ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ СИСТЕМ И ПЕРСРНАЛЬНЫХ ДАННЫХ ОБРАБАТЫВАЕМЫХ В МАДОУ «ДЕТСКИЙ САД № 2» ПИОНЕРСКОГО ГОРОДСКОГО ОКРУГА»

1.Перечень персональных данных.

Автоматиз. средства обработки ПДн	Содержание ПДн	Должностные лица обрабатывающие ПДн	Максимальный срок хранения ПДн	Обоснование обработки
АИС СП Автоматизированная система	ФИО, паспортные данные, дата рождения национальность, образование, адрес по прописке, адрес фактического места проживания, ИНН, страховое свидетельство государственного пенсионного страхования должность, результаты медицинского осмотра, сведения о трудовом стаже, о составе семьи, характеристики, копии приказов по личному составу, фотографии	Заведующий, заместитель заведующего, делопроизводитель, главный бухгалтер бухгалтер	75 лет	Трудовой Кодекс Российской Федерации, Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

2. Перечни персональных данных, обрабатываемых в МАДОУ «Детский сад № 2» Пионерского городского округа» :
фамилия, имя, отчество;
адрес проживания и прописки;
иные паспортные данные;
семейное положение;
телефон;
ИНН;
СНИЛС;
трудовые книжки;
иные сведения, указанные заявителем, а также персональные данные, содержащиеся в:

письменном заявлении с просьбой о поступлении на работу;

собственноручно заполненной и подписанной гражданином Российской Федерации анкеты;

документах о прохождении конкурса на замещение вакантной должности (если гражданин назначен на должность по результатам конкурса);

копиях паспорта и свидетельства о государственной регистрации актов гражданского состояния;

трудовой книжки или документе, подтверждающем периоды работы, прохождение военной или иной службы;

копии документов о профессиональном образовании, профессиональной переподготовке, повышении квалификации, стажировке, присвоении ученой степени, ученого звания (если таковые имеются);

экземпляр трудового договора, а также экземпляр письменных дополнительных соглашений, которыми оформляются изменения и дополнения, внесенные в трудовой договор;

копии распоряжения администрации о переводе работника на иную должность, о временном замещении им иной должности;

копии документов воинского учета (для граждан, пребывающих в запасе);

копии распоряжения администрации об освобождении от замещаемой должности, о прекращении трудового договора или его приостановлении;

аттестационном листе работника, прошедшего аттестацию, и отзыве об исполнении им должностных обязанностей за аттестационный период;

копии документов о включении работника в кадровый резерв, а также об исключении его из кадрового резерва;

копии распоряжения администрации о поощрении работника, а также о наложении на него дисциплинарного взыскания до его снятия или отмены;

копии документов о начале служебной проверки, ее результатах, об отстранении от замещаемой должности;

документах, связанных с оформлением допуска к сведениям, составляющим государственную или иную охраняемую законом тайну, если исполнение обязанностей по замещаемой должности связано с использованием таких сведений;

сведениях о доходах, имуществе и обязательствах имущественного характера работника;

копии страхового свидетельства обязательного пенсионного страхования;

копии свидетельства о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации;

копии страхового медицинского полиса обязательного медицинского страхования граждан;

медицинском заключении установленной формы об отсутствии у гражданина заболевания, препятствующего поступлению на работу..

3. Перечень персональных данных, обрабатываемых без использования средств автоматизации.

- На основании Федерального закона от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», в администрации обрабатываются персональные данные граждан (ФИО, адрес, паспортные данные), и представлены в следующих документах:

- Обращения и жалобы сотрудников;

- Ответы по обращениям сотрудников.

РАЗРЕШИТЕЛЬНАЯ СИСТЕМА (МАТРИЦА) ДОСТУПА
К ПЕРСОНАЛЬНЫМ ДАННЫМ В МАДОУ «ДЕТСКИЙ САД № 2» ПИОНЕРСКОГО ГОРОДСКОГО ОКРУГА»:

1. Список сотрудников, имеющих доступ к персональным данным

1.1. К персональным данным обрабатываемых неавтоматизированным способом, для выполнения своих должностных обязанностей имеют доступ сотрудники, замещающие должности, не являющиеся должностями муниципальной службы.

1.2. Каждый сотрудник имеет доступ к своим персональным данным.

1.3. Ответственность за работу с бумажными носителями персональных данных обратившихся граждан несут следующие сотрудники:

- и.о.заведующего — Спетницкая Л.Н.
- заместитель заведующего — Капущинская Т.В.
- Заместитель по АХЧ — Грацианова Г.А.
- делопроизводитель – Мурашова И.Д.
- главный бухгалтер – Ковалева Е.С.
- Бухгалтер — Крестенкова С.С.

Каждый сотрудник, чьи персональные данные имеются в учреждении, может обратиться в учреждение для получения своих персональных данных.

2.Пользователи информационных систем персональных данных

№	ФИО	Должность	Наименование рабочих станций, к работе на которых допущен пользователь	Группа, в которую входит сотрудник
1.	Спетницкая Л.Н..	и.о. заведующего	электронный детский сад, сайт, «Аверс»	Пользователи
2.	Капущинская Т.В.	Заместитель заведующего	сайт, электронный детский сад	Пользователи, ответственный за организацию обработки ПДн
3.	Грацианова Г.А..	Заместитель заведующего	сайт	Пользователи, ответственный за обработку
4.	Мурашова И.Д.	делопроизводитель	сайт	Пользователи, ответственный за обработку
5	Ковалева Е.С.	Главный бухгалтер	«1С»,»Аверс»	Пользователи, ответственный за обработку
6	Крестенкова С.С.	бухгалтер	«1С», «Аверс»	Пользователи, ответственный за обработку

Правила
обработки персональных данных,
устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований

1. Обработка персональных данных должна осуществляться на законной основе.

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

3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

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

7. Меры, направленные на выявление и предотвращение нарушений, предусмотренных законодательством:

1) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону от 27.07.2006г. №152-ФЗ «О персональных данных» (далее - Федеральный закон);

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

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

8. Обеспечение безопасности персональных данных достигается, в частности:

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

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

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

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

5) учетом машинных носителей персональных данных ;

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

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

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

9. Целями обработки персональных данных работников являются:

1) обеспечение соблюдения законов и иных нормативных правовых актов;

2) учет работников в учреждении;

3) соблюдение порядка и правил приема в учреждение;

4) использование в уставной деятельности с применением средств автоматизации или без таких средств, включая хранение этих данных в архивах и размещение в информационно-телекоммуникационных сетях с целью предоставления доступа к ним;

5) заполнение базы данных автоматизированной информационной системы в целях повышения эффективности и быстрого поиска, проведение мониторинговых исследований, формирование статистических и аналитических отчётов в вышестоящие органы;

6) обеспечение личной безопасности работников;

10. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом. Уничтожение носителей персональных данных производится комиссией с оформлением Акта об уничтожении согласно приложению к данным правилам.. Уничтожение может быть произведено любым способом, исключающим возможность восстановления носителя.

11. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий 3 (трех) рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий 10 (десяти) рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

12. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий 30 (тридцати) дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом.

13. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий 3-х дней с даты получения указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом персональных данных. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.

14. В случае отсутствия возможности уничтожения персональных данных в течение сроков, указанных выше, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем 6 (шесть) месяцев, если иной срок не установлен федеральными законами.

Приложение
к Правилам обработки персональных данных,
устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований

А К Т
уничтожения носителей
персональных данных
«___»_____2017г.

Настоящий Акт составлен в том, что комиссией, в составе:

ПРЕДСЕДАТЕЛЬ:

_____ - _____
(ФИО) (должность)

ЧЛЕНЫ КОМИССИИ:

_____ - _____
(ФИО) (должность)
_____ - _____
(ФИО) (должность)
_____ - _____
(ФИО) (должность)

произведено уничтожение носителей, содержащих персональные данные сотрудников _____
_____.

Уничтожение произведено путем _____.

Опись носителей:

Наименование	Учетный номер	Примечание

Председатель:

_____ - _____
(ФИО) (должность)

Члены комиссии

Положение
об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации

I. Общие положения

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

2.Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.

3.Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установленные нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами МАДОУ «Детский сад №2» Пионерского городского округа» (далее – МАДОУ «Детский сад №2», должны применяться с учетом требований настоящего Положения.

II. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации

4.Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).

5.При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

6. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники МАДОУ «Детский сад № 2» - оператора или лица, осуществляющие такую обработку по договору с оператором), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами МАДОУ (при их наличии).

7.При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), 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 обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки

персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

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

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

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

8.При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях, должны соблюдаться следующие условия:

а) необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом оператора, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

б) копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

в) персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию, на которой находится оператор.

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

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

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

10.Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

11.Правила, предусмотренные пунктами 9 и 10 настоящего Положения, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

12. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

III. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

13.Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

14.Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

15.При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором.

Порядок
доступа работников МАДОУ «Детский сад № 2» Пионерского городского округа» в помещения,
в которых ведется обработка персональных данных

1. Настоящий Порядок доступа сотрудников в помещении, в которых ведется обработка персональных данных, (далее – Порядок) устанавливают единые требования к доступу сотрудников в служебные помещения в целях предотвращения нарушения прав субъектов персональных данных, обрабатываемых в МАДОУ «Детский сад № 2» и обеспечения соблюдения требований законодательства о персональных данных.

2. Настоящий Порядок обязателен для применения и исполнения всеми сотрудниками.

3. Помещения, в которых сотрудника ведется обработка персональных данных, должны отвечать определенным нормам и исключать возможность бесконтрольного проникновения в них посторонних лиц и гарантировать сохранность находящихся в этих помещениях документов и средств автоматизации.

4. Входные двери оборудуются замками, гарантирующими надежное закрытие помещений в нерабочее время.

5. По завершению рабочего дня, помещения, в которых ведется обработка персональных данных, закрываются.

6. Вскрытие помещений, где ведется обработка персональных данных, производят сотрудники, работающие в этих помещениях.

7. При отсутствии сотрудников, работающих в этих помещениях, помещения могут быть вскрыты комиссией, созданной по указанию заведующей.

8. В случае утраты ключей от помещений немедленно заменяется замок.

9. Уборка в помещениях, где ведется обработка персональных данных, производится только в присутствии служащих, работающих в этих помещениях.

10. При обнаружении повреждений запоров или других признаков, указывающих на возможное проникновение в помещения, в которых ведется обработка персональных данных, посторонних лиц, эти помещения не вскрываются, а составляется акт и о случившемся немедленно ставятся в известность заведующую и органы МВД.

11. Одновременно принимаются меры по охране места происшествия и до прибытия работников органов МВД в эти помещения никто не допускается.

Журнал учета обращений субъектов персональных данных по вопросам обработки персональных данных

Журнал начат «____» _____ 20__г.

Журнал завершен «____» _____ 20__г.

заведующая_____

/Должность/ _____ / ФИО должностного лица

На _____ листах

№ п/п	Сведения о запрашивающем лице	Краткое содержание обращения	Цель запроса	Отметка о предоставлении информации или отказе в ее предоставлении	Дата передачи / отказа в предоставлении информации	Подпись ответственного лица	Примечание
1							
2							
3							
4							
5							

ПРАВИЛА
рассмотрения запросов субъектов персональных данных
в МАДОУ «Детский сад №2» Пионерского городского округа»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила разработаны в соответствии с Федеральным законом «О персональных данных» от 27.07.2006г. № 152-ФЗ и Трудовым Кодексом Российской Федерации и определяют порядок обработки поступающих в МАДОУ «Детский сад № 2» обращений субъектов персональных данных (сотрудников).

2. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. В соответствии с действующим законодательством субъект персональных данных имеет право на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных, в том числе содержащей:
- подтверждение факта обработки персональных данных МАДОУ«Детский сад № 2», а также цель такой обработки;
- способы обработки персональных данных, применяемые МАДОУ«Детский сад № 2»;
- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

2.2. Право субъекта персональных данных на доступ к своим персональным данным ограничивается в случае, если:
- обработка персональных данных, в том числе персональных данных, полученных в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;
- обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;
- предоставление персональных данных нарушает конституционные права и свободы других лиц.

2.3. Если субъект персональных данных считает, что МАДОУ«Детский сад № 2» осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» от 27.07.2006г. № 152-ФЗ или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие МАДОУ«Детский сад № 2» в уполномоченном органе по защите прав субъектов персональных данных или в судебном порядке.

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

3. ПОРЯДОК РАБОТЫ С ОБРАЩЕНИЯМИ СУБЪЕКТОВ

3.1. При поступлении обращения субъекта, МАДОУ«Детский сад № 2» должно зарегистрировать его в Журнале учета обращений субъектов персональных данных.

3.2. МАДОУ«Детский сад №2» обязано сообщить субъекту персональных данных или его законному представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с ними при обращении субъекта персональных данных или его законного представителя либо в течение десяти рабочих дней с даты получения запроса субъекта персональных данных или его законного представителя.

3.3. В случае отказа в предоставлении субъекту персональных данных или его законному представителю при обращении либо при получении запроса субъекта персональных данных или его законного представителя информации о наличии персональных данных о соответствующем субъекте персональных данных, а также таких персональных данных МАДОУ«Детский сад №2» обязан дать в письменной форме мотивированный ответ в срок, не превышающий семи рабочих дней со дня обращения субъекта персональных данных или его законного представителя либо с даты получения запроса субъекта персональных данных или его законного представителя.

3.4. МАДОУ«Детский сад № 2» обязано безвозмездно предоставить субъекту персональных данных или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлении субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет МАДОУ«Детский сад №2», являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах МАДОУ«Детский сад № 2» обязано уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы.

