Приложение № 1
к приказу от 15.08.2017 №157

ПОЛОЖЕНИЕ
по организации работы по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в МДОУ «Детский сад «Ёлочка» г. Надыма» (далее - Положение)

1. Общие положения

1.1. Положение определяет основные мероприятия и порядок проведения работ по обеспечению безопасности персональных данных (далее – ПД) при их обработке в информационных системах ПД (далее – ИСПД) в МДОУ «Детский сад «Ёлочка» г. Надыма» (далее – МДОУ, оператор). Положение распространяется на работников (далее – сотрудники).

1.2. Все сотрудники МДОУ, участвующие в обработке ПД в информационных системах МДОУ, должны быть ознакомлены с Положением.

2. Порядок организации работ по обеспечению безопасности ПД

2.1. Обработка ПД в ИСПД МДОУ осуществляется в соответствии с требованиями федерального закона, нормативных и методических документов уполномоченных федеральных органов исполнительной власти по обеспечению безопасности ПД и иными правовыми актами в области защиты ПД.

2.2. С целью организации обработки ПД и обеспечения безопасности ПД в МДОУ:

– назначается ответственный за организацию обработки ПД – специалист по кадрам;

– назначается администратор безопасности ИСПД – инженер-электорник;

– утверждается перечень должностных лиц, допущенных к обработке ПД;

– утверждается перечень ИСПД.

2.2.1. Помещения, в которых разрешена обработка ПД, расположены в зданиях по адресам:

- Ямало-Ненецкий автономный округ, г. Надым, ул. Зверева, 9/1;

- Ямало-Ненецкий автономный округ, г. Надым, ул. Геологоразведчиков, 3/1.

2.3. Лица, допущенные к обработке ПД, в обязательном порядке под подпись знакомятся с настоящим Положением и подписывают обязательство о неразглашении информации, содержащей ПД, по форме согласно приложению № 1 к настоящему Положению.

2.4. Защищаемая информация ИСПД МДОУ определяется в соответствии с Перечнем ПД, подлежащих защите.

2.5. Безопасность ПД при их обработке в информационной системе обеспечивают ответственные лица за обеспечение безопасности персональных данных МДОУ, осуществляющие обработку ПД.

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

2.7. Выбор средств защиты информации для системы защиты ПД осуществляется уполномоченным лицом оператора по защите ПД в соответствии с утвержденным уровнем защищенности.

3. Требования к обеспечению безопасности ПД

3.1. Требования к обеспечению безопасности ПД при их обработке в ИСПД МДОУ формируются на основании установленного уровня защищенности ИСПД и перечня актуальных угроз безопасности ПД.

3.2. Требования к обеспечению безопасности ПД при их обработке в ИСПД МДОУ реализуются комплексом организационных и технических мер, средств и механизмов защиты информации.

4. Порядок обработки ПД

4.1. Обработка ПД осуществляется в целях соблюдения законов и других нормативных правовых актов РФ, осуществления и выполнения возложенных на оператора функций, полномочий и обязанностей.

4.2. Оператор получает и обрабатывает ПД только с письменного согласия субъекта ПД по форме согласно приложению № 2 к настоящему Положению.

4.3. Операторы и иные лица, получившие доступ к ПД, обязаны не раскрывать третьим лицам и не распространять ПД без согласия субъекта ПД.

4.4. Все ПД оператор получает непосредственно от самого субъекта ПД путем анкетирования и сбора официальных документов.

4.5. Оператор вправе организовывать проверки ПД с целью формирования кадрового резерва.

4.6. Оператор сообщает субъекту ПД цели, предположительные источники, способы получения ПД, характер ПД и последствия отказа субъекта ПД дать письменное согласие на их получение.

4.7. Оператор имеет право передавать ПД субъектов ПД в налоговые органы, Пенсионный фонд РФ, Фонд социального страхования РФ, Федеральную инспекцию труда и иные установленные федеральным законодательством РФ органы и организации. Использование ПД допустимо только в соответствии с целями, определившими их получение. Передача ПД субъекта ПД возможна только с согласия субъекта ПД, если иное не предусмотрено законодательством РФ.

4.8. При обработке ПД оператор обязан обеспечить право субъекта ПД на:

- получение полной информации об их ПД и обработке этих данных;
- свободный бесплатный доступ к своим ПД, включая право на получение копий любой записи, содержащей ПД, за исключением случаев, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон);
- обжалование в суде любых неправомерных действий или бездействия оператора при обработке и защите ПД субъекта ПД.

4.9. Все представленные ПД остаются на хранении у оператора. За хранение ПД субъектов ПД отвечает ответственное должностное лицо. Режим хранения ПД должен исключать возможность их утраты или неправомерного использования.

4.10. Оператор вправе поручить обработку ПД другому лицу с согласия субъекта ПД.

4.11. В случае, если оператор поручает обработку ПД другому лицу, ответственность перед субъектом ПД за действия указанного лица несет оператор.

4.12. В целях информационного обеспечения могут создаваться общедоступные источники ПД (в том числе справочники, адресные книги). В общедоступные источники ПД с письменного согласия субъекта ПД могут включаться его фамилия, имя, отчество, абонентский номер, сведения о профессии и иные ПД, сообщаемые субъектом ПД.

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

5. Порядок обработки ПД в ИСПД с использованием средств автоматизации

5.1. Обработка ПД с использованием средств автоматизации осуществляется в соответствии с требованиями постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их

обработке в информационных системах персональных данных», нормативных и методических документов уполномоченных федеральных органов исполнительной власти по обеспечению безопасности ПД.

5.2. Под актуальными угрозами безопасности ПД понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к ПД при их обработке в ИСПД, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение ПД, а также иные неправомерные действия.

5.3. Определение типа угроз безопасности ПД, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона.

5.4. Не допускается обработка ПД в ИСПД с использованием средств автоматизации при отсутствии:

– утвержденной организационно-распорядительной документации о порядке работы и защиты ПД в организации, включающих акт определения уровня защищенности ИСПД, инструкции ответственного за организацию обработки ПД в структурных подразделениях, администратора безопасности ПД, пользователя ИСПД, по организации антивирусной защиты ИСПД, организации парольной защиты ИСПД 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 ИСПД и в помещения, предназначенные для обработки ПД.

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

5.6. Решение, порождающее юридические последствия в отношении субъекта ПД или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его ПД только при наличии согласия в письменной форме субъекта ПД или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта ПД.

5.7. Оператор обязан разъяснить субъекту ПД порядок принятия решения па основании исключительно автоматизированной обработки его ПД и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом ПД своих прав и законных интересов.

5.8. Оператор обязан рассмотреть возражение в течение тридцати дней со дня его получения и уведомить субъекта ПД о результатах рассмотрения такого возражения.

6. Порядок обработки ПД в ИСПД без использования средств автоматизации

6.1. Обработка ПД без использования средств автоматизации (неавтоматизированная) – обработка ПД, содержащихся в ИСПД либо извлеченных из такой системы, если такие действия с ПД, как использование, уточнение, распространение, уничтожение ПД в отношении каждого из субъектов ПД, осуществляются при непосредственном участии человека.

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

6.3. При неавтоматизированной обработке различных категорий ПД должен использоваться отдельный материальный носитель для каждой категории ПД.

6.4. При неавтоматизированной обработке ПД на бумажных носителях:

– не допускается фиксация на одном бумажном носителе ПД, цели обработки которых заведомо не совместимы;

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

– документы, содержащие ПД, формируются в дела в зависимости от цели обработки ПД;

– дела с документами, содержащими ПД, должны иметь внутренние описи документов с указанием цели обработки и категории ПД.

6.5. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПД (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 ПД, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта ПД, источник получения ПД, сроки обработки ПД, перечень действий с ПД, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки ПД;

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

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

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

6.6. Неавтоматизированная обработка ПД в электронном виде осуществляется на внешних электронных носителях информации.

6.7. При отсутствии технологической возможности осуществления неавтоматизированной обработки ПД 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 ПД лиц, не допущенных к их обработке.

6.8. Электронные носители информации, содержащие ПД, учитываются в журнале учета электронных носителей ПД, 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 ПД.

Порядок ведения журнала учета электронных носителей ПД осуществляет ответственный из числа сотрудников отдела автоматизированных систем оператора.

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

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

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

6.10. Документы и внешние электронные носители информации, содержащие ПД, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах. При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

7. Меры, направленные на обеспечение безопасности ПД

7.1. Оператор обязан принимать меры, необходимые и достаточные для обеспечения безопасности ПД.

7.2. К мерам обеспечения безопасности ПД относятся:

1) назначение оператором ответственного за организацию обработки ПД;

2) издание оператором документов, определяющих политику оператора в отношении обработки ПД, локальных актов по вопросам обработки ПД, 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 ПД в соответствии со статьей 19 Федерального закона.

7.3. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПД, к сведениям о реализуемых требованиях к защите ПД.

7.4. Оператор обязан представить документы и локальные акты и (или) иным образом подтвердить принятие мер по запросу уполномоченного органа по защите прав субъектов ПД.

7.5. Оператор определяет уровень защищенности ПД в соответствии с требованиями к защите ПД при их обработке в ИСПД, утвержденным постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

8. Порядок контроля и ответственность должностных лиц

8.1. Контроль за выполнением настоящих требований организуется и проводится оператором (уполномоченным лицом). Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом).

8.2. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности ПД в ИСПД, осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, в пределах их полномочий и без права ознакомления с ПД, обрабатываемыми в информационных системах ПД.

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

8.4. Сотрудники МДОУ, допущенные установленным порядком к ПД, виновные в нарушении норм, регулирующих получение, обработку и защиту ПД, несут дисциплинарную, административную, гражданско-правовую, уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение № 1
к Положению по организации работ
по обеспечению безопасности
персональных данных при их
обработке в информационных
системах ПД в МДОУ

ОБЯЗАТЕЛЬСТВО
о неразглашении информации, содержащей персональные данные

Я, _____,
(ФИО работника)

исполняющий (ая) должностные обязанности по замещаемой должности _____

_____
(структурное подразделения)

предупрежден(а) о том, что на период исполнения должностных обязанностей в соответствии с должностной инструкцией 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 сведения содержащие персональные данные, служебную или иную конфиденциальную информацию, немедленно сообщать непосредственному руководителю, начальнику Департамента образования или лицу его заменяющего;

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

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

5. при прекращении моего права на допуск к конфиденциальной информации, содержащей персональные данные (перевод на должность, не предусматривающую доступ к персональным данным, прекращение трудовых отношений), прекратить обработку персональных данных, все документы и иные материальные носители информации со сведениями, содержащими служебную информацию ограниченного распространения, и другие документы, которые находились в моем распоряжении в связи с выполнением мною должностных обязанностей на время работы, сдать непосредственному руководителю.

6. в течение 3-х лет после прекращения права на допуск к информации, содержащей персональные данные, не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

До моего сведения доведено (разъяснено) Положение по организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в МДОУ, утвержденное приказом МДОУ.

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.

«__» _____20__г _____

(подпись, фамилия, имя, отчество прописью полностью)

Приложение № 2
к Положению по организации работ
по обеспечению безопасности
персональных данных при их
обработке в информационных
системах ПД в МДОУ

СОГЛАСИЕ
на обработку персональных данных

_____
(наименование предприятия, адрес, Ф.И.О. руководителя)

_____
_____
_____
_____
(фамилия, инициалы заявителя)

_____

_____
(адрес, место регистрации)

_____
(паспортные данные, серия, номер, кем и когда выдан)

В соответствии со ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», не возражаю против _____ Вами сведений обо мне,
получения/сообщения

содержащих данные о: _____
перечень ПД

_____
указать, откуда могут быть получены или куда переданы ПД

с целью _____
указать цель обработки ПД

в _____ форме
документальной/электронной/устной (по телефону)

в течение _____
указать срок действия согласия

Настоящее заявление может быть отозвано мной в письменной форме.
Юридические последствия отказа предоставить свои ПД мне разъяснены.

_____
подпись заявителя, дата

Приложение № 3
к Положению по организации работ
по обеспечению безопасности
персональных данных при их обработке в
информационных системах ПД в МДОУ

Форма журнала
учета электронных носителей персональных данных

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

Приложение № 2
к приказу МДОУ
от 15.08.2017 № 157

ПОЛОЖЕНИЕ
об организации работы с персональными данными работников
МДОУ «Детский сад «Ёлочка» г. Надыма» (далее - Положение)

1. Общие положения

1.1. Настоящее Положение об организации работы с персональными данными работников Муниципального дошкольного образовательного учреждения «Детский сад «Ёлочка» г. Надыма» (далее – МДОУ) определяет порядок обработки, хранения, использования и защиты персональных данных лиц, работающих в МДОУ, обеспечение защиты прав работников при обработке их персональных данных, а также ответственность лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.2. Настоящее Положение разработано в соответствии с Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 25.12.2008 № 273-ФЗ «О противодействии коррупции».

1.3. С настоящим Положением граждане при поступлении на работу знакомятся под роспись.

1.4. Для целей настоящего Положения используются следующие установленные федеральными законами основные понятия:

- **персональные данные** (далее-ПД) **–** любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных) и необходимая работодателю в связи с трудовыми отношениями;

- **оператор** – МДОУ, организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

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

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

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

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

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

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

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

- **информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

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

2. Состав персональных данных

2.1. ПД и иные сведения, содержащиеся в личных делах работников, относятся к сведениям конфиденциального характера (за исключением сведений, которые в установленных федеральными законами случаях могут быть опубликованы в средствах массовой информации).

2.2. К документам, содержащим информацию ПД, относятся следующие документы и их комплексы:

1) документы, удостоверяющие личность работника или содержащие сведения о работнике:

- паспорт гражданина Российской Федерации (временное удостоверение личности гражданина Российской Федерации, выдаваемого на период оформления паспорта в порядке, утверждаемом уполномоченным федеральным органом исполнительной власти);
- документы воинского учета;
- страховое свидетельство обязательного пенсионного страхования;
- документы об образовании и (или) квалификации (аттестаты, дипломы, удостоверения, свидетельства, сертификаты, др.);
- трудовая книжка;
- медицинские справки и заключения;
- свидетельство о присвоении идентификационного номера налогоплательщика;
- анкета, заполняемая лицом при поступлении на муниципальную службу.

2) учетные документы по личному составу:

- личная карточка (формы N Т-2**,** N Т-2 ГС (МС);

- личное дело работника;

- трудовая книжка работника;

- вспомогательные регистрационно-учетные формы, содержащие сведения персонального характера (журнал (книга) регистрации распоряжений по личному составу, книга учета движения трудовых книжек и вкладышей к ним, журнал регистрации справок и других документов, журнал регистрации служебных удостоверений, журнал учета листков нетрудоспособности, журнал регистрации трудовых договоров и дополнительных соглашений к ним, журнал учета личных дел, журнал учета работников направленных в командировки);

3) трудовые договоры (контракты), соглашения об изменении (дополнении) трудовых договоров (контрактов), договоры о материальной ответственности;

4) приказы по личному составу (подлинники и копии):

- приказы о приеме работника на работу, о переводе работника на другую работу, о прекращении (расторжении) трудового договора с работником (увольнении);

- приказы о предоставлении отпуска, о поощрении, взыскании;

5) документы об оценке деловых и профессиональных качеств работника при приеме на работу и в процессе работы (тесты, анкеты, резюме, отзывы и т.д.);

6) документы, отражающие деятельность аттестационных и конкурсных комиссий (протоколы заседаний, аттестационные и экзаменационные листы, решения и др.);

7) документы, отражающие результаты служебных расследований и (или) рассмотрение вопроса о привлечении работника к дисциплинарной ответственности (служебные и объяснительные записки, акты, справки, протоколы и др.);

8) копии отчетов, иных документов, направляемых в государственные органы статистики, налоговые органы и другие организации;

9) документы бухгалтерского учета, содержащие информацию о расчетах с персоналом (лицевые счета, расчетно-платежные ведомости, платежные ведомости и т.д.);

10) записи актов гражданского состояния;

11) номера телефонов;

12) наличие (отсутствие) судимости;

13) классный чин федеральной государственной гражданской службы, гражданской службы субъекта Российской Федерации, муниципальной службы, дипломатический ранг, воинское, специальное звание, классный чин правоохранительной службы (кем и когда присвоены);

14) государственные награды, иные награды и знаки отличия (кем награжден и когда);

15) результаты обязательных предварительных (при поступлении на работу) и периодических медицинских осмотров (обследований).

