Центр развития ребенка – детский сад №14 «Родничок»» г. Лениногорска муниципального образования «Лениногорский муниципальный район» Республики Татарстан

Номер документа	Дата составления
215	02.10.2017 г.

ПРИКАЗ

Об утверждении документов по организации работы по защите перональных данных в МБДОУ «ЦРР- детский сад №14».

В соответствии с федеральным законом «О защиете персональных данных» от 27.07.2006г №152-ФЗ, Постановлением Правительства РФ от 15.09.2008г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации» и Политикой МБДОУ «ЦРР- детский сад №14» в отношении обработки персональных данных приказываю:

П.1. Утвердить Должностную инструкцию ответственного лица по организации обработки и защиты персональных данных работников, воспитанников (обучающихся) и родителей (законных представителей) воспитанникв МБДОУ «ЦРР- детский сад №14» г. Лениногорска МО «ЛМР» РТ.

П.2. Утвердить Инструкцию о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные.

П.3.Утвердить Инструкцию по организации парольной защиты.

П.4.Утвердить требования к оборудованию помещений и размещение технических средств, используемых для обработки персональных данных в МБДОУ «ЦРР- детский сад №14» г. Лениногорска МО «ЛМР» РТ.

П.5. Утвердить форму акта об уничтожении персональных данных.

П.6. Поместить на сайт ДОУ вышеперечисленные документы.

П.7. Познакомить под подпись с выше перечисленными документами ответственных за зашиту персональных данных работников ДОУ.

П.8. Довести до сведения всех работников ДОУ выше перечисленные документы по защите персональных данных в МБДОУ «ЦРР- детский сад №14»

П. 9 Контроль за исполнением приказа оставляю за собой.

Заведующая МБДОУ «ЦРР -детский сад№14»_____Н.И. Загородская

С приказом ознакомлены:

Ибайс (Ибай И.С.) 02.10.2017 г.
Вал (В.А. Павлина) 02.10.2017 г.
Фаза (К.В. Фазлиева) 02.10.2017

Инструкция ответственного лица по организации обработки и защиты персональных данных работников, воспитанников и родителей (законных представителей) воспитанников МБДОУ «Центр развития ребенка - детский сад №14 «Родничок»» г. Лениногорска МО «ЛМР» РТ

Утверждаю:

заведующий МБДОУ «ЦРР - детский сад № 14»

_____Н.И. Загородская

Приказ от 02.10.2017г. № 215

Должностная инструкция
ответственного лица по организации обработки и защиты персональных данных работников, воспитанников (обучающихся) и родителей (законных представителей) воспитанников МБДОУ «ЦРР - детский сад № 14»г. Лениногорска МО «ЛМР» РТ.

1. Общие положения

1.1. Настоящая Инструкция муниципального бюджетного дошкольного образовательного учреждения «Центр развития ребенка - детский сад № 14» г. Лениногорска муниципального образования «Лениногорский муниципальный район» Татарстан (далее - ДОУ) разработана в соответствии с Трудовым кодексом Российской Федерации, Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом «Об информации, информационных технологиях и о защите информации», Федеральным законом «О персональных данных», Постановлением Правительства Российской Федерации от 15 сентября 2008 г. N 687 г. «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»; Постановлении Правительства РФ от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»; Правилами внутреннего трудового распорядка МБДОУ, Положениями о персональных данных работников, воспитанников (обучающихся) и родителей (законных представителей) воспитанников МБДОУ «ЦРР - детский сад № 14» (далее – Положение).
1.2. Цель разработки Инструкции - обеспечение защиты прав и свобод работников, воспитанников (обучающихся) и родителей (законных представителей) воспитанников (обучающихся) ДОУ при обработке их персональных данных, а также установление ответственности

должностных лиц, имеющих доступ к персональным данным граждан, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. Порядок ввода в действие и изменения Инструкции.

1.3.1. Настоящая Инструкция вступает в силу с момента ее утверждения заведующей ДОУ и действует бессрочно, до замены ее новой Инструкцией.

1.3.2. Все изменения в Инструкцию вносятся приказом.