3.5. МАДОУ«Детский сад № 2» обязано сообщить в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение семи рабочих дней с даты получения такого запроса.

СПИСОК ПОМЕЩЕНИЙ
МАДОУ«Детский сад № 2» Пионерского городского округа,
в котором обрабатываются персональные данные и доступ к ним, а также перечень должностей учреждения, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

1. Для хранения бумажных документов предназначен кабинеты: заведующего, делопроизводителя, главного бухгалтера в здании МАДОУ«Детский сад № 2» по адресу: Калининградская обл, г.Пионерский, ул. Шаманова,5а

2. Для размещения автоматизированных рабочих мест (АРМ) информационных систем персональных данных (ИСПДн) предназначены кабинеты: заведующего, старшего воспитателя в здании по адресу: Калининградская обл, г.Пионерский, ул. Шаманова,5а.

Перечень помещений,
в которых осуществляется обработка и хранение персональных данных

кабинет	Наименование должности сотрудника, осуществляющего обработку ПД	Обрабатываемые персональные данные
Кабинет заведующей	заведующая	все виды персональных данных персональные данные сотрудников
Кабинет делопроизводителя	делопроизводитель	все виды персональных данных персональные данные сотрудников относительно педагогического образования, педагогического стажа, курсов повышения квалификации, аттестации
Кабинет бухгалтера	главный бухгалтер	все виды персональных данных исполнения договоров и другие

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в МАДОУ«Детский сад № 2» Пионерского городского округа»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных МАДОУ«Детский сад № 2» разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и постановления 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».

1.2. Настоящие Правила определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных и действуют постоянно.

2. ТЕМАТИКА ВНУТРЕННЕГО КОНТРОЛЯ

2.1. Тематика проверок обработки персональных данных с использованием средств автоматизации:

- соответствие полномочий пользователя матрице доступа;
- соблюдение пользователями информационных систем персональных данных МАДОУ«Детский сад № 2» парольной политики;
- соблюдение пользователями информационных систем персональных данных МАДОУ«Детский сад № 2» политики;
- соблюдение пользователями информационных систем персональных данных МАДОУ«Детский сад № 2» правил работы со съемными носителями персональных данных;
- соблюдение порядка доступа в помещения МАДОУ«Детский сад № 2» доложены элементы информационных систем персональных данных;
- соблюдение порядка резервирования баз данных и хранения резервных копий;
- соблюдение порядка работы со средствами защиты информации;
- знание пользователей информационных систем персональных данных о своих действиях во внештатных ситуациях.

2.2. Тематика проверок обработки персональных данных без использования средств автоматизации:

- хранение бумажных носителей с персональными данными;
- доступ к бумажным носителям с персональными данными;
- доступ в помещения, где обрабатываются и хранятся бумажные носители с персональными данными.

3.ПОРЯДОК ПРОВЕДЕНИЯ ВНУТРЕННИХ ПРОВЕРОК

3.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям МАДОУ «Детский сад № 2» проведение периодических проверок условий обработки персональных данных (приложение 1 план внутренних проверок условий обработки персональных данных в МАДОУ.

3.2. Проверки осуществляются ответственным за организацию обработки персональных данных (далее - Ответственный) либо комиссией, образуемой заведующей МАДОУ по необходимости.

3.3. Проверки осуществляются Ответственным либо комиссией непосредственно на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки персональных данных.

Для каждой проверки составляется Протокол проведения внутренней проверки. Форма Протокола приведена в Приложении 2 к настоящим Правилам.

3.4. При выявлении в ходе проверки нарушений, Ответственным либо Председателем комиссии в Протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.

3.5. Протоколы хранятся у Ответственного либо Председателя комиссии в течение текущего года. Уничтожение Протоколов проводится Ответственным либо комиссией самостоятельно в январе следующего за проверочным годом.

3.6. О результатах проверки и мерах, необходимых для устранения нарушений, заведующей докладывает Ответственный либо Председатель комиссии.

Приложение № 1
к Правилам осуществления внутреннего контроля соответствия
обработки персональных данных требованиям к защите персональных данных
в МАДОУ «Детский сад № 2»

План
внутренних проверок условий обработки персональных данных
в МАДОУ «Детский сад №2» Пионерского городского округа»

№	Тема проверки	Нормативный документ, предъявляющий требования	Срок проведения	Исполнитель
1.	Соответствие полномочий пользователя правилам обработки персональных данных	Правила обработки персональных данных Политика МАДОУ «Детский сад №2» в отношении обработки персональных данных	ежегодно	Ответственный за организацию обработки персональных данных
2.	Соблюдение пользователями информационных систем персональных данных парольной политики	Положение по защите персональных данных МАДОУ«Детский сад №2», обрабатываемых в ИС ПДн	еженедельно	Ответственный за организацию обработки персональных данных
3.	Соблюдение пользователями информационных систем персональных данных антивирусной политики		еженедельно	Ответственный за организацию обработки персональных данных
4.	Соблюдение порядка доступа в помещения, где расположены элементы информационных систем персональных данных	Список помещений МАДОУ «Детский сад №2», в которых обрабатываются персональные данные и доступ к ним	ежегодно	Ответственный за организацию обработки персональных данных
5.	Соблюдение порядка резервирования баз данных и хранения резервных копий	Положение по защите персональных данных МАДОУ«Детский сад №2», обрабатываемых в ИС ПДн	еженедельно	Ответственный за организацию обработки персональных данных
6.	Соблюдение порядка работы со средствами защиты информации		ежегодно	Ответственный за организацию обработки персональных данных
7.	Знание пользователей информационных систем персональных данных о своих действиях во внештатных ситуациях		ежегодно	Ответственный за организацию обработки персональных данных
8.	Хранение бумажных носителей с	Положение по защите персональных данных	ежегодно	Ответственный за организацию

	персональными данными	МАДОУ «Детский сад №2», обрабатываемых без использования средств автоматизации		обработки персональных данных
9.	Доступ к бумажным носителям с персональными данными		ежегодно	Ответственный за организацию обработки персональных данных
10.	Доступ в помещения, где обрабатываются и хранятся бумажные носители с персональными данными	Положение по защите персональных данных МАДОУ «Детский сад №2» без использования средств автоматизации Список помещений МАДОУ, в которых обрабатываются персональные данные и доступ к ним	ежегодно	Ответственный за организацию обработки персональных данных

Приложение № 2
к Правилам осуществления внутреннего контроля соответствия
обработки персональных данных требованиям к защите персональных данных
в МАДОУ «Детский сад № 2»

Протокол
проведения внутренней проверки условий обработки персональных данных в МАДОУ «Детский сад №2» Пионерского городского округа»

Настоящий Протокол составлен в том, что __.__.20_ ответственным за организацию обработки персональных данных/ комиссией по внутреннему контролю проведена проверка _____.
тема проверки

Проверка осуществлялась в соответствии с требованиями _____
_____.
название документа

В ходе проверки проверено:
_____
_____
_____
_____
_____

Выявленные нарушения:
_____
_____
_____
_____
_____
_____
_____

Меры по устранению нарушений:
_____
_____
_____
_____
_____
_____
_____

Срок устранения нарушений: _____.