2.3. Если ПД содержатся в иных документах, на них распространяется действие настоящего Положения.

3. Обработка, хранение, использование и защита ПД

3.1. Обработка ПД осуществляется с соблюдением действующего законодательства РФ в целях обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации, Ямало-Ненецкого автономного округа в сфере трудовых правоотношений, при обращении граждан для содействия в трудоустройстве и иным вопросам, для обучения и продвижения по службе, для обеспечения

личной безопасности, для обеспечения сохранности имущества, для оформления доверенностей, для прохождения конкурсного отбора, для перечисления безналичных платежей на счет работников, для заключения и регулирования трудовых отношений и иных непосредственно связанных с ними отношений между работниками и оператором как работодателем, для подтверждения этапов и характера трудовой деятельности, в том числе муниципальной службы, для ее взаимодействия с федеральными и региональными органами, органами местного самоуправления и организациями всех форм собственности, для совершения сбора, систематизации, накопления, хранения, уточнения, обновления, изменения, использования (в том числе и для передачи), обезличивания, блокирования, уничтожения и трансграничной передачи персональных данных с учетом действующего законодательства, с использованием как автоматизированных средств обработки персональных данных, так и без использования средств автоматизации.

3.2. Трансграничная передача ПД, осуществляемая в соответствии с законодательством Российской Федерации, международными соглашениями может быть запрещена или ограничена в целях безопасности Российской Федерации.

3.3. Получение ПД.

3.3.1. Граждане при поступлении на работу в МДОУ, а также работники МДОУ лично предоставляют свои ПД специалисту по кадрам.

3.3.2. Оператор вправе обрабатывать ПД только с письменного согласия работника по форме согласно приложению № 1 к настоящему Положению.

3.3.3. Если ПД возможно получить только у третьей стороны, то работник уведомляется об этом заранее и дает письменное согласие. Работнику сообщается о целях, предполагаемых источниках и способах получения ПД, а также о характере подлежащих получению ПД и последствиях отказа работника дать письменное согласие на их получение по форме согласно приложению № 1 к настоящему Положению.

3.3.4. Запрещается требовать от гражданина (работника) представления информации о политических, религиозных и иных убеждениях и частной жизни, получать и обрабатывать ПД о членстве в общественных объединениях или профсоюзной деятельности, за исключением случаев, предусмотренных Трудовым кодексом Российской Федерации или иными федеральными законами.

3.3.5. Оператор предоставляет работнику или его представителю возможность ознакомления с ПД, относящимися к работнику. В срок, не превышающий семи рабочих дней со дня предоставления работником ПД или его представителем сведений, подтверждающих, что ПД являются неполными, неточными или неактуальными, оператор вносит в них необходимые изменения.

3.3.6. ПД могут быть получены Оператором от лица, не являющимся субъектом ПД при наличии оснований в п. 2-11 части 1 ст. 6, части 2 ст.10, части 2 ст. 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

3.4. Хранение ПД.

3.4.1. Все представленные при оформлении на работу ПД остаются на хранении у оператора. За хранение ПД сотрудников отвечает специалист по кадрам, осуществляющий ведение личных дел сотрудников. Режим хранения ПД должен исключать возможность их утраты или неправомерного использования.

3.4.2. В отделе по работе с кадрами ПД хранятся на бумажных носителях в личных карточках и личных делах.

Хранение трудовых книжек работников осуществляется в соответствии с Правилами ведения и хранения трудовых книжек, изготовления бланков трудовых книжек и обеспечения

ими работодателей, утвержденными постановлением Правительства Российской Федерации от 16.04.2003 № 225.

Личные карточки и личные дела хранятся на бумажных носителях в папках в шкафах.

Учетные данные работников хранятся на бумажных и электронных носителях. Специалист по кадрам обеспечивает защиту ПД от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении ПД.

3.4.3. ПД, содержащиеся в первичной учетной документации по оплате труда работников, хранятся в централизованной бухгалтерии Департамента образования Надымского района.

В централизованной бухгалтерии ПД хранятся на бумажных носителях в папках в шкафах и в базах данных программ, используемых для осуществления деятельности.

3.4.4. ПД могут храниться в электронном виде в локальной компьютерной сети. Доступ к электронным базам данных, содержащим ПД, осуществляется через учетные записи, защищенные паролем, которые сообщаются индивидуально лицам, имеющим разрешенный доступ к ПД, необходимым им для выполнения трудовых функций или иными техническими способами ограничения доступа.

ПД, которые обрабатываются в информационных системах, подлежат защите от несанкционированного доступа и копирования. Безопасность ПД при их обработке в информационных системах обеспечивается с помощью системы защиты ПД, включающей организационные меры и средства защиты информации.

Отдел автоматизированных систем управления организационно-методического обеспечения муниципальных образовательных организаций Департамента образования (далее – отдел АСУ) осуществляет технические меры для защиты ПД от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении ПД в соответствии с требованиями законодательства.

3.4.5. ПД хранятся не дольше, чем этого требуют цели их обработки, и подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

Документы, содержащие ПД, подлежащие хранению в соответствии с номенклатурой дел, утвержденной в МДОУ, оформляются для архивного хранения в соответствии с действующим законодательством.

3.5. Использование ПД (в том числе их передача).

3.5.1. ПД данные работника используются для целей, связанных с выполнением трудовых функций.

3.5.2. Право доступа к ПД работника МДОУ с целью ознакомления имеют: заведующий, заместители заведующего.

3.5.3. Лица, уполномоченные на обработку ПД, имеют доступ только к тем ПД работников и в том объеме, которые необходимы им для выполнения функций, возложенных на них трудовым договором, должностной инструкцией.

Доступ других лиц к ПД осуществляется на основании письменного разрешения представителя нанимателя (работодателя).

3.5.4. Передача ПД работников третьим лицам и сторонним организациям.

Оператор вправе передавать ПД работника третьим лицам и сторонним организациям только при наличии письменного согласия работника.

При передаче ПД работника лица, получающие данную информацию, предупреждаются о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены.

3.5.5. Передача ПД работников в пределах МДОУ.

Специалист по кадрам вправе передавать ПД работника в централизованную бухгалтерию в случаях, установленных законодательством, необходимых для исполнения ими должностных обязанностей.

Обработку ПД, содержащихся в трудовых книжках, личных карточках, личных делах, а также хранение документов, содержащих ПД работников, уволенных из МДОУ, в течение установленного срока с дальнейшей их передачей в установленном порядке в архив осуществляет специалист по кадрам.

Обработку документации по оплате труда работников (лицевые счета, платежные ведомости, расчетные листки и др.) осуществляют специалисты централизованной бухгалтерии.

3.5.6. Лица, имеющие доступ к ПД работника, обязаны соблюдать режим конфиденциальности.

3.5.7. Сведения о доходах, расходах, об имуществе и обязательствах имущественного характера руководителя муниципальной образовательной организации, его супруги (супруга) и несовершеннолетних детей размещаются на официальном сайте Администрации муниципального образования Надымский район в порядке, утвержденном муниципальным правовым актом.

3.5.8. Разглашение конфиденциальной и иной информации работником, получившим доступ к ней или ставшей известной работнику при выполнении должностных обязанностей, не допускается.

3.6. Уничтожение ПД.

3.6.1. Документы, содержащие ПД, подлежат уничтожению в порядке, предусмотренном законодательством в области архивного делопроизводства РФ.

3.6.2. В случае отзыва работником согласия на обработку ПД оператор вправе продолжить обработку ПД без согласия субъекта ПД при наличии оснований, установленных Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных".

3.7. Защита ПД.

3.7.1. Оператор принимает меры по обеспечению защиты ПД от неправомерного их использования, для обеспечения выполнения обязанностей, предусмотренными действующим законодательством РФ.

3.7.2. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных действующим законодательством РФ, в том числе:

- назначает ответственных лиц по обработке ПД;

- применяет правовые, организационные и технические меры по обеспечению безопасности ПД;

- знакомит работников с настоящим Положением и их правами в области защиты ПД под роспись;

- обеспечивает доступ работникам к своим ПД, включая право на получение копий любой записи, содержащей его ПД, за исключением случаев, предусмотренных законодательством.

4. Права и обязанности субъекта ПД

4.1. В соответствии с законодательством в целях обеспечения защиты ПД, хранящихся у оператора, работник имеет право:

- получать полную информацию о своих ПД и обработке этих данных (в том числе автоматизированной);

- свободный доступ к своим ПД, включая право получать копии любой записи, содержащей ПД, за исключением случаев, предусмотренных федеральным законом;

- определять своих представителей для защиты своих ПД;

- требовать исключения или исправления неверных, или неполных ПД, а также данных, обработанных с нарушением действующего законодательства. Работник при отказе уполномоченного лица исключить или исправить его ПД имеет право заявить в письменной форме представителю нанимателя (работодателю) или уполномоченному им лицу о своем несогласии, обосновав соответствующим образом такое несогласие. ПД оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;

- требовать от оператора или уполномоченного им лица об извещении лиц, которым ранее были сообщены неверные или неполные ПД обо всех произведенных в них исключениях, исправлениях или дополнениях;

- обжаловать в суд любые неправомерные действия или бездействие оператора, или уполномоченного им лица при обработке и защите своих ПД.

4.2. В целях обеспечения требований законодательства при обработке ПД работника работник обязан передавать оператору или его представителю достоверные ПД и документы, содержащие информацию персонального характера, в случаях и порядке, установленных Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», иными федеральными законами и нормативно-правовыми актами.

5. Порядок контроля и ответственность должностных лиц

5.1. Контроль за выполнением настоящих требований организуется и проводится оператором (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 оператором (уполномоченным лицом).

5.2. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности ПД в информационных системах МДОУ, 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 ПД, обрабатываемыми в информационных системах оператора.

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

5.4. Сотрудники МДОУ, допущенные установленным порядком к ПД, виновные в нарушении норм, регулирующих получение, обработку и защиту ПД, несут дисциплинарную, административную, гражданско-правовую, уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение
к Положению об организации работы
с персональными данными работников
МДОУ «Детский сад «Ёлочка» г. Надыма»

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я _____
(фамилия, имя, отчество)
проживающий (-ая) по адресу: _____
_____
(номер основного документа, удостоверяющего личность, сведения о дате выдачи
_____
указанного документа и выдавшем его органе)
в соответствии со ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» даю свое согласие МДОУ «Детский сад «Ёлочка» г. Надыма» (далее - Оператор), расположенному по адресу: 629730, ЯНАО, г. Надым, ул. Зверева, 9/1, на обработку следующих моих персональных данных, которые получены от меня лично и/или любых третьих лиц (путем направления Оператором запросов в государственные органы, органы местного самоуправления, правоохранительные органы, судебные органы, органы прокуратуры, налоговые органы и другие компетентные уполномоченные органы, из иных общедоступных информационных ресурсов, из архивов, из информационных ресурсов, в том числе в рамках межведомственного электронного взаимодействия и т.д.):
- фамилия, имя, отчество (в том числе информацию о смене фамилии, имени, отчества);
- год, месяц, дата и место рождения;
- биографические данные;
- биометрические данные;
- адрес места жительства (по месту регистрации и (или) фактического проживания);
- контактная информация (номера телефонов (городской, мобильный), адрес электронной почты и т.д.);
- семейное и социальное положение;
- сведения о близких родственниках (родители (отец, мать), дети, муж, жена, родные братья, сестры);
- сведения о постановке на воинский учет и прохождении службы в Вооруженных Силах, отношение к воинской обязанности, воинское знание, состав рода войск, военный билет (приписное свидетельство);
- сведения о местах обучения (место нахождения, название образовательной организации, период обучения, специальность, квалификация, направление подготовки и др. в соответствии с документом об образовании и о квалификации);
- сведения о предыдущей трудовой деятельности, трудовая книжка и сведения, содержащиеся в ней (сведения о продолжительности общего трудового стажа, страхового стажа, непрерывного стажа, стажа государственной и/или муниципальной службы, награды (поощрения) и др.);
- сведения о состоянии здоровья и его соответствии выполняемой работе;
- сведения об отпусках и командировках;
- данные паспорта или иного документа, удостоверяющего личность;
- идентификационный номер налогоплательщика;
- страховой номер государственного (обязательного) пенсионного страхования;

- данные о допуске к сведениям, составляющим государственную тайну;
- сведения о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по учетам органов внутренних дел МВД России;
- сведения о социальных льготах, на которые я имею право в соответствии с законодательством РФ;
- иных,

в целях обеспечения соблюдения законов РФ и иных нормативных правовых актов в сфере трудовых правоотношений, оформления и регулирования трудовых отношений и иных, непосредственно связанных с ними отношений, между мной и Оператором как работодателем, взаимодействия с федеральными и региональными органами, органами местного самоуправления и организациями всех форм собственности для совершения сбора, систематизации, накопления, хранения, уточнения, обновления, изменения, использования (в том числе и для передачи), обезличивания, блокирования, уничтожения и трансграничной передачи персональных данных с учетом действующего законодательства РФ с использованием как автоматизированных средств обработки персональных данных, так и без использования средств автоматизации.

В случае изменения моих персональных учетных данных в течение срока действия трудового договора, обязуюсь информировать об этом Оператора в течение 30 дней с момента изменения моих персональных данных.

При оформлении трудовых отношений между мной и Оператором как работодателем согласие действует со дня его подписания до дня отзыва в письменной форме или в течение 50 лет с даты прекращения трудовых отношений.

При обращении мной к Оператору с целью участия в конкурсном отборе, рассмотрения обращений, в том числе резюме по вопросам, связанных с трудовыми отношениями, согласие действует со дня его подписания в течение 1 (одного) года.

В случае неправомерного использования моих персональных данных согласие на обработку персональных данных отзывается моим письменным заявлением.

"____"_____ 20____ г. _____

(подпись и фамилия, имя, отчество прописью полностью)

Приложение № 3
к приказу МДОУ «Детский сад
«Ёлочка» г. Надыма»
от 15.08.2017 № 157

ПРАВИЛА
работы с обезличенными персональными данными, обрабатываемыми в МДОУ «Детский сад «Ёлочка» г. Надыма»

1. Основные положения

1. Правила работы с обезличенными персональными данными, обрабатываемыми в в МДОУ «Детский сад «Ёлочка» г. Надыма» (далее – МДОУ) разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон) и Приказа Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных». Правила распространяются на работников МДОУ (далее – сотрудники).

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

1.1. Настоящие Правила определяют порядок работы с обезличенными персональными данными, обрабатываемыми в МДОУ.

2. Условия и методы обезличивания персональных данных

2.1. Обезличивание персональных данных может быть проведено с целью снижения ущерба от разглашения защищаемых персональных данных, снижения класса (уровня защищенности) информационных систем персональных данных (далее – ИСПД), в статистических или иных исследовательских целях, и по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Методы обезличивания должны обеспечивать требуемые свойства обезличенных данных, соответствовать предъявляемым требованиям к их характеристикам (свойствам), быть практически реализуемыми в различных программных средах и позволять решать поставленные задачи обработки персональных данных. К наиболее перспективным и удобным для практического применения относятся следующие методы обезличивания:

– метод введения идентификаторов (замена части сведений (значений персональных данных) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным);

– метод изменения состава или семантики (изменение состава или семантики персональных данных путем замены результатами статистической обработки, обобщения или удаления части сведений);

– метод декомпозиции (разбиение множества (массива) персональных данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств);

- метод перемешивания (перестановка отдельных записей, а также групп записей в массиве персональных данных).

2.1.1. Метод введения идентификаторов реализуется путем замены части персональных данных, позволяющих идентифицировать субъекта, их идентификаторами и созданием таблицы соответствия.

Метод обеспечивает следующие свойства обезличенных данных:

– полнота;
– структурированность;
– семантическая целостность;
– применимость.

Оценка свойств метода:

– обратимость (метод позволяет провести процедуру деобезличивания); вариативность (метод позволяет перейти от одной таблицы соответствия к другой без проведения процедуры деобезличивания);
– изменяемость (метод не позволяет вносить изменения в массив обезличенных данных без предварительного деобезличивания);
– стойкость (метод не устойчив к атакам, подразумевающим наличие у лица, осуществляющего несанкционированный доступ, частичного или полного доступа к справочнику идентификаторов, стойкость метода не повышается с увеличением объема обезличиваемых персональных данных);
– возможность косвенного деобезличивания (метод не исключает возможность деобезличивания с использованием персональных данных, имеющихся у других операторов);
– совместимость (метод позволяет интегрировать записи, соответствующие отдельным атрибутам);
– параметрический объем (объем таблицы (таблиц) соответствия определяется числом записей о субъектах персональных данных, подлежащих обезличиванию);
– возможность оценки качества данных (метод позволяет проводить анализ качества обезличенных данных).