1.5. Ответственные лица должны быть ознакомлены с настоящей Инструкцией под роспись.

1.6. Персональную ответственность за соблюдение всеми ответственными лицами настоящей инструкции, а также контроль за ее соблюдением возложен на заведующего ДОУ.

2. Основные понятия и состав персональных данных.

2.1. Для целей настоящей Инструкции используются следующие **основные понятия**:

- **персональные данные** - любая информация, относящаяся к определенному или определяемому на основании такой информации работнику, воспитаннику (обучающемуся) или родителю (законному представителю) воспитанника (обучающегося) ДОУ;
- **обработка персональных данных** - сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование и уничтожение персональных данных;
- **конфиденциальность персональных данных** - обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным работников, воспитанников (обучающихся) и родителей (законных представителей) воспитанников (обучающихся) ДОУ;
- требование не допускать их распространения без согласия работников и родителей (законных представителей) воспитанников (обучающихся) или иного законного основания;
- **распространение персональных данных** - действия, направленные на передачу персональных данных работников, воспитанников (обучающихся) и родителей (законных представителей) воспитанников (обучающихся) ДОУ определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных работников, воспитанников (обучающихся) и родителей (законных представителей) воспитанников (обучающихся) ДОУ; в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным работников, воспитанников (обучающихся) и родителей (законных представителей) воспитанников (обучающихся) ДОУ каким-либо иным способом;

- **использование персональных данных** - действия (операции) с персональными данными, совершаемые должностным лицом ДОУ в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении граждан либо иным образом затрагивающих их права и свободы или права и свободы других лиц;
- **блокирование персональных данных** - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;
- **уничтожение персональных данных** - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных граждан или в результате которых уничтожаются материальные носители персональных данных граждан;
- **обезличивание персональных данных** - действия, в результате которых невозможно определить принадлежность персональных данных конкретному гражданину;
- **общедоступные персональные данные** - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия гражданина или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;
- **информация** - сведения (сообщения, данные) независимо от формы их представления.
- **документированная информация** - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.
- **ИСПДн** - Информационные системы персональных данных;

2.2. Состав персональных данных

- фамилия, имя, отчество;
- дата и место рождения;
- паспортные данные;
- сведения об ИНН, СНИЛС;
- адрес проживания (регистрации);
- домашний, контактный телефон;
- семейное, социальное, имущественное положение;
- образование;
- профессия, специальность, занимаемая должность;
- автобиография;
- сведения о трудовом и общем стаже;
- сведения о предыдущем месте работы;
- сведения о воинском учете;
- сведения о социальных льготах;
- размер заработной платы;

- наличие судимостей, ответственности по исполнительному листу;
- содержание трудового договора;
- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
- привычки и увлечения, в том числе вредные (алкоголь, наркотики и др.);
- реквизиты счёта банковской карты;
- семейное положение;
- прочие сведения, которые могут идентифицировать человека.

2.3. У администрации ДОУ создаются и хранятся следующие **группы документов**, содержащие данные о работниках, воспитанниках (обучающихся) и родителях (законных представителях) воспитанников (обучающихся) ДОУ в единичном или сводном виде:

- Документы, содержащие персональные данные работников: комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплекс материалов по анкетированию, тестированию; проведению собеседований с кандидатом на должность; подлинники и копии приказов по личному составу; личные дела работников, трудовые книжки работников; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации работников; дела, содержащие материалы служебных расследований; справочно-информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Учреждения, копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения.

3. Права работников и родителей (законных представителей) воспитанников ДОУ.

3.2. Работники и родители (законные представители) воспитанников ДОУ имеют право:

3.2.1.Получать доступ к своим персональным данным и ознакомление с ними, включая право на безвозмездное получение копий любой записи, содержащей персональные данные.

3.2.2.Требовать от ДОУ уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющих необходимыми для ДОУ персональных данных.

3.2.3. Получать от ДОУ

- 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.

3.2.4. Требовать извещения ДОУ всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.
3.2.5.Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия ДОУ при обработке и защите его персональных данных.
3.3. Копировать и делать выписки персональных данных граждан разрешается исключительно в служебных целях с письменного разрешения заведующей.

