДн.

1.9. Ответственные за обеспечение безопасности ПДн несеут ответственность за качество проводимых ими работ по контролю действий пользователей при работе в ИСПДн, состояние и поддержание установленного уровня защиты ИСПДн.

2 Должностные обязанности

Ответственные за обеспечение безопасности ПДн обязаны:

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

2.2. Осуществлять контроль над соблюдением режима обработки ПДн и режима защиты ПДн.

2.3. Анализировать состояние защиты ИСПДн и ее отдельных подсистем.

2.4. Осуществлять организацию анализа и пересмотра имеющихся угроз безопасности ПДн, а так же предсказание появления новых, еще неизвестных, угроз.

2.5. Поддержание в актуальном состоянии нормативно-организационных документов.

2.6. Осуществлять контроль над внесением изменений в штатное программное обеспечение.

2.7. Контролировать работу пользователей в сетях общего пользования и (или) международного обмена.

2.8. Своевременно анализировать журнал учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений.

2.9. Не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач.

2.10. Не допускать к работе на элементах ИСПДн посторонних лиц.

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

3.Ответственность сотрудника

3.1.Сотрудники, участвующие в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных несут персональную ответственность за свои действия.

4.Сотруднику запрещается

4.1.Использовать для хранения персональных данных неучтенные носители информации;

4.2.Оставлять во время работы носители информации без присмотра, передавать их другим лицам и выносить за пределы помещения, в котором разрешена обработка персональных данных;

4.3.Отключать (блокировать) средства защиты информации;

производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств;

4.4.Обрабатывать информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя;

4.5.Сообщать (или передавать) посторонним лицам личные атрибуты доступа.