Должность ответственного _____ И.О. Фамилия

либо

Председатель комиссии _____ И.О. Фамилия

Члены комиссии:

УТВЕРЖДАЮ
и.е.заведующего Муниципального автономного дошкольного образовательного учреждения «Детский сад № 2» Пионерского городского округа»
_____ Л.Н.спетницкая
«_____»_____ 2017 г.
м.п.

ПРАВИЛА
работы с обезличенными персональными данными
в МАДОУ «Детский сад №2» Пионерского городского округа»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила работы с обезличенными персональными данными в МАДОУ «Детский сад № 2» разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и постановления Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

1.2.Настоящие Правила определяют порядок работы с обезличенными данными МАДОУ «Детский сад №2».

1.3.Настоящие Правила утверждаются заведующей детским садом и действуют постоянно.

2.ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»:

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

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

- обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

3.УСЛОВИЯ ОБЕЗЛИЧИВАНИЯ

3.1.Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных администрации и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

3.2.Способы обезличивания при условии дальнейшей обработки персональных данных:

3.2.1. уменьшение перечня обрабатываемых сведений;

3.2.2. замена части сведений идентификаторами;

3.2.3. обобщение – понижение точности некоторых сведений;

3.2.4. понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, населенного пункта, улицы, дома и квартиры, а может быть указан только город, населенный пункт)

3.2.5. деление сведений на части и обработка в разных информационных системах;

3.2.6. другие способы.

3.3. Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

3.4. Для обезличивания персональных данных годятся любые способы явно не запрещенные законодательно.

3.5. Перечень должностей в МАДОУ «Детский сад №2» (заведующий, делопроизводитель, делопроизводитель, главный бухгалтер) ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных.

3.5.1. Заведующая МАДОУ «Детский сад №2» принимает решение о необходимости обезличивания персональных данных;

3.5.2. Сотрудники МАДОУ «Детский сад №2», непосредственно осуществляющие обработку персональных данных, готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания и совместно с ответственным за организацию обработки персональных данных, осуществляют непосредственное обезличивание выбранным способом.

ОБЯЗАТЕЛЬСТВО
о неразглашении информации, содержащей персональные данные

Я, _____

проживающий по адресу:_____

_____

паспорт _____

предупрежден(а) о том, что на период исполнения мною должностных обязанностей по трудовому договору, заключенному между мною и МАДОУ «Детский сад №2» предусматривающих работу с персональными данными сотрудников МАДОУ «Детский сад №2» мне будет предоставлен доступ к указанной информации.

В соответствии со статьей 7 Федерального закона от 27 июля 2006г № 152-ФЗ «О персональных данных» я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией и я обязан(а):

– не передавать (в любом виде) и не разглашать третьим лицам и работникам, не имеющим на это право в силу выполняемых ими должностных обязанностей или в соответствии с решением руководителя, информацию, содержащую персональные данные сотрудников (граждан) (за исключением собственных данных), которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей;

– в случае попытки третьих лиц или работников, не имеющих на это право, получить от меня информацию, содержащую персональные данные, немедленно сообщать об этом факте своему непосредственному или (в случае отсутствия непосредственного) вышестоящему руководителю;

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

– выполнять требования закона и иных нормативных правовых актов Российской Федерации, а так же внутренних документов МАДОУ «Детский сад № 2», регламентирующих вопросы защиты интересов субъектов персональных данных, порядка обработки и защиты персональных данных;

– после прекращения моих прав на допуск к информации, содержащей персональные данные (переход на должность, не предусматривающую доступ к персональным данным или прекращения Трудового договора), не обрабатывать, не разглашать и не передавать третьим лицам и неуполномоченным на это работникам, известную мне информацию, содержащую персональные данные.

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

_____ /_____ /_____/_____/20__/

УТВЕРЖДЕНО:
и.о.заведующего МАДОУ«Детский сад № 2»
_____Л.Н.спетницкая
«_____» _____ 2017 г.
м.п.

Должностная инструкция
должностного лица, ответственного за организацию обработки персональных данных
**в МАДОУ «Детский сад №2» Пионерского городского округа»

1. Должностное лицо, ответственное за организацию обработки персональных данных должно руководствоваться в своей деятельности Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», нормативными правовыми актами в области защиты персональных данных, настоящей должностной инструкцией.

2. Должностное лицо, ответственное за организацию обработки персональных данных обязано:

- осуществлять внутренний контроль за соблюдением работниками МАДОУ «Детский сад №2» требований законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доводить до сведения работников МАДОУ «Детский сад №2» положения законодательства РФ о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- осуществлять контроль за приемом и обработкой обращений и запросов субъектов персональных данных или их представителей;
- предоставлять субъекту персональных данных по его просьбе информацию;
- разъяснять субъекту персональных данных юридические последствия отказа предоставления его персональных данных;

С инструкцией ознакомлен:
_____ _____ /_____/
_____ _____ /_____/
_____ _____ /_____/
_____ _____ /_____/

ПОЛИТИКА
В МАДОУ «ДЕТСКИЙ САД №2»
ПИОНЕРСКОГО ГОРОДСКОГО ОКРУГА»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Термины и определения

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

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

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

1.2. Назначение и правовая основа документа

Политика МАДОУ «Детский сад №2» определяет систему взглядов на проблему обеспечения безопасности персональных данных и представляет собой систематизированное изложение целей и задач защиты, как одно или несколько правил, процедур, практических приемов и руководящих принципов в области информационной безопасности, которыми руководствуется Администрация в своей деятельности, а также основных принципов построения, организационных, технологических и процедурных аспектов обеспечения безопасности персональных данных.

Законодательной основой настоящей Политики являются Конституция Российской Федерации, Гражданский, Уголовный и Трудовой кодексы, Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», законы, указы, постановления, другие нормативные документы действующего законодательства Российской Федерации.

Использование данной Политики в качестве основы для построения комплексной системы информационной безопасности персональных данных МАДОУ «Детский сад №2» позволит оптимизировать затраты на ее построение.

При разработке Политики учитывались основные принципы создания комплексных систем обеспечения безопасности информации, характеристики и возможности организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам безопасности информации.

Основные положения Политики базируются на качественном осмыслении вопросов безопасности информации и не затрагивают вопросов экономического (количественного) анализа рисков и обоснования необходимых затрат на защиту информации.

2. ОБЪЕКТЫ ЗАЩИТЫ

2.1. Основными объектами системы безопасности персональных данных в МАДОУ являются:

– информационные ресурсы с ограниченным доступом, содержащие персональные данные;

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

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

3. ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Интересы затрагиваемых субъектов информационных отношений. Субъектами информационных отношений при обеспечении безопасности персональных данных МАДОУ являются:

– руководство и сотрудники МАДОУ, в соответствии с возложенными на них функциями.

Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

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

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

– конфиденциальности (сохранения в тайне) персональных данных;

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

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

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

– защиты персональных данных от незаконного распространения.

3.2. Цели защиты

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

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

– доступности персональных данных для легальных пользователей (устойчивого функционирования информационных систем МАДОУ, при котором пользователи имеют возможность получения необходимых персональных данных и результатов решения задач за приемлемое для них время);

– целостности и аутентичности (подтверждение авторства) персональных данных, хранимых и обрабатываемых в информационных системах МАДОУ и передаваемой по каналам связи;

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

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

3.3. Основные задачи системы обеспечения безопасности персональных данных

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

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

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

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

- защиту от вмешательства в процесс функционирования информационных систем МАДОУ посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);

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

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

- защиту от несанкционированной модификации используемых в информационных системах МАДОУ программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;

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

3.4. Основные пути решения задач системы защиты

Поставленные основные цели защиты и решение перечисленных выше задач достигаются:

– строгим учетом всех подлежащих защите ресурсов информационных систем МАДОУ (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);

– журнал действий персонала, осуществляющего обслуживание и модификацию программных и технических средств информационной системы;

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

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

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

– четким знанием и строгим соблюдением всеми пользователями информационных систем МАДОУ требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;

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

– непрерывным поддержанием необходимого уровня защищенности элементов информационной среды МАДОУ;

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

– эффективным контролем над соблюдением пользователями информационных ресурсов МАДОУ требований по обеспечению безопасности информации;

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

4. ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Построение системы, обеспечения безопасности персональных данных МАДОУ, и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- разумная достаточность (экономическая целесообразность);
- персональная ответственность;
- минимизация полномочий;
- исключение конфликта интересов;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- открытость алгоритмов и механизмов защиты;
- простота применения средств защиты;
- обоснованность и техническая реализуемость;
- специализация и профессионализм;
- обязательность контроля.

4.2. Законность

Предполагает осуществление защитных мероприятий и разработку системы безопасности персональных данных МАДОУ в соответствии с действующим законодательством в области защиты персональных данных, а также других законодательных актов по безопасности информации РФ, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с персональными данными. Принятые меры безопасности персональных данных не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством случаях.

Все пользователи информационной системы МАДОУ должны иметь представление об ответственности за правонарушения в области обработки персональных данных.

4.3. Системность

Системный подход к построению системы защиты информации в МАДОУ предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности персональных данных.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места информационных систем МАДОУ, а также характер, возможные объекты и направления атак на нее со стороны нарушителей (особенно высококвалифицированных злоумышленников). Система защиты должна строиться с учетом не только всех известных каналов проникновения и несанкционированного доступа к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

4.4. Комплексность

Комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых

мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами.

4.5. Непрерывность защиты

Обеспечение безопасности персональных данных - процесс, осуществляемый руководством МАДОУ, администратором безопасности информационной системы и сотрудниками всех уровней. Это не только и не столько процедура или политика, которая осуществляется в определенный отрезок времени или совокупность средств защиты, сколько процесс, который должен постоянно идти на всех уровнях внутри МАДОУ и каждый сотрудник должен принимать участие в этом процессе. Деятельность по обеспечению информационной безопасности является составной частью повседневной деятельности. И ее эффективность зависит от участия руководства МАДОУ в обеспечении информационной безопасности персональных данных.

Кроме того, большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных "закладок" и других средств преодоления защиты.

4.6. Своевременность

Предполагает упреждающий характер мер обеспечения безопасности персональных данных, то есть постановку задач по комплексной защите персональных данных и реализацию мер обеспечения безопасности персональных данных на ранних стадиях разработки информационных систем в целом и их систем защиты, в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой информационной системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) системы, обладающие достаточным уровнем защищенности.

4.7. Преемственность и совершенствование

Предполагает постоянное совершенствование мер и средств защиты персональных данных на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем и системы ее защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

4.8. Разумная достаточность (экономическая целесообразность)

Предполагает соответствие уровня затрат на обеспечение безопасности персональных данных ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать эргономические показатели работы компонентов информационных систем МАДОУ. Излишние меры безопасности, помимо экономической неэффективности, приводят к утомлению и раздражению персонала.

Создать абсолютно непреодолимую систему защиты принципиально невозможно. Пока персональные данные находятся в обращении, принимаемые меры могут только снизить вероятность негативных воздействий или ущерб от них, но не исключить их полностью. При достаточном количестве времени и средств возможно преодолеть любую защиту. Поэтому имеет смысл рассматривать некоторый приемлемый уровень обеспечения безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть ресурсов и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми.

4.9. Персональная ответственность

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

4.10. Минимизация полномочий

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

4.11. Исключение конфликта интересов (разделение функций)

Эффективная система обеспечения информационной безопасности предполагает четкое разделение обязанностей сотрудников и исключение ситуаций, когда сфера ответственности сотрудников допускает конфликт интересов. Сферы потенциальных конфликтов должны выявляться, минимизироваться, и находится под строгим независимым контролем. Реализация данного принципа предполагает, что не один сотрудник не должен иметь полномочий, позволяющих ему единолично осуществлять выполнение критичных операций. Наделение сотрудников полномочиями, порождающими конфликт интересов, дает ему возможность подтасовывать информацию в корыстных целях или с тем, чтобы скрыть проблемы или понесенные убытки. Для снижения риска манипулирования персональными данными и риска хищения, такие полномочия должны в максимально возможной степени быть разделены между различными сотрудниками МАДОУ «Детский сад №3» Колокольчик». Необходимо проводить периодические проверки обязанностей, функций и деятельности сотрудников, выполняющих ключевые функции, с тем, чтобы они не имели возможности скрывать совершение неправомерных действий. Кроме того, необходимо принимать специальные меры по недопущению сговора между сотрудниками.

4.12. Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективе МАДОУ. В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие деятельности ответственным за организацию обработки персональных данных.

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

4.13. Гибкость системы защиты

Система обеспечения информационной безопасности должна быть способна реагировать на изменения внешней среды и условий осуществления МАДОУ своей деятельности. В число таких изменений входят:

- изменения организационной и штатной структуры МАДОУ;
- изменение существующих или внедрение принципиально новых информационных систем;
- новые технические средства.

Свойство гибкости системы обеспечения информационной безопасности избавляет в таких ситуациях от необходимости принятия кардинальных мер по полной замене средств и методов защиты на новые, что снижает ее общую стоимость.

4.15. Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Это, однако, не означает, что информация об используемых системах и механизмах защиты должна быть общедоступна.

4.16. Простота применения средств защиты

Механизмы и методы защиты должны быть интуитивно понятны и просты в использовании. Применение средств и методов защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций.

4.17. Обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты персональных данных должны быть реализованы на современном уровне развития науки и техники, обоснованы с точки зрения достижения заданного уровня безопасности информации и экономической целесообразности, а также должны соответствовать установленным нормам и требованиям по безопасности персональных данных.