4. Порядок обработки персональных данных.

4.1. При обработке персональных данных граждан, т.е. их получении, хранении, комбинировании, передаче или любом другом использовании, сотрудники, назначенные ответственными за обработку персональных данных граждан обязаны соблюдать следующие общие требования:
4.1.1. Обрабатывать персональные данные граждан исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия гражданам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;
4.1.2. Не допускается запрашивать информацию о состоянии здоровья гражданина, за исключением тех сведений, которые относятся к вопросу о возможности выполнения трудовой функции, посещения ДОУ;
4.1.3. Ответственному лицу разрешается доступ только к тем персональным данным сотрудников, которые необходимы для выполнения им его должностных обязанностей;
4.1.4. Ответственное лицо не имеет права получать и обрабатывать персональные данные гражданина о его политических, религиозных и иных убеждениях, частной жизни, членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, непосредственно связанных с вопросами трудовых отношений с письменного согласия гражданина, а также случаев предусмотренных федеральным законом.

4.2. Порядок получения персональных данных

4.2.1. Персональные данные работника и родителя (законного представителя) воспитанника (обучающегося) ДОУ следует получать у него самого, с его письменного согласия.

4.2.2. Согласие работников и родителей (законных представителей) воспитанников (обучающихся) ДОУ не требуется в следующих случаях:

- персональные данные являются общедоступными;
- обработка персональных данных осуществляется на основании Трудового кодекса РФ или иного федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия работодателя;
- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- обработка персональных данных осуществляется в целях исполнения трудового договора;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов работников, воспитанников (обучающихся) и родителей (законных представителей) воспитанников (обучающихся) ДОУ, если получение его согласия невозможно.

4.2.3. Если персональные данные работника и родителя (законного представителя) воспитанника (обучающегося) ДОУ возможно получить только у третьей стороны, то работник и родитель (законный представитель) воспитанника (обучающегося) ДОУ должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Ответственный должен сообщить работнику и родителю (законному представителю) воспитанника (обучающегося) ДОУ о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.
4.2.4.Все персональные данные воспитанников (обучающихся) следует получать от родителей (законных представителей) воспитанников (обучающихся) .
4.2.5. Работники, родители (законные представители) воспитанников (обучающихся) ДОУ предоставляют ответственному за обработку и защиту персональных данных, достоверные сведения о себе и воспитаннике. Ответственный за обработку и защиту персональных данных проверяет достоверность сведений, сверяя данные, предоставленные работниками и родителями (законными представителями) воспитанников ДОУ, с имеющимися у работников и родителей (законных представителей) воспитанников (обучающихся) ДОУ документами.

5. Хранение персональных данных.

5.1. Персональные данные граждан могут передаваться на хранение на бумажных носителях и в электронном виде - локальной компьютерной сети и

компьютерной программе
5.1. Персональные данные граждан хранятся у администрации ДОУ.
5.2. Хранение документов, содержащих персональные данные, осуществляется в несгораемых шкафах (сейфах), ключи от которых находятся у заведующей ДОУ, а в его отсутствие у лица его замещающего.

6. Передача персональных данных.

При передаче персональных данных необходимо соблюдать следующие требования:
6.1. Не сообщать персональные данные третьей стороне без письменного согласия гражданина, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью гражданина, а также в случаях, установленных федеральным законом;
6.2. Не сообщать персональные данные в коммерческих целях без письменного согласия гражданина. Обработка персональных данных граждан в целях продвижения работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с его предварительного согласия.
6.3. При передаче персональных данных граждан предупредить лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены. Лицо, получившее персональные данные гражданина, обязан соблюдать режим секретности (конфиденциальности).
6.4. Ответственный за сбор и обработку персональных данных, должен осуществлять передачу персональных данных граждан в пределах ДОУ в соответствии с Положением.