Для реализации метода требуется установить атрибуты персональных данных, записи которых подлежат замене идентификаторами, разработать систему идентификации, обеспечить ведение и хранение таблиц соответствия.

2.1.2. Метод изменения состава или семантики реализуется путем обобщения, изменения или удаления части сведений, позволяющих идентифицировать субъекта.

Метод обеспечивает следующие свойства обезличенных данных:

– структурированность;
– релевантность;
– применимость;
– анонимность.

Оценка свойств метода:

– обратимость (метод не позволяет провести процедуру деобезличивания в полном объеме и применяется при статистической обработке персональных данных);
– вариативность (метод не позволяет изменять параметры метода без проведения предварительного деобезличивания);
– изменяемость (метод позволяет вносить изменения в набор обезличенных данных без предварительного деобезличивания);

– стойкость (стойкость метода к атакам на идентификацию определяется набором правил реализации, стойкость метода не повышается с увеличением объема обезличиваемых персональных данных);

– возможность косвенного деобезличивания (метод исключает возможность деобезличивания с использованием персональных данных, имеющихся у других операторов);

– совместимость (метод не обеспечивает интеграции с данными, обезличенными другими методами);

– параметрический объем (параметры метода определяются набором правил изменения состава или семантики персональных данных);

– возможность оценки качества данных (метод не позволяет проводить анализ, использующий конкретные значения персональных данных).

Для реализации метода требуется выделить атрибуты персональных данных, записи которых подвергаются изменению, определить набор правил внесения изменений и иметь возможность независимого внесения изменений для данных каждого субъекта.

При этом возможно использование статистической обработки отдельных записей данных и замена конкретных значений записей результатами статистической обработки (средние значения, например).

2.1.3. Метод декомпозиции реализуется путем разбиения множества записей персональных данных на несколько подмножеств и создание таблиц, устанавливающих связи между подмножествами, с последующим раздельным хранением записей, соответствующих этим подмножествам.

Метод обеспечивает следующие свойства обезличенных данных:

– полнота;

– структурированность;

– релевантность;

– семантическая целостность;

– применимость.

Оценка свойств метода:

– обратимость (метод позволяет провести процедуру деобезличивания);

– вариативность (метод позволяет изменить параметры декомпозиции без предварительного деобезличивания);

– изменяемость (метод позволяет вносить изменения в набор обезличенных данных без предварительного деобезличивания);

– стойкость (метод не устойчив к атакам, подразумевающим наличие у злоумышленника информации о множестве субъектов или доступа к нескольким частям раздельно хранимых сведений);

– возможность косвенного деобезличивания (метод не исключает возможность деобезличивания с использованием персональных данных, имеющихся у других операторов);

– совместимость (метод обеспечивает интеграцию с данными, обезличенными другими методами);

– параметрический объем (определяется числом подмножеств и числом субъектов персональных данных, массив которых обезличивается, а также правилами разделения персональных данных на части и объемом таблиц связывания записей, находящихся в различных хранилищах);

– возможность оценки качества данных (метод позволяет проводить анализ качества обезличенных данных).

Для реализации метода требуется предварительно разработать правила декомпозиции, правила установления соответствия между записями в различных хранилищах, правила внесения изменений и дополнений в записи и хранилища.

2.1.4. Метод перемешивания реализуется путем перемешивания отдельных записей, а также групп записей между собой.

Метод обеспечивает следующие свойства обезличенных данных:

– полнота;
– структурированность;
– релевантность;
– семантическая целостность;
– применимость;
– анонимность.

Оценка свойств метода:

– обратимость (метод позволяет провести процедуру деобезличивания); вариативность (метод позволяет изменять параметры перемешивания без проведения процедуры деобезличивания);
– изменяемость (метод позволяет вносить изменения в набор обезличенных данных без предварительного деобезличивания);
– стойкость (длина перестановки и их совокупности определяет стойкость метода к атакам на идентификацию);
– возможность косвенного деобезличивания (метод исключает возможность проведения деобезличивания с использованием персональных данных, имеющихся у других операторов);
– совместимость (метод позволяет проводить интеграцию с данными, обезличенными другими методами);
– параметрический объем (зависит от заданных методов и правил перемешивания и требуемой стойкости к атакам на идентификацию);
– возможность оценки качества данных (метод позволяет проводить анализ качества обезличенных данных).

Для реализации метода требуется разработать правила перемешивания и их алгоритмы, правила и алгоритмы деобезличивания и внесения изменений в записи.

Метод может использоваться совместно с методами введения идентификаторов и декомпозиции.

Также в МДОУ могут применяться любые другие, не запрещенные законодательством, методы.

3. Порядок работы с обезличенными персональными данными

3.1. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности без согласия субъекта персональных данных, за исключением их обработки для статистической или иной исследовательской деятельности, иных действий, не противоречащих действующему законодательству.

3.2. Обезличенные персональные данные могут обрабатываться с использованием средств автоматизации и без использования таковых.

3.3. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

- парольной политики;
- антивирусной политики;
- правил работы с отчуждаемыми носителями (в случае их применения);
- правил резервного копирования;
- Инструкции о порядке доступа в помещения, в которых ведется обработка персональных данных.

3.4. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

- правил хранения бумажных носителей;
- правил доступа к бумажным носителям и в помещения, где они хранятся.

Приложение № 4
к приказу МДОУ «Детский сад
«Ёлочка» г. Надыма»
от 15.08.2017 № 157

ИНСТРУКЦИЯ
по эксплуатации аттестованных информационных систем
МДОУ «Детский сад «Ёлочка» г. Надыма»

1. Общие положения

1.1. Настоящая Инструкция по эксплуатации аттестованных информационных систем МДОУ «Детский сад «Ёлочка» г. Надыма» (далее – МДОУ) разработана для реализации меры, установленной в соответствии с требованиями приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», а также Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», другими нормативными документами по безопасности информации, и определяет порядок эксплуатации аттестованных информационных систем в МДОУ, устанавливает ответственность администратора безопасности информации и работников (далее – сотрудники), за обеспечение безопасности информации при эксплуатации аттестованных информационных систем МДОУ.

1.2. Оператор - МДОУ, самостоятельно или совместно с другими лицами организующий и (или) осуществляющий обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

2. Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы

2.1. Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы осуществляется оператором в соответствии с эксплуатационной документацией на систему защиты информации и комплектом организационно-распорядительными документами по защите персональных данных и в том числе включает:

- управление (администрирование) системой защиты информации информационной системы;
- выявление инцидентов и реагирование на них;
- управление конфигурацией аттестованной информационной системы и ее системы защиты информации;
- контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в информационной системе.

В ходе управления (администрирования) системой защиты информации информационной системы осуществляются:

- заведение и удаление учетных записей пользователей, управление полномочиями пользователей информационной системы и поддержание правил разграничения доступа в информационной системе;
- управление средствами защиты информации в информационной системе, в том числе параметрами настройки программного обеспечения, включая программное обеспечение средств защиты информации, управление учетными записями пользователей, восстановление

работоспособности средств защиты информации, генерацию, смену и восстановление паролей;

– установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации, выпускаемых разработчиками (производителями) средств защиты информации;

– централизованное управление системой защиты информации информационной системы (при необходимости);

– регистрация и анализ событий в информационной системе, связанных с защитой информации (далее – события безопасности);

– информирование пользователей об угрозах безопасности информации, о правилах эксплуатации системы защиты информации информационной системы и отдельных средств защиты информации, а также их обучение;

– сопровождение функционирования системы защиты информации информационной системы в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее и организационно-распорядительных документов по защите информации.

2.2. В ходе выявления инцидентов и реагирования на них осуществляются:

– определение лиц, ответственных за выявление инцидентов и реагирование на них;

– обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

– своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами;

– анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

– планирование и принятие мер по устранению инцидентов, в том числе по восстановлению информационной системы и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

– планирование и принятие мер по предотвращению повторного возникновения инцидентов.

2.3. В ходе управления конфигурацией аттестованной информационной системы и ее системы защиты информации осуществляются:

– поддержание конфигурации информационной системы и ее системы защиты информации (структуры системы защиты информации информационной системы, состава, мест установки и параметров настройки средств защиты информации, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на систему защиты информации (поддержание базовой конфигурации информационной системы и ее системы защиты информации);

– определение лиц, которым разрешены действия по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации;

– управление изменениями базовой конфигурации информационной системы и ее системы защиты информации, в том числе определение типов возможных изменений базовой конфигурации информационной системы и ее системы защиты информации, санкционирование внесения изменений в базовую конфигурацию информационной системы и ее системы защиты информации, документирование действий по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации, сохранение данных об изменениях базовой конфигурации информационной системы и ее системы защиты информации, контроль действий по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации;

– анализ потенциального воздействия планируемых изменений в базовой

конфигурации информационной системы и ее системы защиты информации на обеспечение защиты информации, возникновение дополнительных актуальных угроз безопасности информации и работоспособность информационной системы;

– определение параметров настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию информационной системы и ее системы защиты информации;

– внесение информации (данных) об изменениях в базовой конфигурации информационной системы и ее системы защиты информации в эксплуатационную документацию на систему защиты информации информационной системы;

– принятие решения о повторной аттестации информационной системы (в случае изменения по результатам управления конфигурацией класса защищенности информационной системы, состава актуальных угроз безопасности информации или проектных решений по системе защиты информации информационной системы).

2.4. В ходе контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе, осуществляются:

– контроль за событиями безопасности и действиями пользователей в информационной системе;

– контроль (анализ) защищенности информации, содержащейся в информационной системе;

– анализ и оценка функционирования системы защиты информации информационной системы, включая выявление, анализ и устранение недостатков в функционировании системы защиты информации информационной системы;

– периодический анализ изменения угроз безопасности информации в информационной системе, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;

– документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе;

– принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) системы защиты информации информационной системы и повторной аттестации информационной системы (в случае изменения класса защищенности информационной системы, состава актуальных угроз безопасности информации или проектных решений по системе защиты информации информационной системы).

3. Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы

3.1. Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации осуществляется оператором в соответствии с эксплуатационной документацией на систему защиты информации информационной системы и организационно-распорядительными документами по защите информации и в том числе включает:

– архивирование информации, содержащейся в информационной системе;

– уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

3.2. Архивирование информации, содержащейся в информационной системе, должно осуществляться при необходимости дальнейшего использования информации в деятельности оператора.

3.3. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного носителя информации другому пользователю информационной системы или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения.

3.4. При выводе из эксплуатации машинных носителей информации, на которых

осуществлялись хранение и обработка информации, осуществляется физическое уничтожение этих машинных носителей информации.

4. **Ответственность**

Ответственность за проведение мероприятий в соответствии с требованиями настоящей Инструкции возлагается на ответственного за организацию обработки персональных данных в МДОУ, администратора безопасности информации МДОУ, ответственных за обеспечение безопасности, ответственного по защите информации МДОУ и сотрудников МДОУ.

Приложение № 5
к приказу МДОУ «Детский сад
«Ёлочка» г. Надыма»
от 15.08.2017 № 157

ИНСТРУКЦИЯ
по эксплуатации средств защиты информации
в МДОУ «Детский сад «Ёлочка» г. Надыма»

1. Информационная система персональных данных (далее – информационная система; ИС) МДОУ «Детский сад «Ёлочка» г. Надыма» (далее – МДОУ) представляет собой распределённую вычислительную сеть, в которой обрабатывается информация ограниченного доступа, содержащая персональные данные работников МДОУ (далее – сотрудники). Обработка информации осуществляется в многопользовательском режиме с разграничением прав доступа. Осуществляется подключение рабочих станций пользователей к сетям связи общего доступа. На технические средства установлены сертифицированные по требованиям ФСТЭК России средства защиты информации (далее – СЗИ).
2. В ИС установлены и настроены следующие средства защиты информации:
– Kaspersky Endpoint Security 10 для Windows;
– СЗИ от НСД Dallas Lock 8.0-C;
– ПО ViPNet Client 4 (исполнение 1).
3. Обязанности по сопровождению и настройке средств защиты возлагаются на администратора безопасности информации (далее – АБИ), являющегося ответственным за эксплуатацию СЗИ.
4. Ответственный за эксплуатацию СЗИ должен:
4.1. 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 ИС;
– конфигурирование средств межсетевого экрана (далее– МЭ) и коммуникационного оборудования;
– оценку эффективности реализованных механизмов защиты;
4.2. подготавливать предложения для включения в планы и программы работ мероприятий по принятию организационных и инженерно-технических мер защиты ИС;
4.3. выполнять комплекс работ, связанных с контролем и защитой информации, на основе разработанных программ и методик;
4.4. организовывать работы по сбору, анализу и систематизации сведений об объектах ИС и подлежащей защите информации ограниченного доступа, циркулирующей в ИС;
4.5. контролировать защищенность всех пользовательских рабочих мест ИС;
4.6. вести журнал учета средств защиты информации, эксплуатационной и

технической документации к ним, используемых в информационной системе персональных данных МДОУ по форме согласно приложению к настоящей Инструкции.

5. Особенности настройки и конфигурирования средств защиты информации приведены в эксплуатационной и технической документации на соответствующие средства защиты.

6. Обязанности пользователя ИС:

6.1. знать и соблюдать установленные требования по режиму обработки информации ограниченного доступа, учету, хранению и пересылке машинных носителей информации, а также руководящих и организационно-распорядительных документов на ИС;

6.2. пользователи перед началом обработки в ИС 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 АБИ пароль, надежно его запоминать и хранить в тайне;

6.4. немедленно докладывать АБИ обо всех фактах и попытках несанкционированного доступа (далее– НСД) к обрабатываемой на объектах вычислительной техники (далее– ОВТ) информации или об ее исчезновении (искажении).

7. Пользователям ОВТ запрещается:

7.1. записывать и хранить информацию на неучтенных носителях информации;

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

7.3. отключать (блокировать) средства защиты информации, предусмотренные организационно–распорядительными документами на ИС;

7.4. обрабатывать информацию с выключенным или нефункционирующими устройствами защиты информации;

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

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

7.7. работать в ИС при обнаружении каких-либо неисправностей;

8. Все изменения конфигурации технических и программных средств СЗИ, а также внесение необходимых изменений в настройки СЗИ от НСД и средств контроля целостности файлов, должны производиться под контролем администратора безопасности информации.

9. Проведение работ по изменению конфигурации технических и программных средств осуществляется в соответствии с Инструкцией по модификации технических и программных средств.

10. Проведение работ по изменению состава технических и программных средств СЗИ без согласования с органом по аттестации прекращает действие выданного Аттестата соответствия.

Приложение
к Инструкции по эксплуатации
средств защиты информации
в МДОУ

ЖУРНАЛ УЧЕТА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ, ЭКСПЛУАТАЦИОННОЙ И ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ К НИМ, ИСПОЛЬЗУЕМЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В МДОУ «ДЕТСКИЙ САД «ЁЛОЧКА» Г. НАДЫМА»

Начат «___» _____ 20 ___ г.

Окончен «___» _____ 20 ___ г.

На _____ листах

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

Индекс и наименование средства защиты информации (наименование эксплуатационной/ технической документации)	Серийный (заводской) номер	Номер специального защитного знака	Наименование организации, установившей средство защиты информации	Примечание (данные о сертификате, ФИО и подпись ответственного)
1	2	3	4	5

Приложение № 6
к приказу МДОУ «Детский сад «Ёлочка»
г. Надыма»
от 15.08.2017 № 157

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в МДОУ «Детский сад «Ёлочка» г. Надыма» (далее - Правила)

1. Общие положения

1.1. Настоящими Правилами осуществления внутреннего контроля соответствия обработки персональных данных (далее-ПД) требованиям к защите ПД в МДОУ «Детский сад «Ёлочка» г. Надыма» (далее - МДОУ) устанавливаются процедуры (основания, порядок и формы) проведения внутреннего контроля соответствия обработки ПД требованиям к защите персональных данных.

Правила распространяются на работников МДОУ.

1.2. Настоящие Правила разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными и муниципальными органами», и другими нормативными правовыми актами.