4.18. Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты персональных данных специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами (ответственными за организацию обработки персональных данных).

4.19. Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил, обеспечения безопасности персональных данных, на основе используемых систем и средств защиты персональных данных, при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

Кроме того, эффективная система обеспечения информационной безопасности требует наличия адекватной и всеобъемлющей информации о текущем состоянии процессов, связанных с движением информации и сведений о соблюдении установленных нормативных требований, а также дополнительной информации, имеющей отношение к принятию решений. Информация должна быть надежной, своевременной, доступной и правильно оформленной.

Недостатки системы обеспечения информационной безопасности, выявленные сотрудниками должны немедленно доводиться до сведения руководителя и оперативно устраняться. Вопросы, которые кажутся незначительными, когда отдельные процессы рассматриваются изолированно, при рассмотрении их наряду с другими аспектами могут указать на отрицательные тенденции, грозящие перерасти в крупные недостатки, если они не будут своевременно устранены.

5. МЕРЫ, МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ТРЕБУЕМОГО УРОВНЯ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ

5.1. Меры обеспечения информационной безопасности

Все меры обеспечения безопасности информационных систем подразделяются на:

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

Законодательные (правовые) меры защиты

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

Морально-этические меры защиты

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в Администрации. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные

акты, однако, их несоблюдение может привести к падению авторитета, престижа человека, группы лиц или МАДОУ в целом. Морально-этические нормы бывают как неписаные, так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективе.

Технологические меры защиты

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

Организационные (административные) меры защиты

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

5.2. Формирование политики безопасности

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

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

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

– каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности персональных данных;

– кто имеет права доступа к персональным данным, кто и при каких условиях может читать и модифицировать персональные данные и т.д.

Политика нижнего уровня должна:

– предусматривать регламент информационных отношений, исключающих возможность произвольных, монопольных или несанкционированных действий в отношении информационных ресурсов;

– определять коалиционные и иерархические принципы и методы разделения секретов и разграничения доступа к персональным данным;

– выбирать программно-технические (аппаратные) средства противодействия НСД, аутентификации, авторизации, идентификации и других защитных механизмов, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

5.3. Регламентация доступа в помещения

Компоненты информационных систем МАДОУ должны размещаться в помещениях, находящихся под охраной или наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении защищаемых ресурсов (документов, АРМ и т.п.). Уборка таких помещений должна производиться в присутствии ответственного сотрудника, за которым закреплены данные компоненты, с соблюдением мер, исключающих доступ посторонних лиц к защищаемым информационным ресурсам.

Во время обработки персональных данных в таких помещениях должен присутствовать только персонал, допущенный к работе с персональными данными. Запрещается прием посетителей в помещениях, когда осуществляется обработка персональных данных.

По окончании рабочего дня, помещения, в которых размещаются компоненты информационных систем МАДОУ, должны запираться на ключ.

В случае оснащения помещений средствами охранной сигнализации, а также автоматизированной системой приема и регистрации сигналов от этих средств, прием-сдача таких помещений под охрану осуществляется на основании специально разрабатываемой инструкции.

5.4. Регламентация допуска сотрудников к использованию информационных ресурсов

В рамках разрешительной системы (матрицы) доступа устанавливается: кто, кому, какую информацию и для какого вида доступа может предоставить и при каких условиях.

Допуск пользователей к работе с информационными системами МАДОУ и доступ к ее ресурсам должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться установленным порядком.

Уровень полномочий каждого пользователя определяется индивидуально, соблюдая следующие требования:

– каждый сотрудник пользуется только предписанными ему правами по отношению к персональным данным, с которыми ему необходима работа в соответствии с должностными обязанностями. Расширение прав доступа и предоставление доступа к дополнительным информационных ресурсам, в обязательном порядке, должно согласовываться с ответственными за организацию обработки персональных данных;

– руководитель МАДОУ имеет права на просмотр информации своих подчиненных только в установленных пределах в соответствии со своими должностными обязанностями.

Все сотрудники МАДОУ и обслуживающий персонал, должны нести персональную ответственность за нарушения установленного порядка обработки персональных данных, правил хранения, использования и передачи находящихся в их распоряжении защищаемых ресурсов системы. Каждый сотрудник (при приеме на работу) должен подписывать обязательство о соблюдении и ответственности за нарушение установленных требований по сохранению персональных данных МАДОУ.

Обработка персональных данных в компонентах информационных систем должна производиться в соответствии с утвержденными технологическими инструкциями.

5.5. Регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов

В целях поддержания режима информационной безопасности аппаратно-программная конфигурация автоматизированных рабочих мест сотрудников, с которых возможен доступ к ресурсам информационной системы, должна соответствовать кругу возложенных на данных пользователей функциональных обязанностей.

В компонентах информационной системы и на рабочих местах пользователей должны устанавливаться и использоваться лицензионные программные средства.

5.6. Обеспечение и контроль физической целостности (неизменности конфигурации) аппаратных ресурсов

Оборудование информационной системы, используемое для доступа и хранения персональных данных, к которому доступ обслуживающего персонала в процессе эксплуатации не требуется, после наладочных, ремонтных и иных работ, связанных с доступом к его компонентам должно закрываться.

5.7. Подбор и подготовка персонала, обучение пользователей

Пользователи информационных систем МАДОУ, а также руководящий и обслуживающий персонал должны быть ознакомлены со своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки персональных данных в МАДОУ.

Обеспечение безопасности персональных данных возможно только после выработки у пользователей определенной культуры работы, т.е. норм, обязательных для исполнения всеми, кто работает с информационными ресурсами МАДОУ. К таким нормам можно отнести запрещение любых умышленных или неумышленных действий, которые нарушают нормальную работу компонентов информационных систем Администрации, вызывают дополнительные затраты ресурсов, нарушают целостность хранимой и обрабатываемой информации, нарушают интересы законных пользователей, владельцев или собственников.

Все пользователи информационных систем МАДОУ должны быть ознакомлены с организационно - распорядительными документами по обеспечению безопасности персональных данных, в части, их касающейся, должны знать и неукоснительно выполнять инструкции и знать общие обязанности по обеспечению безопасности персональных данных. Доведение требований указанных документов до лиц, допущенных к обработке защищаемых персональных данных, должно осуществляться под роспись.

5.8. Ответственность за нарушения установленного порядка пользования ресурсами информационных систем МАДОУ**.**

Мера ответственности персонала за действия, совершенные в нарушение установленных правил обеспечения безопасной работы с персональными данными, должна определяться нанесенным ущербом, наличием злого умысла и другими факторами по усмотрению руководства МАДОУ.

Для реализации принципа персональной ответственности пользователей за свои действия необходимы:

- индивидуальная идентификация пользователей и инициированных ими процессов, т.е. установление за ними идентификатора (login, Username), на базе которого будет осуществляться разграничение доступа в соответствии с принципом обоснованности доступа;
- проверка подлинности пользователей (аутентификация) на основе паролей;
- реакция на попытки несанкционированного доступа (сигнализация, блокировка и т.д.).