7. Защита персональных данных

7.1. Обеспечение безопасности персональных данных в соответствии с российским законодательством не требуется:

- Для обезличенных персональных данных. Персональные данные могут быть обезличенными, в случае, если над ними были произведены действия, в результате которых невозможно определить их принадлежность конкретному работнику, воспитаннику и/или родителю (законному представителю) воспитанника ДОУ.
- Для общедоступных персональных данных. Персональные данные могут быть общедоступными только с письменного согласия работника и родителя (законного представителя) воспитанника ДОУ. Они могут включать фамилию, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные работником и/или родителем (законным представителем) воспитанника (обучающегося) ДОУ.

7.2. Обязанность по обеспечению безопасности персональных данных при их обработке полностью возлагается на ответственного за обработку и защиту персональных данных.
7.3.Право доступа к персональным данным имеют только ответственные лица, назначенные приказом заведующей:

- заведующий ДОУ;
- старший воспитатель;
- ответственный за функционирование сайта ДОУ;
- старшая медицинская сестра;
- делопроизводитель (при наличии);

7.4. Обработка персональных данных должна проводиться в следующих предназначенных для этого помещениях ДОУ:

- кабинет заведующей;
- методический кабинет;
- медицинский кабинет.

7.5. При обработке персональных данных в помещении не должны находиться посторонние лица.
7.6. Ответственные лица должны соблюдать конфиденциальность при обработке персональных данных.
7.7. Ответственные работники должны быть предупреждены о мерах ответственности за разглашение сведений о персональных данных под роспись.
7.8. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.
7.9. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.
7.10. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.
7.11. Обеспечение безопасности персональных данных при их обработке в ИСПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование и распространение персональных данных.

7.12.Ответственный обязан:

- проводить мероприятия, направленные на предотвращение несанкционированного доступа (далее НСД) к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- Соблюдать требования парольной защиты (длина пароля должна быть не менее 6 символов; пароль не должен включать в себя легко вычисляемые сочетания символов, а также общепринятые сокращения; при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях; ответственный не имеет права сообщать пароль постороннему лицу; полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу, другие обстоятельства) ответственных за обработку и защиту персональных данных и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ПК ДОУ); хранение паролей на бумажном носителе допускается только в сейфе у руководителя учреждения);
- своевременно обнаруживать факты НСД к персональным данным;
- обеспечивать оптимальный уровень антивирусной защиты ИСПДн;
- незамедлительно восстанавливать персональные данные, модифицированные или уничтоженные вследствие несанкционированного доступа к ним;
- осуществлять постоянный контроль за обеспечением уровня защищенности персональных данных;
- обеспечивать резервное копирование персональных данных на отчуждаемые носители информации;

8. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

Ответственные ДОУ, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных граждан, несут административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами

С инструкцией ознакомлены:

Вал /В.А. Павлинв/ 02.10.2018г

УТВЕРЖДАЮ:
Заведующий
МБДОУ «ЦРР - детский сад № 14»
г. Лениногорска МО «ЛМР» РТ
_____Н.И. Загородская
Приказ №215 от 02.10. 2017 г.

Инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные

1. Общие положения

1.1. Инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные (далее – Инструкция), является обязательной для всех структурных подразделений дошкольного образовательного учреждения (далее – ДОУ).

1.2. Под персональными данными понимается любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в т. ч. его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное и имущественное положение, образование, профессия, доходы и др.

1.3. Обеспечение конфиденциальности персональных данных не требуется в случае обезличивания персональных данных, а также в отношении общедоступных персональных данных. В общедоступные источники персональных данных (в т. ч. справочники, адресные книги) в целях информационного обеспечения с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес и другие сведения.

1.4. Конфиденциальность персональных данных предусматривает обязательное получение согласия субъекта персональных данных (наличие иного законного основания) на их обработку.

Согласие не требуется на обработку данных:

- необходимых для доставки почтовых отправлений организациями почтовой связи;
- включающих в себя только фамилию, имя и отчество субъекта;
- данных, работа с которыми проводится в целях исполнения обращения (запроса) субъекта персональных данных, трудового или иного договора с ним, однократного пропуска в здание или в иных аналогичных целях;
- обработка которых осуществляется без средств автоматизации.

