ПРИНЯТО
на Общем собрании работников
МДОБУ «Детский сад № 25»
Протокол № 4 от «23» декабря2021 г.

МНЕНИЕ
Профсоюзного комитета учтено
Протокол № 10 от «23 » декабря 2021 г.

УТВЕРЖДЕНО
Заведующий МДОБУ "Детский сад № 25"
Приказ № 01-07/149 от «23 »декабря 2021г.
_____ Л.В. Лапина

Лапина Л.В. Заведующий МДОБУ Детский сад №25
Подписано цифровой подписью: Лапина Л.В. Заведующий МДОБУ Детский сад №25
Дата: 2022.06.21 15:19:32 +05'00'

ПОЛОЖЕНИЕ
об обработке и защите персональных данных работников муниципального дошкольного образовательного бюджетного учреждения города Бузулука «Детский сад № 25»

Бузулук,2021

1. Общие положения

1.1. Настоящее Положение об обработке и защите персональных данных работников (далее - Положение) муниципального дошкольного образовательного бюджетного учреждения города Бузулука "Детский сад № 25" (далее - ДОУ) определяет порядок организации и проведения работ по защите конфиденциальной информации.

1.2. Под информацией ограниченного доступа понимаются сведения, доступ к которым ограничен нормативно-правовыми актами, в частности Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера».

1.3. Персональные данные (далее – ПДн) относятся к информации ограниченного доступа (далее - информация), так как попадают под действие Федерального закона Российской Федерации от 27.07.2006 № 152 «О персональных данных».

1.4. Целью данного Положения является защита персональных данных работников ДОУ от несанкционированного доступа, неправомерного их использования или утраты.

1.5. Настоящее Положение разработано на основании:

- ст. 24 Конституции РФ,
- главы 14 Трудового Кодекса РФ,
- Закона «Об информации, информатизации и защите информации» № 149-ФЗ от 27.07.2006 г.,
- Федерального закона РФ «О персональных данных» № 152-ФЗ от 27.07.2006 г.,
- Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным Постановлением Правительства РФ от 15.09.2008 № 687,
- Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденным Постановлением Правительства РФ от 17.11.2007 № 781,
- Кодекса об административных нарушениях РФ,
- Гражданского Кодекса РФ,
- Уголовного Кодекса,
- также иными нормативно-правовыми актами в сфере защиты персональных данных.

1.6. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75-летнего срока хранения, если иное не определено законом.

1.7. Положение предназначено для практического использования должностным лицам ответственным за защиту информации.

1.8. Настоящее Положение утверждается и вводится в действие приказом заведующего ДОУ и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным.

1.9. Персональная ответственность за организацию и выполнение мероприятий по защите информации в ДОУ возлагается на сотрудника ДОУ, назначенного приказом.

1.10. Ответственность за обеспечение защиты информации возлагается непосредственно на пользователя информации.

1.11. Проведение работ по защите информации в ИС с помощью встроенных средств безопасности сертифицированных лицензионных операционных систем и антивирусного программного обеспечения, выполнения требований настоящего

Положения, возлагается на ответственного за защиту информации в ДОУ (далее - ответственный).

1.12. Лица, виновные в нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральным законодательством.

1.13. Положение может уточняться и корректироваться по мере необходимости.

2. Основные термины

2.1. В соответствии с действующим законодательством в настоящем положении применяются следующие термины:

Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

Использование персональных данных - действия (операции) с персональными данными, совершаемые в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

Информационная система персональных данных - информационная система (далее ИС), представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение

в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

3. Понятие и состав персональных данных

3.1. Персональные данные работника (сотрудника ДОУ) - информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника.

Под информацией о работниках понимаются сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.

3.2. В состав персональных данных работника входят:

- анкетные и биографические данные;
- занимаемая должность;
- сведения о текущем должностном окладе;
- паспортные данные;
- адрес регистрации;
- адрес проживания;
- ИНН;
- номер страхового свидетельства;
- сведения об ограничении трудоспособности;
- информация о постановке на воинский учет;
- номер телефона;
- данные об образовании;
- данные о детях;
- данные о семейном положении;
- содержание трудового договора;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- основания к приказам по личному составу;

4. Обработка персональных данных

4.1. Под обработкой персональных данных работника понимается получение, хранение, комбинирование, передача или любое другое использование персональных данных работника.