1.3. Целью настоящих Правил является выявление и предотвращение нарушений законодательства Российской Федерации в сфере ПД в МДОУ.

1.4. В Правилах используются основные понятия, определенные в статье 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

2. Процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных

2.1. В целях осуществления внутреннего контроля соответствия обработки ПД установленным требованиям в МДОУ организуется проведение проверок условий обработки ПД.

2.2. Проверки условий обработки ПД на соответствие требованиям к защите ПД, установленных в МДОУ (далее–проверки) осуществляются комиссией по защите персональных данных в МДОУ (далее–Комиссия). Проверки условий обработки ПД могут быть плановыми и внеплановыми.

2.3. Плановые проверки проводятся в соответствии с ежегодным планом проведения проверок, утвержденным председателем Комиссией.

2.4. План проведения проверок разрабатывается Комиссией.

2.5. Внеплановые проверки проводятся на основании поступившего в МДОУ письменного заявления физического лица (субъекта ПД) о нарушениях правил обработки персональных данных.

2.6. В течение 3-х (трех) рабочих дней с момента поступления в МДОУ заявления о

нарушениях правил обработки ПД принимается решение о проведении внеплановой проверки, которое оформляется протоколом Комиссии.

2.7. Проведение внеплановой проверки организуется в течение трех рабочих дней с момента оформления протокола Комиссии о проведении внеплановой проверки.

2.8. При проведении проверок условий обработки ПД должен быть полностью, объективно и всесторонне исследован порядок обработки ПД и его соответствие требованиям обработки ПД, установленным в МДОУ, а именно:

– порядок и условия применения организационных и технических мер по обеспечению безопасности ПД при их обработке, необходимых для выполнения требований к защите ПД, исполнение которых обеспечивает установленные уровни защищенности ПД;

– порядок и условия применения средств защиты информации эффективность принимаемых мер по обеспечению безопасности ПД до ввода в эксплуатацию информационной системы ПД;

– состояние учета машинных носителей ПД; соблюдение правил доступа к ПД; наличие (отсутствие) фактов несанкционированного доступа к ПД и принятие необходимых мер;

– мероприятия по восстановлению ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– осуществление мероприятий по обеспечению целостности ПД.

2.9. В случае выявления фактов:

– несоблюдения установленного порядка обработки ПД;

– несоблюдения условий хранения носителей ПД;

– использования средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/целостность/доступность) ПД или другим нарушениям, приводящим к снижению уровня защищенности ПД;

– нарушения заданного уровня безопасности ПД (конфиденциальность/целостность/доступность);

– в обязательном порядке устанавливаются причины нарушения обработки ПД и наличие (отсутствие) вины.

2.10. Комиссия имеет право:

– запрашивать у сотрудников МДОУ информацию, необходимую для реализации полномочий;

– требовать от уполномоченных на обработку ПД лиц уточнения, блокирования или уничтожения недостоверных, или полученных незаконным путем ПД;

– принимать меры по приостановлению или прекращению обработки ПД, осуществляемой с нарушением требований законодательства Российской Федерации;

– вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности ПД при их обработке;

– вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки ПД.

2.11. В процессе проведения внутреннего контроля (проверок) соответствия обработки ПД требованиям к защите ПД разрабатываются меры, направленные на предотвращение негативных последствий выявленных нарушений.

2.12. В случаях выявления нарушений обработки ПД, требующих немедленного устранения, принимаются меры оперативного реагирования.

2.13. Плановая проверка должна быть завершена не позднее чем через месяц со дня её назначения. Заключение о результатах проведенной проверки и принятых по устранению выявленных нарушений мерах, а также мерах, необходимых для устранения нарушений.

2.14. Устранение выявленных нарушений проводится не позднее 30 дней с момента завершения проверки.

2.15. В отношении ПД, ставших известными Комиссии в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность ПД.

Приложение № 7
к приказу МДОУ «Детский сад «Ёлочка»
г. Надыма»
от 15.08.2017 № 157

ПОЛОЖЕНИЕ
о порядке выявления и реагирования на инциденты информационной безопасности в МДОУ «Детский сад «Ёлочка» г. Надыма»

1. Общие положения

1.1. Настоящее Положение устанавливает порядок управления инцидентами (одним событием или группой событий), способными привести к сбоям или нарушению функционирования информационной системы персональных данных МДОУ «Детский сад «Ёлочка» г. Надыма» (далее – МДОУ) и (или) возникновению угроз безопасности конфиденциальной информации МДОУ (далее – инциденты ИБ), а также регулирует порядок проведения служебного расследования нарушений режима служебной тайны (далее – служебное расследование) в МДОУ.

1.2. Настоящее Положение распространяется на работников МДОУ (далее – сотрудники).

1.3. Процесс управления инцидентами ИБ включает:

- учет и регистрацию инцидентов ИБ;
- оповещение ответственного лица о возникновении инцидентов ИБ;
- расследование обнаруженных инцидентов ИБ;
- устранение причин и последствий инцидентов ИБ;
- определение плана корректирующих и превентивных мероприятий.

1.4. Требования настоящего Положения являются обязательными для выполнения всеми сотрудниками МДОУ.

2. Учет и регистрация инцидентов информационной безопасности

2.1. Для выявления инцидентов ИБ должны использоваться встроенные механизмы регистрации и учета событий безопасности операционных систем, систем управления базами данных, прикладного программного обеспечения и средств защиты информации, а также специализированные средства анализа защищенности информационных систем МДОУ.

2.2. В обязательном порядке должны регистрироваться следующие события безопасности:

- попытки входа (выхода) пользователей в операционную систему (из операционной системы);
- загрузка и инициализация операционной системы рабочих станций и серверов;
- попытка доступа к средствам виртуализации;
- факт изменения конфигурации средств виртуализации;
- запуск и остановка служб (системных сервисов) средств виртуализации;
- попытки подключения к рабочим станциям и серверам мобильных устройств и внешних носителей информации.

2.3. В параметрах регистрации событий безопасности в обязательном порядке должны указываться следующие параметры:

- тип события;
- дата и время события;
- результат события;
- источник события;

– идентификатор пользователя информационной системы, предъявленный при попытке доступа.

2.4. Хранение информации об инцидентах ИБ должно осуществляться в течение срока, достаточного для проведения служебного расследования.

2.5. Учет инцидентов ИБ осуществляется администратором безопасности информации (далее– АБИ), назначенным приказом МДОУ. Допускается ведение учета инцидентов ИБ в электронном виде.

2.6. При обнаружении инцидента ИБ АБИ проводит его классификацию в соответствии с Приложением к настоящему Положению. Инциденты ИБ и их последствия классифицируются по значимости на текущие, значимые и имеющие признаки преступления.

3. Порядок оповещения ответственного лица о возникновении инцидентов информационной безопасности

3.1. Средства защиты информации должны обеспечивать возможность информирования администратора безопасности информации о критических событиях безопасности в информационной системе по электронной почте или посредством смс.

3.2. В случае если зафиксированный инцидент ИБ был классифицирован как «значимый» или «имеющий признаки компьютерного преступления», АБИ обязан незамедлительно сообщить о выявленном инциденте ИБ ответственному по защите информации по электронной почте или иному средству связи.

3.3. Ответственный по защите информации должен провести внеплановый анализ выявленного инцидента ИБ и, в случае необходимости, инициировать процедуру служебного расследования в соответствии с порядком, установленным данным Положением.

4. Порядок расследования обнаруженных инцидентов информационной безопасности

4.1. Проведение служебного расследования инициируется ответственным за организацию обработки персональных данных МДОУ и осуществляется комиссией по защите персональных данных в МДОУ (далее – Комиссия).

4.2. Служебное расследование может быть возбуждено по:

– решению заведующего МДОУ;

– инициативе любого сотрудника МДОУ на основании служебной записки в произвольной форме на имя ответственного за организацию обработки персональных данных МДОУ;

– устному докладу ответственного по защите информации.

4.3. В состав Комиссии входят следующие сотрудники МДОУ:

4.3.1. в обязательном порядке:

– Председателя Комиссии – ответственного за организацию обработки персональных данных МДОУ;

– Заместителя председателя Комиссии;

– Секретаря Комиссии;

– Членов Комиссии;

– Ответственного по защите информации;

– Администратора безопасности информации;

4.3.2. в случае необходимости Комиссия вправе привлекать к расследованию:

– непосредственного руководителя сотрудника, в отношении которого проводится служебное расследование;

– экспертов из структурных подразделений Департамента образования Надымского района и, при необходимости, представителей сторонних организаций.

4.4. Комиссия для проведения служебного расследования в рабочем порядке в максимально короткие сроки, привлекая все необходимые ресурсы, проводит служебное

расследование.

4.5. Результаты работы Комиссии оформляются в виде аналитического экспертного заключения – протокола Комиссии на заведующего МДОУ, с предложениями:

– по внесению изменений в организационные и (или) технические меры по защите информации;

– по внесению изменений и улучшений в комплект организационно-распорядительной документации по защите персональных данных МДОУ;

– по расширению или дополнению списка инцидентов ИБ, установленного данным Положением, если это необходимо.

4.6. В аналитическом экспертном заключении должен быть приведен перечень ответственных за выполнение запланированных работ и сроки выполнения запланированных работ.

4.7. Материалы служебного расследования, его выводы и заключения могут быть использованы как основание для реализации уголовной, гражданской, административной или дисциплинарной ответственности, в порядке, определяемом действующим законодательством и локальными правовыми актами МДОУ.

5. Ответственность

5.1. Ответственность за проведение служебного расследования и за контроль своевременного и качественного выполнения работ по проведению корректирующих и превентивных мероприятий несет ответственный по защите информации.

5.2. Ответственность за обеспечение своевременной регистрации инцидентов ИБ несет администратор безопасности информации.

Приложение
к Положению о порядке выявления и реагирования на инциденты информационной безопасности в МДОУ «Детский сад «Ёлочка» г. Надыма»

Перечень
инцидентов информационной безопасности

№ п/п	Описание инцидента информационной безопасности
1	2
1. Текущие нарушения	
1.1	Ошибка при регистрации в информационной системе: ввод неправильных персональных регистрационных данных (пароля, имени пользователя и т.п.) более трех раз подряд (однократная)
1.2	Периодические попытки неудачного доступа к объектам: компьютерам, принтерам, файлам, документам
1.3	Несанкционированный перевод времени на рабочей станции либо на других элементах информационной инфраструктуры МДОУ
1.4	Выполнение производственных обязанностей с использованием компьютерного оборудования в нерабочее время
1.5	Оставление работающего (включенного) компьютерного оборудования без запущенного хранителя экрана в нерабочее время
1.6	Перезагрузка рабочей станции при сбоях в работе (однократная), в том числе аварийная перезагрузка путем нажатия кнопки горячей перезагрузки или полного отключения питания
1.7	Нецелевое использование элементов информационной инфраструктуры МДОУ (печать, сервисы сети Интернет, электронная почта, и т.п.)
2. Значимые нарушения	
2.1	Ошибка при регистрации в информационной системе: ввод неправильных персональных регистрационных данных (пароля, имени пользователя и т.п.) более трех раз подряд (многократная)
2.2	Неоднократное оставление работающего (включенного) компьютерного оборудования без запущенного хранителя экрана в нерабочее время
2.3	Утрата учтенного магнитного, оптического или иного носителя конфиденциальной информации
2.4	Утрата носителя информации с резервной копией
2.5	Неудачная попытка регистрации в информационной системе под чужими регистрационными данными (именем пользователя, паролем и т.п.) (многократная)
2.6	Удачная попытка регистрации в информационной системе под чужими регистрационными данными (именем пользователя, паролем и т.п.)
2.7	Нерегламентированная очистка журналов событий безопасности информационных систем МДОУ
2.8	Нерегламентированное подключение неучтенных внутренних и (или) периферийных устройств и носителей информации

2.9	Нерегламентированное изменение аппаратной конфигурации компьютерного оборудования
2.10	Нерегламентированное копирование информации (файлов) на флеш-накопители или иные внешние носители информации, а также нерегламентированная передача подобной информации с использованием сервисов электронной почты и других сервисов сети Интернет
2.11	Нерегламентированная установка (удаление) прикладного программного обеспечения, не разрешенного к использованию на рабочих станциях и серверах МДОУ
2.12	Попытка получения привилегированного доступа к рабочей станции или к другим ресурсам информационных систем МДОУ (повышение уровня прав доступа, получение прав на отладку программ и т.п.)
2.13	Заражение программного обеспечения рабочих станций и серверов вредоносным кодом (непреднамеренное)
2.14	Нерегламентированное использование сканирующего (на различные уязвимости) программного обеспечения
2.15	Нерегламентированное использование анализаторов протоколов (снифферов)
2.16	Нерегламентированный просмотр, вывод на печать, передача третьим лицам сведений, содержащих конфиденциальные данные (информацию, подлежащую защите)
2.17	Несанкционированное проведение обновления версий системного и прикладного программного обеспечения
3. Нарушения, имеющие признаки преступления	
3.1	Несанкционированное получение привилегированного доступа к любым элементам информационной инфраструктуры МДОУ
3.2	Несанкционированное изменение конфигурации элементов информационной инфраструктуры МДОУ
3.3	Утрата резервных копий
3.4	Утечка конфиденциальной информации (баз данных информационных систем и др.)
3.5	Подозрение в умышленном нарушении работоспособности информационной сети МДОУ, элементов информационной инфраструктуры МДОУ, системного и прикладного программного обеспечения
3.6	Юридически не обоснованная передача (распространение) конфиденциальной информации
3.7	Несанкционированное внесение изменений в базы данных информационных систем МДОУ
3.8	Несанкционированное уничтожение конфиденциальной информации
3.9	Проведение обновления версии информационных систем МДОУ (равно как и другого программного обеспечения), повлекшее за собой потерю конфиденциальной информации
3.10	Намеренное заражение информационных систем МДОУ вредоносным кодом

Приложение № 8
к приказу МДОУ «Детский сад
«Ёлочка» г. Надыма»
от 15.08.2017 № 157

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных
в МДОУ «Детский сад «Ёлочка» г. Надыма»

1. Общие положения

1.1. Настоящая Инструкция определяет основные обязанности и права лица, ответственного за организацию обработки, хранения, использования и защиты персональных данных в МДОУ «Детский сад «Ёлочка» г. Надыма» (далее – МДОУ).

1.2. Ответственный за организацию обработки персональных данных в МДОУ специалист по кадрам назначается приказом заведующего МДОУ.

1.3. Ответственный за организацию обработки персональных данных в МДОУ (далее - Ответственный) подчиняется заведующему МДОУ, в части вопросов, касающихся обработки и обеспечения безопасности персональных данных в МДОУ, ему подчиняются все остальные ответственные лица.

1.4. Ответственный отвечает за организацию и состояние процесса обработки персональных данных в МДОУ.

1.5. Ответственный осуществляет руководство должностными лицами МДОУ по вопросам организации обработки и обеспечения безопасности персональных данных.

1.6. Все работники МДОУ (далее – сотрудники) обязаны выполнять требования Ответственного за организацию обработки персональных данных в части вопросов, касающихся обработки и обеспечения безопасности персональных данных в МДОУ.

1.7. Ответственный за организацию обработки персональных данных в МДОУ отвечает за качество проводимых им работ по контролю действий при работе в информационной системе персональных данных (далее – ИСПД), состояние и поддержание установленного уровня защищенности персональных данных при их обработке в ИСПД.

2. Обязанности ответственного за организацию обработки персональных данных

2.1. Обеспечивать выполнение режимных и организационных мероприятий на месте эксплуатации информационной системы, а также следить за выполнением требований по условиям размещения средств вычислительной техники и их сохранностью.

2.2. Знать и представлять администратору безопасности информации изменения к списку лиц, доступ которых к информации ограниченного доступа необходим для выполнения трудовых обязанностей.

2.3. Проводить инструктаж и консультации пользователей информационной системы по соблюдению режима конфиденциальности.

2.4. Участвовать в определении полномочий пользователей информационной системы (оформлении разрешительной системы доступа), минимально необходимых им для выполнения трудовых обязанностей.

2.5. Организовывать периодический контроль за пользователями по соблюдению ими режима конфиденциальности, правил работы со съемными машинными носителями информации, выполнению организационных мер по защите информации, а также принимать участие в проведении проверок уполномоченными структурами.

2.6. Взаимодействовать с администратором безопасности информации по вопросам

обеспечения и выполнения требований обработки персональных данных.