1.5. Порядок ведения перечней персональных данных в структурных подразделениях ДОУ утверждается локальным актом. Осуществлять обработку и хранение конфиденциальных данных, не внесенных в перечень, запрещается.

1.6. Все работники, постоянно работающие в помещениях, в которых ведется обработка персональных данных, должны иметь допуск (разрешение) к работе с соответствующими видами персональных данных.

1.7. Работникам, осуществляющим обработку персональных данных, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью, а также оставлять материальные носители с персональными данными без присмотра в незапертом помещении. После подготовки и передачи документа в соответствии с резолюцией файлы черновиков и вариантов документа должны переноситься подготовившим их работником на маркированные носители, предназначенные для хранения персональных данных. Без согласования с руководителем структурного подразделения формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих конфиденциальные данные, запрещается.

1.8. Передача персональных данных допускается только в случаях, установленных Федеральными законами от 27.07.2006 № 152-ФЗ "О персональных данных" и от 02.05.2006 № 59-ФЗ "О порядке рассмотрения обращений граждан Российской Федерации", действующими инструкциями по работе со служебными документами и обращениями граждан, а также по письменному поручению (резолюции) вышестоящих должностных лиц.

1.9. Запрещается передача персональных данных по телефону, факсу, электронной почте за исключением случаев, установленных законодательством РФ и действующими инструкциями по работе со служебными документами и обращениями граждан. Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать конфиденциальные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках.

1.10. Ответственность за защиту обрабатываемых персональных данных возлагается на работников подразделений ДОУ, осуществляющих такую обработку по договору с оператором, а также на иные лица, осуществляющие обработку или хранение конфиденциальных данных в ДОУ. Лица, виновные в нарушении норм, регулирующих обработку и хранение конфиденциальных данных, несут дисциплинарную, административную и уголовную ответственность в соответствии с законодательством и ведомственными нормативными актами.

2. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемых без использования средств автоматизации

2.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна быть организована таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения материальных носителей персональных данных и установить перечень лиц, осуществляющих обработку.

2.2. При хранении материальных носителей необходимо соблюдать условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах выполнения такой обработки.

2.3. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях. При фиксации персональных данных на материальных носителях не допускается на одном материальном носителе размещать персональные данные, цели обработки которых заведомо не совместимы. Для обработки персональных данных каждой категории должен использоваться отдельный материальный носитель.

2.4. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, и невозможности обработки одних персональных данных отдельно от других, зафиксированных на том же носителе, должны быть приняты меры по обеспечению раздельной обработки персональных данных, исключающие одновременное копирование иных персональных данных, не подлежащих распространению и использованию.

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

3. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемых с использованием средств автоматизации

3.1. Безопасность персональных данных при их обработке в информационных системах, хранении и пересылке обеспечивается с помощью системы защиты персональных данных, включающей специальные средства защиты информации, а также используемые в информационной системе информационные технологии.

3.2. Допуск лиц к обработке персональных данных в информационных системах осуществляется на основании соответствующих разрешительных документов и ключей (паролей) доступа.

3.3. Работа с информационными системами должна быть организована таким образом, чтобы обеспечить сохранность носителей персональных данных и средств защиты информации, а также исключить возможность неконтролируемого пребывания в помещениях, где они находятся, посторонних лиц.

3.4. Компьютеры и (или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, состоящими из шести и более символов.

3.5. Работа на компьютерах с персональными данными без паролей доступа или под чужими или общими (одинаковыми) паролями, а также пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в т. ч. сети Интернет, запрещается.

3.6. При обработке персональных данных в информационных системах пользователями должно быть обеспечено:

- использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;
- недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- недопущение несанкционированного выноса из помещений, установки и подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

3.7. При обработке персональных данных в информационных системах разработчики и администраторы систем должны обеспечивать:

- обучение лиц, использующих средства защиты информации применяемые в информационных системах, правилам работы с ними;
- учет лиц, допущенных к работе с персональными данными в информационных системах, прав и паролей доступа;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;
- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- описание системы защиты персональных данных.