5.9. Средства обеспечения безопасности персональных данных

Для обеспечения информационной безопасности МАДОУ используются следующие средства защиты:

- физические средства;
- технические средства;
- средства идентификации и аутентификации пользователей;
- средства разграничения доступа;
- средства обеспечения и контроля целостности;
- средства оперативного контроля и регистрации событий безопасности.

Средства защиты должны применяться ко всем ресурсам информационных систем, независимо от их вида и формы представления информации в них.

5.10. Физические средства защиты

Физические меры защиты основаны на применении разного рода механических, электронных или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемым персональным данным, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Для обеспечения физической безопасности компонентов информационных систем МАДОУ необходимо осуществлять ряд организационных и технических мероприятий, включающих: проверку оборудования, предназначенного для обработки персональных данных, на:

С учетом всех требований и принципов обеспечения безопасности персональных данных по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

- средства разграничения доступа к данным;
- средства регистрации доступа к компонентам информационной системы и контроля за использованием информации;
- средства реагирования на нарушения режима информационной безопасности.

На технические средства защиты возлагается решение следующих основных задач:

- идентификация и аутентификация пользователей при помощи имен или специальных аппаратных средств (Advantor, Touch Memory, Smart Card и т.п.);
- регламентация и управление доступом пользователей в помещения, к физическим и логическим устройствам;
- защита от проникновения компьютерных вирусов и разрушительного воздействия вредоносных программ;
- регистрация всех действий пользователя в защищенном журнале, наличие нескольких уровней регистрации;

– защита данных системы защиты на файловом сервере от доступа пользователей, в чьи должностные обязанности не входит работа с информации, находящейся на нем.

5.11.Средства идентификации и аутентификации пользователей

В целях предотвращения работы с ресурсами информационных систем МАДОУ посторонних лиц необходимо обеспечить возможность распознавания каждого легального пользователя (или групп пользователей). Для идентификации могут применяться различного рода устройства: магнитные карточки, ключи, ключевые вставки, дискеты и т.п.

Аутентификация (подтверждение подлинности) пользователей также может осуществляться:

– путем проверки наличия у пользователей каких-либо специальных устройств (магнитных карточек, ключей, ключевых вставок и т.д.);

– путем проверки знания ими паролей;

– путем проверки уникальных физических характеристик и параметров самих пользователей при помощи специальных биометрических устройств.

5.12. Средства разграничения доступа

Зоны ответственности и задачи конкретных технических средств защиты устанавливаются исходя из их возможностей и эксплуатационных характеристик, описанных в документации на данные средства.

Технические средства разграничения доступа должны по возможности быть составной частью единой системы контроля доступа:

– на контролируемую территорию;

– в отдельные помещения;

– к компонентам информационной среды Администрации и элементам системы защиты персональных данных (физический доступ);

– к информационным ресурсам (документам, носителям информации, файлам, наборам данных, архивам, справкам и т.д.);

– к активным ресурсам (прикладным программам, задачам и т.п.);

– к операционной системе, системным программам и программам защиты.

5.13.Средства обеспечения и контроля целостности

Средства обеспечения целостности включают в свой состав средства резервного копирования, программы антивирусной защиты, программы восстановления целостности операционной среды и баз данных.

Средства контроля целостности информационных ресурсов системы предназначены для своевременного обнаружения модификации или искажения ресурсов системы. Они позволяют обеспечить правильность функционирования системы защиты и целостность хранимой и обрабатываемой информации.

Контроль целостности информации и средств защиты, с целью обеспечения неизменности информационной среды, определяемой предусмотренной технологией обработки, и защиты от несанкционированной модификации персональных данных должен обеспечиваться:

– средствами разграничения доступа (в помещения, к документам, к носителям информации, к серверам, логическим устройствам и т.п.);

– средствами электронной подписи;

– средствами подсчета контрольных сумм (для используемого программного обеспечения).

5.14.Средства оперативного контроля и регистрации событий безопасности

Средства объективного контроля должны обеспечивать обнаружение и регистрацию всех событий (действий пользователей, попыток НСД и т.п.), которые могут повлечь за собой нарушение безопасности и привести к возникновению кризисных ситуаций. Анализ собранной средствами регистрации информации позволяет выявить факты совершения нарушений, их характер, подсказать метод его расследования и способы поиска нарушителя и исправления ситуации. Средства контроля и регистрации должны предоставлять возможности:

– ведения и анализа журналов регистрации событий безопасности (системных журналов);

– получения твердой копии (печати) журнала регистрации событий безопасности;

– упорядочения журналов, а также установления ограничений на срок их хранения;

– оперативного оповещения ответственного за организацию обработки персональных данных о нарушениях.

При регистрации событий безопасности в журнале должна фиксироваться следующая информация:

– дата и время события;
– идентификатор субъекта, осуществляющего регистрируемое действие;
– действие (тип доступа).

5.16. Контроль эффективности системы защиты

Контроль эффективности защиты персональных данных осуществляется с целью своевременного выявления и предотвращения утечки персональных данных за счет несанкционированного доступа, а также предупреждения возможных специальных воздействий, направленных на уничтожение персональных данных, разрушение средств информатизации. Контроль может проводиться привлекаемыми для этой цели организациями, имеющими лицензию на этот вид деятельности.

Оценка эффективности мер защиты персональных данных проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

и.о.заведующему Муниципальным автономным дошкольным образовательным учреждения «Детский сад № 2» Пионерского городского округа»

ЗАЯВЛЕНИЕ-СОГЛАСИЕ
РАБОТНИКА НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я, _____
(Ф.И.О субъекта персональных данных)

зарегистрированный по адресу: _____
документ, удостоверяющий личность (название документа, серия, номер, кем выдан, дата выдачи)_____
_____
именуемый (далее - Субъект персональных данных) даю свое согласие Муниципальному автономному дошкольному общеобразовательному учреждению «Детский сад № 2» Пионерского городского округа (далее – МАДОУ «Детский сад №2», юридический адрес: 238590, г. Пионерский, ул. Комсомольская, д.50 на обработку моих персональных данных с целью:

- обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;
- обеспечения соблюдения законов и иных нормативных правовых актов, исполнения трудового договора, одной стороной которого является субъект персональных данных;
- содействия работнику в осуществлении трудовой деятельности;
- наиболее полного исполнения обязанностей, обязательств и компетенций, определенных должностными инструкциями;
- содействия работникам муниципальной системы образования в обучении, повышении квалификации и должностном росте;
- учета результатов исполнения работником должностных обязанностей;
- ведения уставной деятельности, в том числе пропаганды передового педагогического и методического опыта;
- открытости конкурсного движения;
- презентации деятельности учреждения;
- ведения финансово - хозяйственной деятельности МАДОУ «Детский сад №2»;
- формирования и ведения делопроизводства и документооборота, в том числе в электронном виде.

1. Мои персональные данные, в отношении которых я даю свое согласие.