2.7. Контролировать осуществление мероприятий по установке и настройке средств защиты.

2.8. Организовывать работы по плановому контролю работоспособности технических средств защиты информации, охраны объекта, средств защиты информации от несанкционированного доступа.

2.9. Контролировать периодическое резервное копирование баз данных и сопутствующей защищаемой информации.

2.10. По указанию руководства своевременно и точно отражать изменения в локальных актах по управлению средствами защиты информации в информационной системе и по правилам обработки информации ограниченного доступа.

2.11. Знать перечень и условия обработки персональных данных.

2.12. Знать перечень установленных в подразделении технических средств, входящих в состав информационной системы, и перечень задач, решаемых с их использованием.

2.13. Обеспечивать соблюдение сотрудниками утвержденного порядка проведения работ по установке и модернизации аппаратных и программных средств компьютеров и серверов из состава информационной системы.

2.14. При выявлении возможных каналов неправомерного вмешательства в процесс функционирования информационной системы и осуществления несанкционированного доступа к защищаемой информации и техническим средствам из состава информационной системы подразделения, сообщать о них руководителю.

2.15. Инструктировать сотрудников по вопросам обеспечения информационной безопасности и правилам работы с применяемыми средствами защиты информации.

2.16. Знать законодательство РФ о персональных данных, следить за его изменениями.

2.17. Проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей защищаемой информации, нарушения правил работы с документами, содержащими персональные данные, или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

2.18. Выполнять иные мероприятия, требуемые нормативными документами по защите информации.

3. Права ответственного за организацию обработки персональных данных

3.1. Требовать от всех пользователей информационных систем персональных данных выполнения установленной технологии обработки персональных данных, инструкций и других нормативных правовых документов по обеспечению безопасности персональных данных.

3.2. Инициировать блокирование доступа сотрудников к персональным данным, если это необходимо для предотвращения нарушения режима защиты персональных данных.

3.3. Участвовать в разработке мероприятий по совершенствованию системы защиты персональных данных.

3.4. Инициировать проведение служебных проверок по фактам нарушения установленных требований обеспечения информационной безопасности, несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, несанкционированного доступа, утраты, порчи защищаемых носителей персональных данных и технических средств из состава информационных систем или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

3.5. Обращаться с предложением о приостановке процесса обработки персональных данных или отстранению от работы пользователя в случаях нарушения установленной технологии обработки персональных данных или нарушения режима конфиденциальности.

3.6. Подавать свои предложения по совершенствованию мер защиты персональных данных в ИСПД, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищенности персональных

данных.

4. Действия при обнаружении попыток несанкционированного доступа

4.1. К попыткам несанкционированного доступа относятся:

– сеансы работы с персональными данными незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истек, или превышающих свои полномочия по доступу к данным;

– действия постороннего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПД, при использовании учетной записи администратора или другого пользователя ИСПД, методом подбора пароля, использования пароля, разглашенного владельцем учетной записи или любым другим методом.

4.2. При выявлении факта несанкционированного доступа Ответственный обязан:

– по возможности пресечь дальнейший несанкционированный доступ к персональным данным;

– доложить служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

– известить непосредственного руководителя пользователя, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа.

5. Ответственность

5.1. Ответственный несет персональную ответственность за:

5.1.1. соблюдение требований настоящей Инструкции,

5.1.2. правильность и объективность принимаемых решений,

5.1.3. качество и своевременность проводимых им работ по обеспечению безопасности персональных данных,

5.1.4. Ответственный при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несет дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение № 9
к приказу МДОУ «Детский сад
«Ёлочка» г. Надыма»
от 15.08.2017 № 157

ИНСТРУКЦИЯ
ответственного за обеспечение безопасности персональных данных в МДОУ «Детский сад «Ёлочка» г. Надыма»

1. Общие положения

1.1. Настоящая Инструкция определяет основные обязанности, права ответственного лица за обеспечение безопасности персональных данных в МДОУ «Детский сад «Ёлочка» г. Надыма» (далее – МДОУ).
1.2. Ответственный за обеспечение безопасности персональных данных (далее – Ответственный) назначается приказом МДОУ из числа сотрудников, чья деятельность связана с персональными данными.
1.3. Ответственный за обеспечение безопасности персональных данных в МДОУ подчиняется ответственному за организацию обработки персональных данных в МДОУ, в части вопросов, касающихся обработки и обеспечения безопасности персональных данных в МДОУ, ему подчиняются администраторы безопасности информации (далее-АБИ) МДОУ.
1.4. Ответственный осуществляет методическое руководство АБИ, работниками (далее – сотрудники), имеющих санкционированный доступ к персональным данным, в вопросах обеспечения безопасности персональных данных.
1.5. Все сотрудники обязаны выполнять требования Ответственного за обеспечение безопасности персональных данных в части вопросов, касающихся обеспечения безопасности персональных данных в МДОУ.
1.6. Ответственный за обеспечение безопасности персональных данных в своей работе руководствуется настоящей Инструкцией, руководящими и нормативными документами ФСТЭК России и муниципальными правовыми актами.
1.7. Ответственный за обеспечение безопасности персональных данных отвечает за качество проводимых им работ по контролю за действиями при работе в информационной системе персональных данных (далее – ИСПД), состояние и поддержание установленного уровня защиты ИСПД.

2. Обязанности Ответственного за обеспечение безопасности персональных данных

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, регламентирующих порядок действий по организации обработки персональных данных.
2.2. Ознакомлять под подпись сотрудников, имеющих доступ к персональным данным, с организационно-распорядительными документами обеспечения безопасности персональных данных Департамента образования, и требовать их исполнения.
2.3. Проводить инструктаж и консультации пользователей информационной системы персональных данных по соблюдению режима конфиденциальности.
2.4. Контролировать физическую сохранность средств и оборудования информационной системы персональных данных МДОУ.
2.5. Организовывать периодический контроль пользователей по соблюдению ими режима конфиденциальности, правил работы со съемными машинными носителями информации, выполнению организационных мер по защите информации, а также принимать участие в проведении проверок уполномоченными структурами.

2.6. Взаимодействовать с администратором безопасности по вопросам обеспечения и выполнения требований обработки персональных данных.

2.7. Организовывать работы по плановому контролю работоспособности технических средств защиты персональных данных, охраны объекта, средств защиты информации от несанкционированного доступа.

2.8. Контролировать периодическое резервное копирование баз персональных данных и сопутствующей защищаемой информации.

2.9. По указанию руководства своевременно и точно отражать изменения в локальных нормативно-правовых актах по управлению средствами защиты информации в ИСПД и по правилам обработки персональных данных.

2.10. Знать перечень и условия обработки персональных данных в МДОУ.

2.11. Знать перечень установленных в МДОУ технических средств, входящих в состав информационных систем, и перечень задач, решаемых с их использованием.

2.12. Обеспечивать соблюдение сотрудниками утвержденного порядка проведения работ по установке и модернизации аппаратных и программных средств компьютеров и серверов из состава информационных систем.

2.13. Осуществлять контроль за порядком учета, создания, хранения и использования машинных (выходных) документов, содержащих персональные данные.

2.14. При выявлении возможных каналов неправомерного вмешательства в процесс функционирования информационных систем и осуществления несанкционированного доступа к персональным данным и техническим средствам из состава информационных систем подразделения, сообщать непосредственному руководителю.

2.15. Инструктировать сотрудников по вопросам обеспечения информационной безопасности и правилам работы с применяемыми средствами зашиты информации.

2.16. Знать законодательство РФ о персональных данных, следить за его изменениями.

2.17. Проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

2.18. Выполнять иные мероприятия, требуемые нормативными документами по защите персональных данных.

3. Права ответственного за обеспечение безопасности персональных данных

3.1. Требовать от всех пользователей информационных систем персональных данных подразделения выполнения установленной технологии обработки персональных данных, инструкций и других нормативных правовых документов по обеспечению безопасности персональных данных.

3.2. Инициировать блокирование доступа сотрудников к персональным данным, если это необходимо для предотвращения нарушения режима защиты персональных данных.

3.3. Участвовать в разработке мероприятий по совершенствованию системы защиты персональных данных.

3.4. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, несанкционированного доступа, утраты, порчи защищаемых носителей персональных данных и технических средств из состава информационных систем или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

3.5. Обращаться с предложением о приостановке процесса обработки персональных данных или отстранении от работы пользователя в случаях нарушения установленной технологии обработки персональных данных или нарушения режима конфиденциальности.

3.6. Подавать свои предложения по совершенствованию мер защиты персональных данных в ИСПД, разработке и принятии мер по предотвращению возможных опасных

последствий нарушений, приводящих к снижению уровня защищенности персональных данных.

4. Действия при обнаружении попыток несанкционированного доступа

4.1. К попыткам несанкционированного доступа относятся:

4.1.1. сеансы работы с персональными данными незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истек, или превышающих свои полномочия по доступу к данным;

4.1.2. действия постороннего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПД, при использовании учетной записи администратора или другого пользователя ИСПД, методом подбора пароля, использования пароля, разглашенного владельцем учетной записи или любым другим методом.

4.2. При выявлении факта несанкционированного доступа Ответственный обязан:

4.2.1. по возможности пресечь дальнейший несанкционированный доступ к персональным данным;

4.2.2. доложить в служебной записке о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

4.2.3. известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа;

4.2.4. известить ответственного за организацию обработки персональных данных и администратора безопасности о факте несанкционированного доступа.

5. Ответственность

5.1. Ответственный несет персональную ответственность за:

5.1.1. соблюдение требований настоящей Инструкции;

5.1.2. правильность и объективность принимаемых решений;

5.1.3. качество и своевременность проводимых им работ по обеспечению безопасности персональных данных.

5.2. Ответственный при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несет дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение № 10
к приказу МДОУ «Детский сад «Ёлочка»
г. Надыма»
от 15.08.2017 № 157

ИНСТРУКЦИЯ
администратора безопасности информационных систем персональных данных МДОУ «Детский сад «Ёлочка» г. Надыма»

1. Общие положения

1.1. Настоящий документ разработан в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также другими нормативными правовыми актами по защите информации, и определяет порядок обеспечения безопасности информации при проведении работ администратором безопасности информации (далее – АБИ) в информационных системах персональных данных МДОУ «Детский сад «Ёлочка» г. Надыма» (далее – ИСПД, МДОУ).

1.2. Субъектами доступа к ресурсам ИСПД являются пользователи, сотрудники, осуществляющие техническое обслуживание, ремонт, в соответствии с утвержденным перечнем.

1.3. Обрабатываемая в ИСПД информация относится к сведениям, составляющим персональные данные.

1.4. Машинные носители с защищаемой информацией имеют пометку «персональные данные» (далее– ПД).

1.5. АБИ назначается приказом МДОУ и получает неограниченные права на доступ к ресурсам ИСПД.

1.6. АБИ осуществляет общее руководство и контроль за обеспечением безопасности информации при работе пользователей ИСПД и обслуживающего персонала.

1.7. Методическое руководство по информационной безопасности объектов информатизации осуществляет АБИ.

1.8. АБИ имеет право вносить предложения по изменению и дополнению комплекта организационно-распорядительной документации по защите персональных данных.

1.9. Изменения и дополнения к данной Инструкции утверждаются в установленном порядке.

2. Обязанности администратора безопасности информации

2.1. АБИ обязан знать и выполнять требования комплекта организационно-распорядительной документации по защите персональных данных.

2.2. АБИ, не ознакомленный с данной Инструкцией, а также с изменениями и дополнениями к ней, к работе с ресурсами ИСПД не допускается.

2.3. АБИ осуществляет учет съемных машинных носителей информации, их уничтожение, либо контроль процедуры их уничтожения.

2.4. АБИ обязан немедленно реагировать на сообщения пользователей о любых неисправностях в работе основных и вспомогательных средств и систем (далее – ОТСС и ВТСС), средств защиты информации (далее – СЗИ), системного и прикладного

программного обеспечения (далее – ПО) ИСПД.

2.5. АБИ обязан немедленно ставить в известность ответственного по защите информации Администрации обо всех неисправностях аппаратно-программных средств ИСПД.

2.6. АБИ обязан ставить в известность ответственного по защите информации Департамента образования о необходимости проведения работ по администрированию СЗИ.

2.7. АБИ имеет право проводить внеплановые проверки работоспособности СЗИ и соблюдения пользователями технологии обработки персональных данных.

2.8. АБИ разрабатывает планы мероприятий по администрированию и техническому обслуживанию аппаратных и программных средств ИСПД МДОУ.

2.9. АБИ обязан в случае отказа технических средств или программного обеспечения элементов ИСПД, в том числе СЗИ, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.10. АБИ имеет право требовать прекращения обработки персональных данных как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПД или СЗИ.

2.11. АБИ присутствует при выполнении технического обслуживания элементов ИСПД сторонними специалистами на территории МДОУ.

2.12. АБИ осуществляет разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами ИСПД, в том числе с СЗИ, или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

2.13. В ходе управления (администрирования) системой защиты ИСПД АБИ обязан осуществлять:

– заведение и удаление учетных записей пользователей, управление полномочиями пользователей ИСПД и поддержание правил разграничения доступа в ИСПД;

– управление СЗИ в ИСПД, в том числе параметрами настройки программного обеспечения, включая программное обеспечение СЗИ, управление учетными записями пользователей, восстановление работоспособности СЗИ, генерацию, смену и восстановление паролей;

– изменение аутентификационной информации (средств аутентификации), заданной их производителями и (или) используемой при внедрении системы защиты информации ИСПД;

– установку обновлений программного обеспечения, включая программное обеспечение СЗИ, выпускаемых разработчиками (производителями) СЗИ или по их поручению;

– централизованное управление системой защиты информации ИСПД (при необходимости);

– регистрацию и анализ событий в ИСПД, связанных с защитой информации;

– информирование пользователей об угрозах безопасности информации, о правилах эксплуатации системы защиты информации ИСПД и отдельных СЗИ, а также их обучение;

– сопровождение функционирования системы защиты информации ИСПД в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее и организационно–распорядительных документов по защите информации.

2.14. В ходе выявления инцидентов и реагирования на них АБИ обязан осуществлять:

– обнаружение и идентификацию инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и СЗИ, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к

возникновению инцидентов;

– своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в ИСПД;

– анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

– планирование и принятие мер по устранению инцидентов, в том числе по восстановлению ИСПД и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

– планирование и принятие мер по предотвращению повторного возникновения инцидентов.

2.15. В ходе контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИСПД, АБИ обязан осуществлять:

– анализ и оценку функционирования системы защиты информации ИСПД, включая выявление, анализ и устранение недостатков в функционировании системы защиты информации ИСПД;

– проверку работоспособности и параметров настройки программного обеспечения, аппаратных и программных СЗИ ИСПД;

– проверку состава технических средств, программного обеспечения и СЗИ;

– контроль целостности печатей (пломб, наклеек) технических средств, используемых для обработки персональных данных;

– еженедельное отслеживание появления новых видов уязвимостей ПО ИСПД. По необходимости АБИ производит устранение уязвимостей согласно рекомендациям разработчика;

– периодический анализ изменения угроз безопасности информации в ИСПД, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;

– контроль за событиями безопасности и действиями пользователей в ИСПД. В частности, АБИ обязан осуществлять постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации;

– контроль (анализ) защищенности информации, содержащейся в ИСПД;

– документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИСПД;

– принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) системы защиты информации ИСПД, повторной аттестации ИСПД или проведении дополнительных аттестационных испытаний.

3. Доступ к ресурсам ИСПД

3.1. Обязательными условиями получения доступа к ресурсам ИСПД являются:

– право доступа в помещение;

– наличие допуска к персональным данным;

– право доступа к ИСПД;

– знание технологии обработки информации в ИСПД с учетом требований информационной безопасности.

3.2. Идентификация АБИ в ИСПД осуществляется по уникальному имени и персональному идентификатору (при его наличии).

3.3. Длина пароля АБИ и всех пользователей – не менее 8 буквенно-цифровых символов.

3.4. Уникальное имя, персональный идентификатор (при его наличии) и пароль АБИ получает в установленном порядке. АБИ обязан их помнить и не допускать раскрытия, не допускается запись на каких-либо носителях в целях напоминания. Во время ввода пароля на клавиатуре должна быть исключена возможность его просмотра другими лицами. Не допускается оставление без присмотра и передача другим лицам персонального идентификатора (при его наличии).