3.8. Специфические требования к защите персональных данных в отдельных автоматизированных системах устанавливаются инструкциями по их использованию и эксплуатации.

3.9. Работники подразделений ДОУ и лица, выполняющие работы по договорам и контрактам, имеющие отношение к обработке персональных данных, должны быть ознакомлены с Инструкцией под расписку.

Ознакомлены:

УТВЕРЖДАЮ:
Заведующий
МБДОУ «ЦРР - детский сад № 14»
г. Лениногорска МО «ЛМР» РТ
_____Н.И. Загородская
Приказ № №215 от 02.10. 2017

Инструкция по организации парольной защиты

1. Общие положения

1.1. Инструкция по организации парольной защиты (далее – Инструкция) призвана регламентировать организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах дошкольного образовательного учреждения (далее – ДОУ), а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

1.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах информационной системы (далее – ИС) ДОУ и контроль за действиями исполнителей и обслуживающего персонала при работе с паролями возлагается на системного администратора ДОУ.

2. Правила формирования паролей

2.1. Личные пароли генерируются и распределяются централизованно либо выбираются пользователями информационной системы самостоятельно с учетом следующих требований:

- пароль должен состоять не менее чем из восьми символов;
- в пароле обязательно должны присутствовать буквы из верхнего и нижнего регистров, цифры и специальные символы (@, #, $, &, *, % и т. п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т. д.), последовательности символов и знаков (111, qwerty, abcd и т. д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т. п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетания букв и знаков, которые можно угадать, основываясь на информации о пользователе;
- при смене пароля новый пароль должен отличаться от старого не менее чем

- в шести позициях.

2.2. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на уполномоченных сотрудников центра дистанционного образования.

2.3. При технологической необходимости использования имен и паролей некоторых работников (исполнителей) в их отсутствие (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т. п.) такие работники обязаны сразу же после смены своих паролей их новые значения (вместе с именами своих учетных записей) в запечатанном конверте или опечатанном пенале передать на хранение ответственному за информационную безопасность подразделения (руководителю своего подразделения). Опечатанные конверты (пеналы) с паролями исполнителей должны храниться в сейфе. Для их опечатывания рекомендуется использовать печать отдела кадров.

3. Ввод пароля

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

4. Порядок смены личных паролей

4.1. Смена паролей проводится регулярно, не реже одного раза в три месяца.

4.2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т. п.) системный администратор должен немедленно удалить его учетную запись сразу после окончания последнего сеанса работы данного пользователя с системой.

4.3. Срочная (внеплановая) полная смена паролей производится в случае прекращения полномочий (увольнение, переход на другую работу и т. п.) администраторов информационной системы и других работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

4.4. Смена пароля производится самостоятельно каждым пользователем в соответствии с п. 2.1 Инструкции и/или в соответствии с указанием в системном баннере-предупреждении (при наличии технической возможности).

4.5. Временный пароль, заданный системным администратором при регистрации нового пользователя, следует изменить при первом входе в систему.

5. Хранение пароля

5.1. Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе либо в сейфе у системного администратора или руководителя подразделения в опечатанном пенале.
5.2. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации.
5.3. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

6. Действия в случае утери и компрометации пароля

В случае утери или компрометации пароля пользователя должны быть немедленно предприняты меры в соответствии с п. 4.3 или п. 4.4 Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

7. Ответственность при организации парольной защиты

7.1. Владельцы паролей должны быть ознакомлены под расписку с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение информации о пароле.
7.2. Ответственность за организацию парольной защиты в структурных подразделениях ДОУ возлагается на системного администратора.
7.3. Работники ДОУ и лица, имеющие отношение к обработке персональных данных в информационных системах ДОУ, должны быть ознакомлены с Инструкцией под расписку.

Ознакомлены:

2.10.17 Фомичева К.В.
(число, год, роспись, расшифровка)

2.10.17г. Бабанина В.Д.
(число, год, роспись, расшифровка)

(число, год, роспись, расшифровка)

(число, год, роспись, расшифровка)

(число, год, роспись, расшифровка)

(число, год, роспись, расшифровка)

(число, год, роспись, расшифровка)

(число, год, роспись, расшифровка)

(число, год, роспись, расшифровка)

УТВЕРЖДАЮ:
Заведующий
МБДОУ «ЦРР-детский сад № 14»
г. Лениногорска МО «ЛМР» РТ
_____Н.И. Загородская
Приказ №215 от 02.10.2017 г.