4.2. В целях обеспечения прав и свобод человека, и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

4.2.1. Обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

4.2.2. При определении объема и содержания, обрабатываемых персональных данных работника, работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым Кодексом и иными федеральными законами.

4.2.3. Получение персональных данных может осуществляться как путем представления их самим работником, так и путем получения их из иных источников.

4.2.4. Персональные данные следует получать у самого работника.

Если персональные данные работника, возможно, получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

4.2.5. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях, и частной жизни.

В случаях, непосредственно связанных с вопросами трудовых отношений данные о частной жизни работника (информация о жизнедеятельности в сфере семейных бытовых, личных отношений) могут быть получены и обработаны работодателем только с его письменного согласия.

4.2.6. Работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

4.3. К обработке, передаче и хранению персональных данных работника могут иметь доступ сотрудники:

- сотрудники службы управления персоналом;
- сотрудники медицинской службы.

4.4. Использование персональных данных возможно только в соответствии с целями, определившими их получение.

4.4.1. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации.

Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

4.5. Передача персональных данных работника возможна только с согласия работника или в случаях, прямо предусмотренных законодательством.

4.5.1. При передаче персональных данных работника работодатель должен соблюдать следующие требования:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом;
- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено.

Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности).

Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;
- разрешать доступ к персональным данным работников только специально уполномоченным лицам, определенным приказом по организации, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
- передавать персональные данные работника представителям работников в порядке, установленном Трудовым Кодексом, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

4.5.2. Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

4.5.3. При передаче персональных данных работника потребителям (в том числе и в коммерческих целях) за пределы ДОУ работодатель не должен сообщать эти данные третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника или в случаях, установленных федеральным законом.

4.6. Все меры конфиденциальности при сборе, обработке и хранении персональных данных сотрудника распространяются как на бумажные, так и на электронные (автоматизированные) носители информации:

4.6.1. Обработка персональных данных без использования средств автоматизации осуществляется в соответствии с «Инструкцией по обработке персональных данных, осуществляемой без использования средств автоматизации».

4.6.2. Трудовые книжки хранятся в сейфе в кабинете заведующего ДОУ.

4.6.3. Личные дела, личные карточки по форме Т-2, документы, содержащие персональные данные, необходимые для осуществления выплат заработной платы работникам и других выплат, и отчислений (в Пенсионный фонд, в Фонд социального страхования) хранятся в кабинете заведующего ДОУ.

4.6.4. Персональные данные в бухгалтерии расчетного отдела Управления образования администрации города Бузулука хранятся, в том числе, в архиве и в программе по выплате зарплаты.

4.7. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

4.8. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

4.9. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

Работодатель учитывает личные качества работника, его добросовестный и эффективный труд.

5. Доступ к персональным данным

5.1. Внутренний доступ (доступ внутри ДОУ).

5.1.1. Право доступа к персональным данным сотрудника имеют:

- заведующий;
- старший воспитатель;
- заведующий хозяйством (доступ к личным данным только сотрудников своего подразделения);
- сотрудники бухгалтерии расчетного отдела Управления образования администрации города Бузулука в сфере своей компетенции;
- делопроизводитель (если таковой имеется в штатной единице);
- сам работник, носитель данных;
- другие сотрудники ДОУ при выполнении ими своих служебных обязанностей.

5.1.2. Перечень лиц, имеющих доступ к персональным данным работников, определяется приказом заведующего ДОУ.

5.2. Внешний доступ.

5.2.1. К числу массовых потребителей персональных данных вне ДОУ можно отнести государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения Управления образования администрации города Бузулука;

5.2.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

5.2.3. Организации, в которые сотрудник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.

5.2.4. Другие организации.

Сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления работника.

Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника.

В случае развода бывшая супруга (супруг) имеют право обратиться в ДОУ с письменным запросом о размере заработной платы сотрудника без его согласия. (УК РФ).