Общая информация:

Фамилия, имя, отчество
Дата и место рождения
Адрес места жительства
Адрес регистрации
Паспортные данные
Контактная информация
Данные об образовании (какое образовательное учреждение закончил, дата окончания учебы, серия и номер документа об образовании, специальность по диплому)
Послевузовское профессиональное образование (период обучения в аспирантуре)
Профессия, Должность
Квалификационная категория
Дата получения (подтверждения) категории
Дата окончания последних курсов повышения квалификации
Информация о курсах повышения квалификации в межкурсовой период

Информацию по повышению квалификации и переподготовке сотрудника, его аттестация, Служебное расследование.

Общий стаж,

Педагогический стаж

Стаж работы в данном образовательном учреждении

Вид работы (основная или совместительство)

Наличие ведомственных наград и грамот

Информация об участии в конкурсах

Доходы с предыдущего места работы

Сведения о наградах (поощрениях) и почетных званиях

Информация медицинского характера, в случаях, предусмотренных законодательством

Информация, содержащаяся в трудовой книжке работника

Содержание трудового договора

Подлинники и копии приказов по личному составу

Основания к приказам по личному составу

Сведения о наличии судимостей

Сведения о предоставлении субъекту ежегодных, учебных отпусках, отпусках без сохранения заработной платы и др.

Сведения, содержащиеся в документах воинского учета для военнообязанных и лиц, подлежащих призыву на военную службу

ИНН

Информация, содержащаяся в страховом свидетельстве государственного пенсионного страхования. (СНИЛС)

Номера зарплатных (банковских) счетов

Сведения о заработной плате работника

Сведения о социальных льготах

Сведения о семейном положении работника

Данные о детях сотрудников(дата рождения и место обучения)

Биометрические данные:

Фотоматериалы

Аудио-, видеоматериалы

Пол

2. Перечень действий с персональными данными в отношении которых даю свое согласие включает:

- обработку персональных данных (смешанным способом с использованием средств информатизации и/или без использования таких средств),

- сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование (в том числе передачу), блокирование, уничтожение персональных данных (в соответствии с положениями Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

Подтверждаю свое согласие на передачу моих персональных данных третьим лицам с правом обмена информацией с другими организациями в соответствии с действующим законодательством Российской Федерации.

Настоящее согласие действует с момента подписания и до прекращения трудовых и /или и иных договорных отношений. Согласие может быть отозвано мной в письменной форме в любое время. При этом учреждение хранит персональные данные в течение срока хранения документов установленного архивным делопроизводством, а в случаях, предусмотренных законодательством, передает уполномоченным на то органам.

Подтверждаю, что ознакомлен (а) с положениями Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных», права и обязанности в области защиты персональных данных мне разъяснены.

«____»_____20____ г. _____ _____

/подпись/ /Ф.И.О./

Форма разъяснения
субъекту персональных данных юридических последствий отказа предоставить свои персональные данные

Мне, _____
разъяснены юридические последствия отказа предоставить свои персональные данные в МАДОУ «Детский сад №3» «Колокольчик».

В соответствии со статьями 57, 65 Трудового кодекса Российской Федерации субъект персональных данных, поступающий на работу или работающий в МАДОУ «Детский сад №2», обязан представить определенный перечень информации о себе.

Без предоставления субъектом персональных данных обязательных для заключения трудового договора сведений, трудовой договор не может быть заключен.

На основании пункта 11 части 1 статьи 77 Трудового кодекса Российской Федерации трудовой договор прекращается вследствие нарушения установленных обязательных правил его заключения, если это нарушение исключает возможность продолжения работы.

«____»_____ _____
дата подпись

Лист ознакомления
работника МАДОУ «Детский сад № 2», непосредственно осуществляющего обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных
(в том числе с требованиями к защите персональных данных

Я, _____

(фамилия, имя, отчество)

_____

(должность)

ознакомлен(а) с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами по вопросам обработки персональных данных.

Мною изучены положения Федерального закона от 27 июля 2006г № 152-ФЗ «О персональных данных», Трудового кодекса Российской Федерации, Постановления Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», Постановления Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», Постановления Правительства Российской Федерации от 21 марта 2012 г. № 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», Приказа Федеральной службы по техническому и экспортному контролю от 05 февраля 2010 г. № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных» и локальные акты МАДОУ «Детский сад №2», определяющие политику в отношении обработки персональных данных.

Я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставших известных мне в связи с исполнением должностных обязанностей.

Ответственность и права, предусмотренные Федеральным законом от 27 июля 2006г № 152-ФЗ «О персональных данных» и другими федеральными законами, мне разъяснены.

____ _____ 20 ____ г _____ _____

(дата) (подпись) (расшифровка подписи)

ЖУРНАЛ

инструктажа сотрудников МАДОУ «Детский сад №2»,

имеющих доступ к персональным данным в соответствии с настоящим постановлением

Срок хранения: 3 года

Начат «___» _____ 20__г.

Окончен «___»_____20__ г.

На _____ листах

2017 г.

№	Организационно-распорядительные документы по защите персональных данных	ФИО Ответственного	ФИО инструктируемого	Подпись инструктируемого и дата

МЕТОДИКА
проведения классификации информационных систем персональных данных в МАДОУ «Детский сад №2»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данный документ применяется для проведения классификации информационных систем персональных данных (далее - ИСПДн) МАДОУ «Детский сад №2».

1.2. Для проведения классификации ИСПДн в МАДОУ «Детский сад №2» распоряжением заведующей назначается комиссия из числа штатных сотрудников.

1.3. Порядок проведения классификации и параметры ИСПДн приведены в «Порядке проведения классификации ИСПДн», который утвержден совместным приказом ФСТЭК/ФСБ/МИТС России от 13.02.2008г. № 55/86/20.

2. ИСХОДНЫЕ ДАННЫЕ ОБ ИСПДН

1.1. Общие данные

При обработке персональных данных (ПДн) в ИСПДн в МАДОУ «Детский сад №2» является оператором персональных данных (ПДн) физических лиц, юридических лиц.

Цели и условия обработки, состав ПДн определяются Федеральным законодательством, законами Калининградской области, локальными актами МАДОУ «Детский сад №2» и другими нормативно-правовыми актами.

1.2. Описание ИСПДн

ИСПДн «АИС СП» состоит из 6 АРМ, входящих в состав общей ЛВС МАДОУ «Детский сад №3» «Колокольчик».

Они расположены на первом этаже двухэтажного административного здания в кабинете заведующего (1 АРМ), в кабинете старшего воспитателя (2 АРМ), в кабинете главного бухгалтера (3 АРМ) в помещении в групповой детской комнате «Теремок» Интернет организован через модем, на втором этаже двухэтажного административного здания в помещении групповых детских комнатах «Гномики» (4 АРМ), «Игрушки» (5 АРМ).

Административное здание МАДОУ «Детский сад №2» находится по адресу: Калининградская область, г. Пионерский, ул. Шаманова,д.5а.