3.5. При утере или подозрении на утечку своего имени, пароля или персонального идентификатора АБИ должен немедленно изменить свои идентификационные данные и проконтролировать возможные изменения в настройках СЗИ.

3.6. Регистрация пользователя осуществляется АБИ в соответствии с Инструкцией по организации парольной защиты и состоит в определении имени регистрируемого пользователя, присвоении ему персонального идентификатора (при его наличии) и назначении пароля.

3.7. При заведении новой учетной записи АБИ должен проверить личность пользователя и его должностные обязанности.

3.8. Предоставление пользователям прав доступа к объектам доступа ИСПД должно осуществляться на основании задач, решаемых пользователями.

3.9. АБИ не имеет права требовать у пользователей раскрытия их паролей, а также передачи ему персональных идентификаторов (при их наличии), кроме случая изменения идентификационных данных.

3.10. АБИ имеет право требовать у пользователя изменения его пароля, но не имеет права самостоятельно изменять его пароль.

4. Порядок работы с ресурсами ИСПД

4.1. Проверка работоспособности и настройка системы доступа.

АБИ присваивает пользователям идентификационные данные к ресурсам ИСПД. При этом должны выполняться следующие требования:

– АБИ определяет политику изменения учетных данных пользователей и периодически контролирует ее соблюдение;

– АБИ сообщает пользователю его уникальное имя и предоставляет возможность задать пароль, далее кодирует персональный идентификатор (при его наличии) пользователя;

– изменение учетных данных пользователя производится АБИ по указанию ответственного за обеспечение безопасности персональных данных МДОУ, а также периодически по утвержденному плану и в случае увольнения сотрудника.

4.2. Проверка работоспособности и настройка аппаратных и программных средств защиты информации (СЗИ).

АБИ обязан перед началом работ включить и убедиться в работоспособности аппаратных СЗИ, в случае сбоя– работы прекратить.

В случае сбоя СЗИ, таких, как неправильная идентификация пользователей, АБИ обязан приостановить обработку защищаемой информации до устранения неисправности. В случае производственной необходимости– отключить СЗИ и лично контролировать проведение работ пользователями.

4.3. Антивирусная защита ресурсов ИСПД

АБИ разрабатывает и контролирует реализацию антивирусной политики, а именно:

– настраивает параметры антивирусной программы;

– контролирует работоспособность антивирусной программы;

– немедленно реагирует на сообщения пользователей о подозрительном поведении ПО, а также о появлении любых сообщений антивирусной программы и принимает соответствующие меры;

– имеет право на проведение внеплановой проверки на наличие вирусов;

– периодически (один раз в неделю) контролирует корректность процесса

обновления антивирусных баз, а также исполняемых модулей антивирусной программы.

4.4. Хранение дистрибутивов программного обеспечения СЗИ.

АБИ должен хранить дистрибутивы программного обеспечения СЗИ и прикладного программного обеспечения, установленного в ИСПД МДОУ в месте, исключающем доступ посторонних лиц.

4.5. Проверка целостности системного и прикладного ПО.

Контролю целостности подлежат файлы программного обеспечения ИСПД с расширениями: *.exe, *.com, * .dll, *.sys, *.vxd,*.drv.

4.6. Резервное копирование и восстановление информации.

Резервное копирование производится регулярно с заданной периодичностью, а также в случае производственной необходимости. При этом необходимо выполнять следующие требования:

– обязательное резервное копирование производится в случае обнаружения неисправностей в работе ПЭВМ или отчуждаемых машинных носителей информации (далее – МНИ);

– допускается обоснованное внеплановое резервное копирование информации как по инициативе пользователя, так и АБИ, если это не нарушает технологию обработки информации;

– резервные копии пользовательской информации и информации операционной системы хранятся на учтенных внешних МНИ;

– ответственным лицом за хранение резервных копий является АБИ.

По мере устранения неисправностей ПЭВМ АБИ производит восстановление информации ограниченного доступа с резервных копий.

АБИ разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования информационной системы в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

4.7. Конфигурирование ИСПД.

Конфигурационной единицей являются услуги, оборудование, программное обеспечение, здания, люди, документы и пр.

Управление изменениями конфигурации осуществляет ответственный по защите информации. Планирование реализации и непосредственно реализация необходимых изменений возлагается на АБИ.

В ходе управления конфигурацией аттестованной информационной системы и ее системы защиты информации АБИ обязан осуществлять:

– поддержание конфигурации ИСПД и ее системы защиты информации (структуры системы защиты информации ИСПД, состава, мест установки и параметров настройки СЗИ, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на систему защиты информации (поддержание базовой конфигурации ИСПД и ее системы защиты информации);

– управление изменениями базовой конфигурации ИСПД и ее системы защиты информации, в том числе определение типов возможных изменений базовой конфигурации ИСПД и ее системы защиты информации, санкционирование внесения изменений в базовую конфигурацию ИСПД и ее системы защиты информации, документирование действий по внесению изменений в базовую конфигурацию ИСПД и ее системы защиты информации, сохранение данных об изменениях базовой конфигурации ИСПД и ее системы защиты информации, контроль действий по внесению изменений в базовую конфигурацию ИСПД и ее системы защиты информации;

– анализ потенциального воздействия планируемых изменений в базовой конфигурации ИСПД и ее системы защиты информации на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность ИСПД;

– определение параметров настройки программного обеспечения, включая

программное обеспечение СЗИ, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию ИСПД и ее системы защиты информации;

– внесение информации (данных) об изменениях в базовой конфигурации ИСПД и ее системы защиты информации в документацию на систему защиты информации ИСПД;

– принятие решения по результатам управления конфигурацией о повторной аттестации ИСПД или проведении дополнительных аттестационных испытаний.

Обязанности по управлению изменениями в аппаратном и программном обеспечении и всех элементах документации, которые связаны с работой, поддержкой и сопровождением систем, находящихся в эксплуатации, возлагаются на АБИ. При возникновении необходимости изменения конфигурации ИСПД, аттестованной по требованиям безопасности информации, АБИ согласовывает планируемые изменения с предприятием-лицензиатом, проводившим аттестационные испытания.

4.8. Вывод ресурсов ИСПД из эксплуатации.

При невозможности ремонта различных ресурсов ИСПД АБИ обязан:

– физически уничтожать любые МНИ, независимо от содержащейся на них информации; картриджи принтера, иные комплектующие могут быть использованы за пределами ИСПД;

– факт выхода из строя и замены оборудования должен быть отражен в Техническом паспорте на ИСПД.

4.9. Реагирование на сбои при регистрации событий безопасности.

Реагирование на сбои при регистрации событий безопасности осуществляется АБИ путем изменения параметров сбора, записи и хранения информации о событиях безопасности в журналах СЗИ от НСД, в том числе отключение записи информации о событиях безопасности от части компонентов ИСПД, запись поверх устаревших хранимых записей событий безопасности.

В случае выявления признаков инцидентов безопасности АБИ обязан:

– немедленно доложить ответственному по защите информации о данном факте;

– по возможности в максимально сжатые сроки установить причину возникновения инцидента и исключить возможность его повторения;

– восстановить работоспособность ИСПД;

– по окончании работ по восстановлению работоспособности ИСПД произвести запись в Журнал регистрации событий информационной безопасности и мер, принятых для устранения попыток несанкционированного системного доступа по форме согласно приложению, к настоящей Инструкции.

5. Действия при обнаружении попыток несанкционированного доступа

5.1. К попыткам несанкционированного доступа относятся:

– сеансы работы с ИСПД незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истек, или превышающих свои полномочия по доступу к данным;

– действия постороннего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПД, при использовании учетной записи администратора или другого пользователя ИСПД, методом подбора пароля, использования пароля, разглашенного владельцем учетной записи или любым другим методом.

5.2. При выявлении факта несанкционированного доступа АБИ обязан:

– пресечь дальнейший несанкционированный доступ к ИСПД;

– доложить ответственному по защите информации МДОУ служебной запиской о факте несанкционированного доступа, его результате (успешный/неуспешный) и предпринятых действиях;

– известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка

несанкционированного доступа, о факте несанкционированного доступа.

6. Ответственность

6.1. АБИ несет персональную ответственность:

– за сохранность носителей информации и содержащейся на них информации в рабочее время;

– за несоблюдение требований данной Инструкции и неправомерное использование ресурсов ИСПД;

– за правильную работу установленных в ИСПД МДОУ средств защиты информации;

– за качество проводимых работ по обеспечению безопасности персональных данных и за все действия, совершенные от имени учетной записи АБИ в ИСПД, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования учетной записи.

6.2. АБИ при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несет дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение № 11
к приказу МДОУ «Детский сад
«Ёлочка» г. Надыма»
от 15.08.2017 № 157

ИНСТРУКЦИЯ
пользователя информационных систем персональных данных
в МДОУ «Детский сад «Ёлочка» г. Надыма»

1. Общие положения

1.1. Настоящая Инструкция разработана в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также другими нормативными документами по безопасности информации, и определяет порядок обеспечения информационной безопасности при проведении работ пользователями информационных систем персональных данных (далее – ИСПД) МДОУ «Детский сад «Ёлочка» г. Надыма» (далее – МДОУ).

1.2. Субъектами доступа к ресурсам ИСПД являются пользователи ИСПД.

1.3. Обрабатываемая в ИСПД информация относится к сведениям, составляющим персональные данные (далее– ПД).

1.4. Машинные носители информации имеют пометку «ПД».

1.5. Пользователи получают свои права на доступ к ресурсам ИСПД от администратора безопасности информации МДОУ (далее – АБИ).

1.6. Изменения и дополнения к данной Инструкции утверждаются в установленном порядке.

2. Обязанности пользователя ИСПД

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

2.2. Выполнять на автоматизированном рабочем месте (далее – АРМ) только те процедуры, которые определены технологическим процессом обработки персональных данных.

2.3. Знать и соблюдать установленные требования к обработке персональных данных, учету и хранению носителей информации, обеспечению безопасности персональных данных, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования парольной политики в соответствии с Инструкцией по организации парольной защиты в информационных системах персональных данных в МДОУ.

2.5. Получать уникальное имя и персональный идентификатор (при его наличии) от АБИ. Пользователь обязан помнить и соблюдать в тайне свои имена и пароли, не допускается их запись на каких-либо носителях в целях напоминания.

2.6. Во время работы располагать экран монитора так, чтобы затруднить посетителям просмотр отображаемой информации.

2.7. При возникновении подозрения на наличие вредоносного программного обеспечения (частые ошибки в работе программ, появление посторонних графических и

звуковых эффектов, искажение данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.) самостоятельно или вместе с АБИ провести внеочередной антивирусный контроль своего АРМ. При самостоятельном проведении антивирусного контроля−уведомить о результатах АБИ для определения им факта наличия или отсутствия вредоносного программного обеспечения.

2.8. В случае появления информационного окна средства антивирусной защиты, сигнализирующего об обнаружении вредоносного программного обеспечения:

2.8.1. приостановить обработку данных;

2.8.2. немедленно поставить в известность о факте обнаружения вредоносного программного обеспечения АБИ владельца зараженных файлов, а также смежные структурные подразделения, использующие эти файлы в работе;

2.8.3. совместно с владельцем файлов, зараженных вредоносным программным обеспечением, провести анализ необходимости дальнейшего их использования;

2.8.4. произвести лечение или уничтожение зараженных файлов (для выполнения требований данного пункта привлечь АБИ).

2.9. Немедленно вызвать АБИ и поставить в известность руководителя структурного подразделения МДОУ при обнаружении:

– фактов совершения в его отсутствие попыток несанкционированного доступа к защищаемой АРМ;

– несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ;

– отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;

– некорректного функционирования установленных на АРМ технических средств защиты;

– непредусмотренных отводов кабелей и подключенных к АРМ дополнительных устройств.

2.10. При утере или подозрении на утечку своего имени, пароля и персональных идентификаторов пользователь должен немедленно сообщить об этом АБИ.

2.11. Обо всех выявленных нарушениях, связанных с информационной безопасностью, а также для получения консультаций по вопросам информационной безопасности, необходимо обратиться к АБИ.

2.12. При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>.

2.13. Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций с целью ликвидации их последствий, в пределах, возложенных на него функций.

2.14. Пользователям запрещается:

– разглашать защищаемую информацию посторонним лицам;

– копировать защищаемую информацию на неучтенные внешние носители;

– самостоятельно устанавливать, тиражировать или модифицировать программное и аппаратное обеспечение, изменять установленный порядок функционирования технических и программных средств;

– подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;

– отключать (блокировать) средства защиты информации;

– выполнять на АРМ работы, не предусмотренные технологическим процессом обработки ПД;

– сообщать (или передавать) посторонним лицам параметры своей учетной записи (имя, персональный идентификатор (при его наличии) и пароль) в ИСПД;

– оставлять без присмотра и передавать другим лицам персональный идентификатор;

– привлекать посторонних лиц для ремонта или настройки АРМ без согласования с ответственным по защите информации;

– оставлять без присмотра свое АРМ, не активизировав блокировку доступа, или оставлять свое АРМ включенным по окончании работы;

– умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению безопасности персональных данных.

3. Порядок работы пользователя с ресурсами ИСПД

3.1. Начало работы на АРМ.

При включении АРМ необходимо дождаться завершения загрузки и готовности системы защиты информации (далее–СЗИ) и операционной системы (далее–ОС) к идентификации пользователя. Идентификация пользователя осуществляется по уникальному имени и паролю с использованием персонального идентификатора, если таковой предусмотрен комплектацией СЗИ. Для получения доступа к ресурсам ИСПД пользователь должен приложить к считывателю персональный идентификатор (при его наличии) и ввести с клавиатуры свой пароль. Если после ввода пароля СЗИ выдаст сообщение об ошибке, пользователь должен обратиться к АБИ.

3.2. Завершение работы на АРМ.

По окончании работы пользователь должен либо завершить штатными средствами сеанс своей работы (без выключения АРМ), либо завершить работу АРМ стандартным способом (при этом выключить АРМ).

3.3. Требования к распечатыванию информации.

Все распечатываемые документы должны быть учтены. Бракованные бумажные носители и черновики документов должны быть уничтожены.

При отсутствии пользователя на рабочем месте либо в присутствии лиц, не имеющих допуска к ресурсам ИСПД, все документы, содержащие ПД, должны быть недоступны для просмотра и иного их использования.

4. Организация парольной защиты

4.1. Личные пароли доступа к элементам ИСПД выдаются пользователям АБИ или создаются самостоятельно.

4.2. Полная плановая смена паролей в ИСПД проводится не реже одного раза в 12 месяцев.

4.3. Правила формирования пароля:

– пароль должен состоять не менее чем из 8 символов;

– в пароле должны присутствовать символы из числа прописных и строчных букв английского алфавита от A до Z; десятичных цифр (от 0 до 9); символы, не принадлежащие алфавитно-цифровому набору (например,!,$,#, %).;

– пароль не должен включать в себя имя пользователя, легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, абвгд и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетания букв и знаков, 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.

4.4. Правила ввода пароля:

– ввод пароля должен осуществляться с учетом регистра, в котором пароль был задан;

– во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами.

4.5. Правила хранения пароля:

– запрещается записывать пароли на бумаге, в файле и других носителях информации, в том числе на предметах;

– запрещается сообщать другим пользователям личный пароль и/или регистрировать их в системе под своей учетной записью.

4.6. Лица, использующие паролирование, обязаны:

– четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов по паролированию;

– своевременно сообщать АБИ об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

5. Ответственность

5.1. Пользователь несет персональную ответственность за:

– сохранность носителей информации и содержащейся на них информации (в рабочее время);

– соблюдение требований данной Инструкции, неправомерное использование ресурсов ИСПД и за все действия, совершенные от имени его учетной записи в ИСПД, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учетной записи.

5.2. За разглашение ПД и нарушение порядка работы со средствами ИСПД, содержащими персональные данные, пользователи могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

Приложение № 12
к приказу МДОУ «Детский сад
«Ёлочка» г. Надыма»
от 15.08.2017 № 157

ИНСТРУКЦИЯ
по организации антивирусной защиты информационных систем персональных данных в МДОУ «Детский сад «Ёлочка» г. Надыма»

1. Общие положения

1.1. Настоящая Инструкция разработана в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также другими нормативными документами по безопасности информации, и определяет требования к организации защиты информационной системы персональных данных (ИСПД) МДОУ «Детский сад «Ёлочка» г. Надыма» (далее – МДОУ) от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения (далее – вредоносное ПО), устанавливает ответственность администратора безопасности информации (далее – АБИ) и других должностных лиц, настраивающих и сопровождающих средства антивирусной защиты в ИСПД, за выполнение указанных требований.