6. Защита персональных данных

6.1. Целью технической защиты информации в ДОУ является предотвращение НСД к информации при её обработке в ИС, связанные с действиями нарушителей, включая пользователей ИС, реализующих угрозы непосредственно в ИС, а также нарушителей, не имеющих доступ к ИС, реализующих угрозы из сетей международного информационного обмена с целью её разрушения, искажения, уничтожения, блокировки и несанкционированного копирования.

6.2. Целями организационных мероприятий по защите информации в ДОУ являются:
- исключение непреднамеренных действий сотрудников ДОУ, приводящих к утечке, искажению, разрушению информации, в том числе ошибки эксплуатации АС;
- сведение к минимуму возможности нарушения политик безопасности с помощью любых средств, не связанных непосредственно с использованием АС (физический вынос информации на электронном носителе).

6.3. Заведующий ДОУ самостоятельно определяет состав, перечень мер необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных п.1.4. настоящего Положения.

К таким мерам могут, в частности, относиться:
- назначение ответственного за организацию защиты информации;
- издание комплекта документов, определяющих политику в отношении обработки ПДн в ДОУ, а также локальные акты, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации;
- использование средств антивирусной защиты;
- предотвращение организационными мерами НСД к обрабатываемой информации;
- организация процесса резервного копирования и архивирования как неотъемлемой части политики защиты информации;
- осуществление учета машинных носителей информации и их хранение в надежно запираемых шкафах;
- строгое соблюдение сотрудниками ДОУ «Инструкции пользователя информационной системы персональных данных».

6.4. Документальное оформление мероприятий по защите объекта информатизации включает:
- приказ об организации работ по защите информации ограниченного доступа;
- акты классификации ИС;
- Положение об обработке и защите персональных данных работников ДОУ;
- технические паспорта;
- инструкции ответственного за защиту персональных данных;
- журнал учёта обращений субъектов персональных данных о выполнении их законных прав, при обработке персональных данных в ИС;
- журнал учёта защищаемых носителей информации.

7. Особенности обработки информации, содержащей персональные данные

7.1. ДОУ не имеет права получать и обрабатывать данные субъекта ПДн о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях.

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

7.2. Обработка указанных данных возможна без его согласия в соответствии со ст. 6 Федеральным законом от 27.07.2006 № 152 «О персональных данных».

7.3. Письменное согласие на обработку своих персональных данных должно включать в себя:
- фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

- наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта ПДн;
- цель обработки ПДн;
- перечень ПДн, на обработку которых дается согласие субъекта персональных данных;
- перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПДн;
- срок, в течение которого действует согласие, а также порядок его отзыва.

7.4. Согласие на обработку ПДн может быть отозвано субъектом ПДн по письменному запросу на имя заведующего ДОУ.

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

7.6. Субъект ПДн имеет право на получение следующей информации:
- сведения о лицах, которые имеют доступ к ПДн или которым может быть предоставлен такой доступ;
- перечень обрабатываемых ПДн и источник их получения;
- сроки обработки ПДн, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для субъекта ПДн может повлечь за собой обработка его ПДн.

7.7. Субъект ПДн вправе требовать от оператора уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

7.8. Сведения о ПДн должны быть предоставлены субъекту ПДн оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам ПДн.

7.9. Доступ к своим ПДн предоставляется субъекту ПДн или его законному представителю оператором при получении письменного запроса субъекта ПДн или его законного представителя.
Письменный запрос должен быть адресован на имя заведующего ДОУ или уполномоченного руководителем лицо.

7.10. Субъект в праве обжаловать в судебном порядке неправомерные действия или бездействия должностных лиц ДОУ при обработке и защите его ПДн.

7.11. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

7.12. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные иные заинтересованные в возникновении угрозы лица.

7.13. Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности компании.

7.14. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.

7.15. «Внутренняя защита».

7.15.1. Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами организации.

7.15.2. Для обеспечения внутренней защиты персональных данных работников необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работником требований нормативно-методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;
- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел сотрудников на рабочие места.

Личные дела могут выдаваться на рабочие места только заведующему, работникам службы управления персоналом и в исключительных случаях, по письменному разрешению заведующего,

- заместителям заведующего (например, при подготовке материалов для аттестации работника).