Требования
к оборудованию помещений и размещению технических средств, используемых для обработки персональных данных
в муниципальном бюджетном дошкольном образовательном учреждении «Центр развития ребенкам- детский сад №14» г. Лениногорска муниципального образования «Лениногорский муниципальный район» Республики Татарстан

- Настоящие Требования определяют порядок оборудования выделенных помещений и условия размещения в них технических средств (персональных компьютеров, серверов и т.п.), используемых для обработки персональных данных в организации.
- Расположение выделенных помещений и размещаемых в них технических средств должно исключать возможность бесконтрольного проникновения в эти зоны посторонних лиц и гарантировать сохранность находящихся в них конфиденциальных документов, содержащих персональные данные.
- Размещение оборудования и технических средств, предназначенных для обработки персональных данных, должно соответствовать требованиям техники безопасности, санитарным нормам, а также требованиям пожарной безопасности.
- Внутренняя планировка и расположение рабочих мест в выделенных помещениях должны обеспечивать исполнителям сохранность доверенных им конфиденциальных документов и сведений, содержащих персональные данные.
- Входные двери выделенных помещений должны быть оборудованы замками, гарантирующими санкционированный доступ в них в нерабочее время.
- В выделенные помещения по утвержденному списку допускаются руководство организации, и иные уполномоченные лица и исполнители, имеющие прямое отношение к приему, обработке и передаче персональных данных.

- Допуск в выделенные помещения вспомогательного и обслуживающего персонала (уборщицы, электромонтеры, сантехники и т.д.) производится только при служебной необходимости и в сопровождении ответственного за помещение, при этом необходимо принять меры, исключающие визуальный просмотр конфиденциальных документов, содержащих персональные данные.
- По окончании рабочего дня выделенные помещения необходимо закрывать .
- Сдачу ключей и выделенных помещений , а также получение ключей и вскрытие выделенных помещений имеют право производить только сотрудники, работающие в этих помещениях и внесенные в утвержденный руководством организации список .
- Перед вскрытием выделенных помещений должна быть проверена исправность замков. При обнаружении нарушения повреждения замков или других признаков, указывающих на возможное проникновение в эти помещения посторонних лиц, помещение не вскрывается, а о случившемся немедленно информируется руководитель
- В выделенных помещениях, где установлены средства защиты информации от утечки по техническим каналам, запрещается приносить и использовать радиотелефоны/сотовые телефоны и другую радиоаппаратуру.
- На случай пожара, аварии или стихийного бедствия должны быть разработаны специальные инструкции, утвержденные руководителем, в которых предусматривается вскрытие выделенных помещений, очередность и порядок спасения конфиденциальных документов, содержащих персональные данные, и дальнейшего их хранения.

Приложение к приказу № 215 от 02.10.2017г.

УТВЕРЖДАЮ
Заведующая МБДОУ « ЦРР - детский сад №14»
_____Н.И. Загородская

«__» _____ 201 г.

Акт
об уничтожении персональных данных

Комиссия в составе:
Председатель:
Члены комиссии –
провела отбор носителей персональных данных и установила, что в соответствии с требованиями руководящих документов по защите информации по МБДОУ «ЦРР- детский сад №14» информация, записанная на них в процессе эксплуатации, подлежит гарантированному уничтожению:

№ п\п	Дата	Тип носителя	Регистрационный номер носителя ПДн	Примечание

Всего съемных носителей _____
(цифрами и прописью)
На указанных носителях персональные данные уничтожены путем
_____
(стирания на устройстве гарантированного уничтожения информации и т.п.)
Перечисленные носители ПДн уничтожены путем
_разрезания_____
(разрезания, сжигания, механического уничтожения и т.п.)

Председатель комиссии: _____/_____./
Члены комиссии: _____/ _____./
_____/ ._____/