1.2. К использованию в МДОУ допускаются только лицензионные средства антивирусной защиты, централизованно закупленные у разработчиков или поставщиков данных средств.

1.3. Установка средств антивирусного контроля на компьютеры и сервера ИСПД МДОУ осуществляется АБИ, настройка параметров средств антивирусного контроля осуществляется в соответствии с руководствами по применению конкретных антивирусных средств и требованиями нормативных документов ФСТЭК РФ в области защиты персональных данных.

2. Применение средств антивирусного контроля

2.1. Антивирусный контроль должен осуществляться в режиме постоянной антивирусной защиты. Ежедневно в начале работы при загрузке компьютера (для серверов– при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль дисков и файлов АРМ.

2.2. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), хранящаяся на АРМ, передающаяся по сети, а также информация на съемных носителях. Контроль входящей информации должен осуществляться автоматически, непосредственно после ее приема. При передаче файлов, запакованных в архивы, без их распаковки, должна вручную инициироваться антивирусная проверка этих архивов.

2.3. Процедура обновления баз данных средств антивирусной защиты должна проводиться не реже одного раза в день на всех АРМ ИСПД, работающих в сети, не реже одного раза в неделю для всех АРМ ИСПД, работающих автономно.

2.4. Устанавливаемое (изменяемое) программное обеспечение должно быть

предварительно проверено АБИ на предмет отсутствия вредоносного программного обеспечения. Непосредственно после установки (изменения) программного обеспечения должна быть выполнена антивирусная проверка на всех защищаемых серверах и АРМ ИСПД.

2.5. При возникновении подозрения на наличие вредоносного программного обеспечения (частые ошибки в работе программ, появление посторонних графических и звуковых эффектов, искажение данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.) самостоятельно или вместе с АБИ провести внеочередной антивирусный контроль своего АРМ. При самостоятельном проведении антивирусного контроля–уведомить о результатах АБИ для определения им факта наличия или отсутствия вредоносного программного обеспечения.

3. Ответственность

3.1. Ответственность за проведение мероприятий антивирусного контроля и настройку средств антивирусного контроля в ИСПД МДОУ в соответствии с требованиями настоящей Инструкции возлагается на АБИ и всех должностных лиц, сопровождающих средства антивирусной защиты в ИСПД МДОУ.

3.2. Периодический контроль за состоянием антивирусной защиты (обновление антивирусной программы и антивирусных баз, а также проверка работоспособности средств антивирусной защиты) в ИСПД МДОУ, осуществляется АБИ и всеми должностными лицами, настраивающими и сопровождающими средства антивирусной защиты в ИСПД МДОУ.

Приложение № 13
к приказу МДОУ «Детский сад
«Ёлочка» г. Надыма»
от 15.08.2017 № 157

ИНСТРУКЦИЯ
по организации парольной защиты в информационных системах персональных данных в МДОУ «Детский сад «Ёлочка» г. Надыма»

1. Общие положения

1.1. Настоящая Инструкция разработана для реализации мер защиты информации, установленных в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также другими нормативными правовыми актами по защите информации, и регламентирует процессы генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах персональных данных (далее – ИСПД) МДОУ «Детский сад «Ёлочка» г. Надыма» (далее – МДОУ), а также контроль над действиями пользователей системы при работе с паролями.

1.2. Осуществление процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПД и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на администратора безопасности ИСПД.

2. Правила формирования паролей

2.1. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями информационной системы самостоятельно с учетом следующих требований:

2.1.1. длина пароля должна быть не менее 8 символов;

2.1.2. в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, <&, % и т.п.);

2.1.3. пароль не должен включать в себя имя пользователя, легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, абвгд и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетания букв и знаков, которые можно угадать, основываясь на информации о пользователе;

2.1.4. при смене пароля новое значение должно отличаться от предыдущего не менее чем в шести позициях.

2.2. Работникам МДОУ (далее – сотрудники) допускается использовать пароли, составленные из первых букв слов запоминающихся высказываний в разном регистре, смешанные в произвольном порядке со специальными символами (например, Кожзгсф7!).

2.3. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на администратора безопасности ИСПД.

2.4. Для обеспечения возможности использования имен и паролей некоторых сотрудников в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), сотрудники обязаны сразу же после установки своих паролей передавать их на хранение вместе с именами своих учетных записей администратору безопасности ИСПД в запечатанном конверте или опечатанном пенале.

3. Ввод пароля

3.1. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его просмотра посторонними лицами и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).

3.2. При неверном вводе пароля более 5 раз учетная запись пользователя должна блокироваться не менее чем на 3 минуты и не более чем на 15 минут.

4. Порядок смены личных паролей

4.1. Смена паролей должна проводиться регулярно, не реже одного раза в 12 месяцев, самостоятельно каждым пользователем.

4.2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) должно производиться немедленное удаление его учетной записи сразу после окончания последнего сеанса работы данного пользователя с системой.

4.3. Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) ответственного за обеспечение безопасности персональных данных, администратора безопасности и других сотрудников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

4.4. Администратор безопасности информации ведет Журнал учета паролей пользователей информационной системы персональных данных, в котором он отмечает причины внеплановой смены паролей пользователей.

4.5. Временный пароль, заданный администратором безопасности ИСПД при регистрации нового пользователя, должен действовать в течение ограниченного срока времени. Пользователь должен изменить временный пароль при первом входе в систему.

5. Хранение пароля

5.1. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке, мобильном телефоне и любых других предметах, и носителях информации.

5.2. Запрещается сообщать свой пароль полностью или частично другим пользователям, спрашивать или подсматривать пароль других пользователей.

5.3. Запрещается регистрировать других пользователей в ИСПД со своим личным паролем, входить в ИСПД под учетной записью и паролем другого пользователя.

6. Действия в случае утери и компрометации пароля

6.1. В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователя должна быть немедленно проведена внеплановая процедура смены пароля.

7. Ответственность

7.1. Каждый пользователь ИСПД несет персональную ответственность за соблюдение требований настоящей Инструкции и за все действия, совершенные от имени

его учетной записи в ИСПД, если с его стороны не было предпринято необходимых действий для предотвращения компрометации пароля его учетной записи.

7.2. Ответственность за контроль проведения мероприятий по организации парольной защиты в МДОУ возлагается на заместителей заведующего.

7.3. За разглашение персональных данных и нарушение порядка работы со средствами ИСПД, обрабатывающими персональные данные, сотрудники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной, предусмотренной законодательством Российской Федерации, ответственности.

Приложение № 14
к приказу МДОУ «Детский сад
«Ёлочка» г. Надыма»
от 15.08.2017 № 157

ИНСТРУКЦИЯ
по организации резервирования и восстановления программного обеспечения, баз персональных данных в информационных системах персональных данных МДОУ «Детский сад «Ёлочка» г. Надыма»

1. Назначение и область действия

1.1. Настоящая Инструкция разработана для реализации меры, направленной на поддержание непрерывности работы и восстановления работоспособности ИСПД, установленной в соответствии с требованиями приказа ФСТЭК России от 11.02.2013 №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», а также Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», другими нормативными документами по безопасности информации.

1.2. Целью настоящей Инструкции является превентивная защита элементов ИСПД от предотвращения потери защищаемой информации в МДОУ «Детский сад «Ёлочка» г. Надыма» (далее– МДОУ).

1.3. Задачей данной Инструкции является:

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

1.4. Действие настоящей Инструкции распространяется на всех пользователей ИСПД, имеющих доступ к ресурсам ИСПД, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

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

1.5. Пересмотр настоящей Инструкции осуществляется по мере необходимости.

1.6. Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается администратор безопасности информации МДОУ.

1.7. Ответственным сотрудником за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, назначаются заместители заведующего.

2. Порядок реагирования на инцидент

2.1. В настоящей Инструкции под инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПД, предоставляемых пользователям ИСПД, а также потерей защищаемой информации.

2.2. 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 ИСПД;
– в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

2.3. Все действия в процессе реагирования на Инцидент должны документироваться ответственным сотрудником в Журнале учета мероприятий по контролю согласно приложению, к данной Инструкции.

2.4. В кратчайшие сроки, администратор безопасности информации предпринимает меры по восстановлению работоспособности.

3. Меры обеспечения непрерывности работы и восстановления ресурсов

3.1. Технические меры.

3.1.1. 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 ИСПД включают:
– пожарные сигнализации и системы пожаротушения;
– системы вентиляции и кондиционирования;
– системы резервного питания.

3.1.2. Помещения, в которых размещаются элементы ИСПД, должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

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

3.1.4. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПД, 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;

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

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

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

3.2. Организационные меры.

3.2.1. Резервное копирование и хранение данных должно осуществляться:
– 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), с которых осуществляется их установка на элементы ИСПД–не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

3.2.2. Данные о проведении процедуры резервного копирования должны отражаться в специально созданном журнале учета.

3.2.3. Носители должны храниться не менее года, для возможности восстановления данных.

4. Ответственность

4.1. Ответственность за проведение мероприятий в соответствии с требованиями настоящей Инструкции возлагается на администратора безопасности информации МДОУ «Детский сад «Ёлочка» г. Надыма».

Приложение
к Инструкции по организации
резервирования и восстановления
программного обеспечения, баз
персональных данных в
информационных системах
персональных данных МДОУ
«Детский сад «Ёлочка» г. Надыма»

ЖУРНАЛ
УЧЕТА МЕРОПРИЯТИЙ ПО КОНТРОЛЮ

Начат «___» _____ 20 ___ г.

Окончен «___» _____ 20 ___ г.

На _____ листах

_____ _____ _____

(должность) (подпись) (Ф.И.О.)

Приложение № 15
к приказу МДОУ «Детский сад
«Ёлочка» г. Надыма»
от 15.08.2017 № 157

ИНСТРУКЦИЯ
о порядке доступа в помещения МДОУ «Детский сад «Ёлочка» г. Надыма», в которых ведётся обработка персональных данных

1. Общие положения

1.1. Настоящая Инструкция разработана в соответствии с федеральными законами от 27.07.2006 № 152-ФЗ «О персональных данных», от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлениями Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», другими нормативными правовыми актами, которые регулируют отношения, связанные с защитой персональных данных, в целях обеспечения защиты персональных данных.

1.2. Положения данной Инструкции обязательны для выполнения всеми работниками МДОУ «Детский сад «Ёлочка» г. Надыма» (далее – МДОУ, сотрудники), которые выполняют работы, связанные с обработкой, хранением, использованием и защитой персональных данных (далее – ПД) с использованием и без использования средств автоматизации.

1.3. Ответственными за организацию доступа в помещения МДОУ, в которых ведется обработка персональных данных, являются ответственные лица за обеспечение безопасности персональных данных, размещающиеся в этих помещениях.

2. Организационные меры по предотвращению несанкционированного доступа в помещения МДОУ, в которых ведется обработка ПД

2.1. Размещение технических средств информационной системы ПД (устройств и носителей информации), наличие специального оборудования в помещениях, в которых ведется работа с ПД (далее – помещения), режима обеспечения безопасности в этих помещениях, предусматривающего контроль доступа в них, должны обеспечивать сохранность носителей ПД и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

2.2. В отсутствии лиц, допущенных к работе с ПД (пользователей), входные двери помещений должны быть закрыты на ключ.

2.3. Пользователи, допущенные в установленном порядке к работе с ПД в информационных системах и прошедшие инструктаж по основам обеспечения режимных требований обязаны:

2.3.1. при уборке помещений посторонними лицами:

– прекратить работу на ПЭВМ и выключить монитор;

– убрать материальные и съемные носители ПД, документы с рабочего стола;
– сейфы закрыть на ключ;
– визуально проверить содержимое урн на наличие черновиков документов с ПД. Уничтожение черновиков производить в бумагорезательных машинах установленным порядком;

2.3.2. при проведении мероприятий по обработке ПД:
– обеспечить безопасность ПД при их обработке;
– окна помещений закрыть шторами (жалюзи);
– исключить обзор мониторов ПЭВМ посторонними лицами (посетителями), в том числе сотрудниками, не допущенными к работе с ПД;
– исключить бесконтрольное пребывание в помещениях посторонних лиц (посетителей) с целью предотвращения неправомерного или случайного доступа к ПД, их уничтожения, изменения, блокирования, копирования и распространения;

2.3.3. по окончании рабочего дня и перед закрытием помещений осмотреть и проверить:
– закрытие окон;
– выключение электроприборов и освещения;
– выключение основных технических средств обработки информации;
– закрытие и опечатывание всех сейфов;
– работоспособность пожарной и охранной сигнализации.

2.4. Нахождение в помещениях посторонних лиц, в том числе посетителей, в часы начала и окончания работы сотрудников допускается с их разрешения.

2.5. Посетители, работники сторонних учреждений, организаций и предприятий имеют право нахождения в зданиях МДОУ в пределах времени, установленного правилами внутреннего трудового распорядка, но не позднее 19 часов.

Пропуск посетителей в здания осуществляется согласно установленному пропускному режиму.

Документами, дающими право входа посетителям в здания МДОУ, являются:

- паспорт;
- удостоверения представителей органов власти и надзора (службы безопасности, министерства внутренних дел, министерства чрезвычайных ситуаций и др.).

Представители органов проходят по предъявлению служебных удостоверений после записи фамилии, имени, отчества прибывшего лица, времени посещения и фамилии сотрудника МДОУ, к которому осуществляется посещение.

3. Порядок доступа в помещения МДОУ, в которых ведется обработка персональных данных

3.1. Доступ и нахождение в помещениях сотрудников в нерабочее время, в выходные и праздничные дни допускается только с письменного разрешения заведующего, заместителей заведующего.

3.2. Доступ в помещения граждан (посетителей) в рамках служебной деятельности сотрудников осуществляется в рабочее время в установленные часы приема посетителей. Доступ в помещения посетителей регулируется пользователем, осуществляющим прием граждан. Прием граждан проводится по одному человеку и с его разрешения. Коллективные приемы посетителей не допускаются.

3.3. Доступ в помещения и прием иностранных граждан не допускается. В исключительных случаях такой прием возможен только по согласованию с заведующим или его заместителями.

3.4. Доступ в помещения и нахождение в них должностных лиц Роскомнадзора (прокуратуры, следственных органов) разрешается по указанию заведующего МДОУ или

его заместителя с целью проведения ими проверочных мероприятий в рамках контроля (надзора) деятельности МДОУ в сфере обработки ПД.

3.5. Внутренний контроль за соблюдением порядка доступа в помещения, в которых ведется обработка персональных данных, осуществляется заместителями заведующего в рамках полномочий.

4. Ответственность за нарушение установленного порядка доступа

4.1. За нарушение требований к обеспечению безопасности ПД при их обработке в автоматизированной системе, включая информационные системы ПД, за нарушение прав субъектов ПД, установленных Федеральным законодательством и иными нормативными правовыми актами Российской Федерации, приведшее к несанкционированному, в том числе случайному, доступу к ПД, повлекшему уничтожение, изменение, блокирование, копирование, распространение ПД, а также иные несанкционированные действия, предусмотрено наказание в соответствии с действующим законодательством Российской Федерации, нормативными правовыми актами Ямало-Ненецкого автономного округа.

Приложение № 16
к приказу МДОУ «Детский сад
«Ёлочка» г. Надыма»
от 15.08.2017 № 157

Инструкция
по порядку учета, хранения и уничтожения персональных данных
в МДОУ «Детский сад «Ёлочка» г. Надыма»

1. Общие положения

1.1. В МДОУ «Детский сад «Ёлочка» г. Надыма» (далее –МДОУ) все информационные ресурсы, содержащие персональные данные, подлежат учету.

1.2. Учет персональных данных осуществляется по журналам установленной формы, в том числе автоматизировано, с использованием средств автоматизированной техники.

1.3. МДОУ ведется Перечень информационных ресурсов, содержащих персональные данные.

1.4. В журнале указываются следующие реквизиты информационных ресурсов, содержащих персональные данные:

- учетный номер и дата поступления;
- откуда поступил;
- другие возможные реквизиты, идентифицирующие информационный ресурс.

1.5. Носители информационных ресурсов, содержащих персональные данные, должны сдаваться на хранение ответственному должностному лицу МДОУ.

2. Хранение и уничтожение персональных данных

2.1. Персональные данные субъекта персональных данных (далее – персональные данные субъекта) хранятся у специалиста по кадрам, который производит их обработку и отвечает за взаимодействие с субъектом персональных данных.

2.2. Персональные данные субъекта на бумажном носителе хранятся в папках в шкафу.

2.3. Персональные данные субъекта в электронном виде хранятся в локализованных электронных базах данных компьютерной сети. Доступ к электронным базам данных, содержащим персональные данные субъекта, обеспечиваются системой защиты персональных данных.

2.4. В нерабочее время помещение, где хранятся персональные данные (хранилище персональных данных) закрывается на ключ. В рабочее время помещение должно быть закрыто на ключ или оставлено под ответственность специалиста по кадрам.

2.5. Сотрудники, имеющие доступ к персональным данным субъектов персональных данных, в связи с исполнением трудовых обязанностей, обеспечивают хранение информации, содержащей персональные данные субъекта, исключающее доступ к ним третьих лиц.

2.6. В отсутствие сотрудника на его рабочем месте не должно быть документов, содержащих персональные данные субъектов (соблюдение «политики чистых столов»).

2.7. При уходе в отпуск, служебной командировке и иных случаях длительного отсутствия сотрудника на своем рабочем месте, он обязан передать документы и иные носители, содержащие персональные данные субъектов, лицу, которое будет исполнять его должностные обязанности в его отсутствие.

2.8. При увольнении сотрудника, имеющего доступ к персональным данным субъектов, документы и иные носители, содержащие персональные данные субъектов, по указанию заведующего передаются другому сотруднику, имеющему доступ к персональным данным субъектов.

2.9. Ежедневный контроль за выполнением требований по защите хранилищ персональных данных осуществляют лица, ответственные за помещение (хранилище персональных данных).

2.10. Периодический контроль эффективности мер защиты хранилищ персональных данных осуществляется комиссией по защите персональных данных в МДОУ.

2.11. Уничтожение персональных данных субъектов на бумажных носителях либо удаление электронных баз данных, содержащих персональные данные субъектов в электронном виде, осуществляется по истечении установленного срока обработки персональных данных комиссией по защите персональных данных в МДОУ.

3. Ответственность

Сотрудники, нарушившие требования настоящей Инструкции, несут ответственность в соответствии с действующим законодательством РФ и локальными правовыми актами.

Приложение № 17
к приказу МДОУ «Детский сад
«Ёлочка» г. Надыма»
от 15.08.2017 № 157

ИНСТРУКЦИЯ
по порядку учета, хранения съемных носителей персональных данных в МДОУ «Детский сад «Ёлочка» г. Надыма»

1. Общие положения

1.1. Администратор безопасности информации – технический специалист, обеспечивающий ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации ПО и оборудования вычислительной техники (далее – Администратор).

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

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

1.4. ИСПД – информационная система персональных данных – это совокупность программных и технических средств (компьютеры, принтеры, сканеры, коммутационное оборудование и т.д.), на которых обрабатываются персональные данные.

1.5. Съемный носитель ПД – любой материальный объект, используемый для хранения и передачи электронной информации содержащей персональные данные (дискеты, флеш-накопитель, съемные жесткие диски, оптические диски и т.д.).

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

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

1.8. ПК– персональный компьютер.

1.9. ПО– программное обеспечение вычислительной техники.

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

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

1.12. Пользователь – работник МДОУ (далее – МДОУ, сотрудник), использующий мобильные устройства и носители информации для выполнения своих служебных обязанностей.

2. Порядок использования съемных носителей ПД

2.1. Под использованием съемных носителей ПД при работе с ИСПД понимается их подключение к инфраструктуре ИСПД с целью обработки, приема/передачи информации между ИСПД и носителями информации.

2.2. В ИСПД допускается использование только учтенных съемных носителей ПД, которые являются собственностью МДОУ и подвергаются регулярной ревизии и контролю.

2.3. К съемным носителям ПД предъявляются те же требования ИБ, что и для стационарных АРМ (целесообразность дополнительных мер обеспечения ИБ определяется администраторами ПД).

2.4. Съемные носители ПД предоставляются сотрудникам по инициативе непосредственных руководителей (заместителей заведующих) в случаях:

– необходимости выполнения вновь принятыми сотрудниками своих должностных обязанностей;

– возникновения производственной необходимости по обработки ПД.

3. Порядок учета, хранения и обращения со съемными носителями ПД

3.1. Все находящиеся на хранении и в обращении съемные носители ПД подлежат учёту.

3.2. Каждый съемный носитель ПД с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

3.3. Учет и выдачу съемных носителей ПД осуществляют заместители заведующего, на которых возложены функции хранения съемных носителей ПД. Факт выдачи съемного носителя ПД фиксируется в журнале учета защищаемых носителей информации по форме согласно приложению № 1 к настоящей Инструкции.

3.4. Сотрудники получают учтенный съемный носитель ПД от заместителя заведующего для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета защищаемых носителей информации. По окончании работ пользователь сдает съемный носитель ПД для хранения заместителю заведующего, о чем делается соответствующая запись в журнале учета защищаемых носителей информации.

3.5. При использовании сотрудниками съемных носителей ПД необходимо:

3.5.1. соблюдать требования настоящей Инструкции;

3.5.2. использовать съемные носители ПД исключительно для выполнения своих служебных обязанностей;

3.5.3. ставить в известность администратора безопасности информации о любых фактах нарушения требований настоящей Инструкции;

3.5.4. бережно относиться к съемным носителям ПД;

3.5.5. обеспечивать физическую безопасность съемным носителям ПД всеми разумными способами;

3.5.6. извещать администратора безопасности информации о фактах утраты (кражи) съемного носителя ПД.

3.6. При использовании съемных носителей ПД запрещено:

3.6.1. использовать съемные носители ПД в личных целях;

3.6.2. передавать съемные носители ПД другим лицам (за исключением администратора безопасности информации);

3.6.3. хранить съемные носители ПД вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

3.6.4. выносить съемные носители ПД из помещений МДОУ, в которых ведётся обработка персональных данных для работы с ними на дому и т.д.

3.7. Любое взаимодействие (обработка, прием/передача информации) инициированное сотрудником между ИСПД и неучтенными (личными) съемными носителями информации, рассматривается как несанкционированное (за исключением случаев, оговоренных с администратором безопасности информации заранее). Администратор безопасности информации оставляет за собой право блокировать или ограничивать использование съемных носителей информации.

3.8. Информация об использовании сотрудником съемных носителей ПД в ИСПД протоколируется и, при необходимости, может быть представлена администратором безопасности информации.

3.9. В случае выявления фактов несанкционированного и/или нецелевого использования съемных носителей ПД инициализируется служебная проверка, проводимая комиссией по защите персональных данных МДОУ (далее– Комиссия).

3.10. По факту выясненных обстоятельств Комиссией составляется акт расследования инцидента для принятия мер согласно локальным правовым актам и действующему законодательству.

3.11. Информация, хранящаяся на съемных носителях ПД, подлежит обязательной проверке на отсутствие вредоносного ПО.

3.12. При отправке или передаче персональных данных адресатам на съемные носители ПД записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съемных носителях ПД осуществляется в порядке, установленном для документов для служебного пользования.

3.13. Вынос съемных носителей ПД для непосредственной передачи адресату осуществляется только с письменного разрешения администратора безопасности информации.

3.14. В случае утраты или уничтожения съемных носителей ПД либо разглашении содержащихся в них сведений, немедленно ставится в известность администратор безопасности информации. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета бумажных и съемных носителей ПД.

3.15. Съемные носители ПД, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей ПД осуществляется Комиссией. По результатам уничтожения съемных носителей ПД составляется акт уничтожения ПД согласно приложению № 2 к настоящей Инструкции.

3.16. В случае увольнения или перевода сотрудника в другое структурное подразделение, предоставленные съемные носители ПД изымаются.

4. Ответственность

4.1. Сотрудники, нарушившие требования настоящей Инструкции, несут ответственность в соответствии с действующим законодательством и локальными правовыми актами.

Приложение № 1
к Инструкции по порядку учета,
хранения съемных носителей
персональных данных в МДОУ
«Детский сад «Ёлочка» г. Надыма»

ЖУРНАЛ
УЧЕТА ЗАЩИЩАЕМЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

МДОУ «ДЕТСКИЙ САД «ЁЛОЧКА» Г. НАДЫМА»

Начат «___» _____ 20 ___ г.

Окончен «___» _____ 20 ___ г.

На _____ листах

_____	_____	_____
(должность)	(подпись)	(Ф.И.О.)

Регистрационный номер, дата регистрации	Тип защищаемого носителя информации (заводской номер)	Назначение (содержимое) носителя	Расписка в получении (Ф.И.О., подпись, дата)	Расписка об обратном приёме (Ф.И.О., подпись, дата)	Местонахождение (хранение) носителя, Ф.И.О. ответственного	Уничтожение носителя (№ и дата акта), отметка об отправке (№ и дата
1	2	3	4	5	6	7

Приложение № 2
к Инструкции по порядку учета,
хранения съемных носителей
персональных данных в МДОУ
«Детский сад «Ёлочка» г. Надыма»

Типовая форма акта об уничтожении носителей персональных данных

В связи с достижением цели обработки персональных данных (ПД) к уничтожению отобраны следующие бумажные носители персональных данных:

№ п/п	Учетный номер носителя	Цель обработки ПД	Дата начала обработки ПД	Дата окончания обработки ПД
1	2	3	4	5
1.				
2.				
3.				

ПДн должны быть уничтожены со следующих материальных носителей:

№ п/п	Учетный номер носителя	Цель обработки ПД	Дата начала обработки ПД	Дата окончания обработки ПД
1	2	3	4	5
1.				
2.				
3.				

Всего подлежат уничтожению _____ бумажных носителей ПД.

Уничтожение информации необходимо с _____ материальных носителей.
Проверка правильности включения материальных носителей ПД в Акт проведена.

Бумажные носители ПД полностью уничтожены путем

_____

ПД с материальных носителей уничтожены путем

_____

СОГЛАСОВАНО
Зам.заведующего

_____ _____ _____
(ФИО) (подпись) (дата)

ОТМЕТКА О ВЫПОЛНЕНИИ
Ответственный за выполнение

_____ _____ _____
(ФИО, должность) (подпись) (дата)

Приложение № 18
к приказу МДОУ «Детский сад
«Ёлочка» г. Надыма»
от 15.08.2017 № 157

ИНСТРУКЦИЯ
по модификации технических и программных средств в МДОУ «Детский сад «Ёлочка» г. Надыма»

1. Порядок изменения конфигурации технических и программных средств

Настоящая Инструкция регламентирует обеспечение безопасности информации при проведении обновления (модификации) общесистемного и прикладного программного обеспечения, технического обслуживания и при возникновении нештатных ситуаций в работе информационной системы персональных данных (далее– ИСПД) МДОУ «Детский сад «Ёлочка» г. Надыма» (далее–МДОУ).

Право внесения изменений в конфигурацию аппаратно-программных средств, защищенных ИСПД предоставляется по согласованию с органом аттестации, проводившим аттестацию данной ИСПД, а именно:

– в отношении системных и прикладных программных средств– администратору безопасности информации;

– в отношении аппаратных средств, а также в отношении программно – аппаратных средств защиты– администратору безопасности информации.

1.1. Изменение конфигурации аппаратно-программных средств ИСПД кем-либо, кроме администратора безопасности ПД, запрещено.

1.2. Внесение всех изменений в конфигурацию системных и прикладных программных средств ИСПД инициируется заявкой администратору безопасности информации МДОУ. Форма заявки приведена в приложении № 1 к настоящей инструкции.

1.3. В заявке могут указываться следующие виды необходимых изменений в состав аппаратных и программных средств ИСПД:

– установка (развертывание) на автоматизированном рабочем месте (далее – АРМ) программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи на данном АРМ);

– обновление (замена) на АРМ программных средств, необходимых для решения определенной задачи (обновление версий программ, используемых для решения определенных задач);

– удаление с АРМ программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на данной АРМ).

1.4. Подготовка обновления (модификации) общесистемного и прикладного программного обеспечения ИСПД, тестирование, стендовые испытания (при необходимости) и передача исходных текстов, документации и дистрибутивных носителей программ в архив дистрибутивов установленного программного обеспечения, внесение необходимых изменений в настройки средств защиты от несанкционированного доступа и средств контроля целостности файлов на компьютерах, (обновление) и удаление системных и прикладных программных средств производятся администратором безопасности информации по согласованию с органом по аттестации, проводившим аттестацию данной ИСПД.

1.5. Установка или обновление подсистем ИСПД должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

1.6. Установка или обновление программного обеспечения (далее – ПО) на ИСПД производится с оригинальных лицензионных дистрибутивных носителей, полученных установленным порядком.

1.7. Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, и, насколько это возможно, на отсутствие опасных функций (не задокументированных возможностей).

1.8. После установки (обновления) ПО администратор безопасности информации Департамента образования должен произвести требуемые настройки средств управления доступом к компонентам ИСПД и проверить работоспособность ПО, правильность их настройки.

Администратор безопасности информации МДОУ делает отметку о выполнении на обратной стороне заявки (Приложение № 2) и в «Техническом паспорте на АРМ».

1.9. Оригиналы заявок (документов), на основании которых производились изменения в составе программных средств АРМ, с отметками о внесении изменений в состав программных средств должны храниться вместе с техническим паспортом на ИСПД у Администратора безопасности информации МДОУ. Эти документы могут впоследствии использоваться:

- для восстановления конфигурации АРМ после аварий;
- для контроля правомерности установки на АРМ средств, для решения соответствующих задач при разборе конфликтных ситуаций;
- для проверки правильности установки и настройки средств защиты на АРМ.

Приложение № 1
к Инструкции
по модификации технических и
программных средств
в МДОУ «Детский сад
«Ёлочка» г. Надыма»

ОБРАЗЕЦ

ЗАЯВКА
на внесение изменений в состав аппаратно-программных средств информационных систем персональных данных автоматизированных рабочих мест

Прошу произвести следующие изменения конфигурации программных (аппаратно-программных) средств информационных систем персональных данных автоматизированных рабочих мест _____:
наименование АРМ

установить (обновить, удалить) новое программное обеспечение (аппаратно-программные средства, компоненты):
_____
_____
_____,

необходимые для решения следующих задач:
_____
_____
_____

Заместитель заведующего
МДОУ «Детский сад «Ёлочка» г. Надыма» _____
(подпись, фамилия, инициалы)

«___» _____ 20 ___ года

Приложение № 2
к Инструкции
по модификации технических и
программных средств
в МДОУ «Детский сад «Ёлочка» г.
Надыма»

ОБРАЗЕЦ

Отметка о выполнении (о внесении изменений в состав аппаратно-программных средств ПЭВМ АРМ)

В соответствии с Инструкцией по модификации технических и программных средств информационных систем персональных данных в Департаменте образования Надымского района рабочей группой в составе:

Администратор безопасности информации МДОУ «Детский сад «Ёлочка» г. Надыма» _____

Заместитель заведующего
_____

указанные в заявке изменения внесены (не внесены по следующей причине):
_____
краткое описание причины

_____
_____
_____

Изменения в технический паспорт на АРМ (ссылка на данную заявку) внесены.

Администратор безопасности информации
_____
(подпись, фамилия, инициалы)

Заместитель заведующего
_____
(подпись, фамилия, инициалы)

«___» _____ 20 ___ года

Приложение № 3
к Правилам рассмотрения запросов субъектов персональных данных или их представителей в МДОУ «Детский сад «Ёлочка» г. Надыма»

Форма журнала
учета обращений субъектов персональных данных о выполнении их законных прав при обработке персональных данных в информационных системах персональных данных

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

ЖУРНАЛ
учета обращений субъектов персональных данных о выполнении их законных прав при обработке персональных данных в информационных системах персональных данных

№	ФИО	Дата	Цель
1	2	3	4

Приложение № 19
к приказу МДОУ
«Детский сад «Ёлочка» г. Надыма»
от 15.08.2017 № 157

ПЕРЕЧЕНЬ

информационных систем персональных данных (ИСПД)
в МДОУ «Детский сад «Ёлочка» г. Надыма»

№ п/п	Название ИСПД	Класс системы (уровень защищенности)	Назначение	Состав ИСПД	Местонахождение ИСПД
1	2	3	4	5	6
1					
2					
3					
4					
5					