7.16. «Внешняя защита».

7.16.1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией.

Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

7.16.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности ДОУ, посетители, работники других организационных структур.

Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе персонала.

7.16.3. Для обеспечения внешней защиты персональных данных сотрудников необходимо соблюдать ряда мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим организации;
- учет и порядок выдачи удостоверений;
- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при интервьюировании и собеседованиях.

7.17. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников.

7.18. По возможности персональные данные обезличиваются.

7.19. Кроме мер защиты персональных данных, установленных законодательством, работодатели, работники и их представители могут вырабатывать совместные меры защиты персональных данных работников.

8. Права и обязанности должностных лиц

8.1. Заведующий ДОУ организует работу по построению системы защиты ИС.

В частности:

8.1.1. Назначает ответственного за организацию защиты информации из числа сотрудников ДОУ.

8.1.2. Утверждает состав комиссии по организации работ по защите информации.

8.1.3. Утверждает комплект документов, определяющих политику в отношении обработки ПДн в учреждении, а также локальные акты, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации.

8.1.4. Утверждает меры и состав средств СЗИ, предложенных для обеспечения безопасности ПДн при их обработке в ИСПДн. При этом оценивает соотношение вреда, который может быть причинен субъектам ПДн и принимаемых мер по защите ИСПДн.

8.2. Заведующий ДОУ:

- составляет Перечень сведений конфиденциального характера в ДОУ;
- контролирует работу ответственного по организации и проведению работ по защите информации в ДОУ;
- предотвращает организационными мерами НСД к обрабатываемой в ИС информации;
- контролирует порядок подготовки, учета и хранения документов конфиденциального характера;
- контролирует порядок передачи информации другим органам и организациям, а также между структурными подразделениями своей организации;
- организуют выполнение мероприятий по защите информации при использовании технических средств;
- участвует в определении мест установки и количества АРМ, необходимых для обработки информации, а также пользователей этих ИС;

- участвует в определении правил разграничения доступа к информации в ИС, используемых в ДОУ.

8.3. Ответственный:

- разрабатывает организационно-распорядительные документы по вопросам защиты информации при её обработке с помощью ИС;
- контролирует исполнение приказов и распоряжений вышестоящих организаций по вопросам обеспечения безопасности информации;
- знакомит работников ДОУ, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн;
- обеспечивает защиту информации, циркулирующей на объектах информатизации, организовывает работы по декларированию (аттестации) ИС на соответствие нормативным требованиям;
- устанавливает систематический контроль работы СЗИ, применяемых в ИС, а также за выполнением комплекса организационных мероприятий по обеспечению безопасности информации;
- проводит инструктаж пользователей ИС;
- контролирует выполнение администратором ИС обязанностей по обеспечению функционирования СЗИ (настройка и сопровождение подсистемы управления доступом пользователя к защищаемым информационным ресурсам ИС, антивирусная защита, резервное копирование данных и т.д.)
- контролирует порядок учёта и хранения машинных носителей конфиденциальной информации;
- присутствует (участвует) в работах по внесению изменений в аппаратно-программную конфигурацию ИС;
- определяет порядок и осуществляет контроль ремонта средств вычислительной техники, входящих в состав ИС;
- принимает меры по оперативному изменению паролей при увольнении или перемещении сотрудников, имевших допуск к ИС;
- требует устранения выявленных нарушений и недостатков, давать обязательные для исполнения указания по вопросам обеспечения положений инструкций по защите информации;
- требует от работников представления письменных объяснений по фактам нарушения режима конфиденциальности;
- об имеющихся недостатках и выявленных нарушениях требований нормативных и руководящих документов по защите информации, а также в случае выявления попыток НСД к информации или попыток хищения, копирования, изменения незамедлительно принимает меры пресечения и докладывает заведующему ДОУ;
- в установленные сроки подготавливает необходимую отчетную документацию о состоянии работ по защите информации.

9. Планирование работ по защите информации

9.1. Планирование работ по защите информации проводится на основании:

- рекомендаций актов проверок контрольными органами;
- результатов анализа деятельности в области защиты информации;
- рекомендаций и указаний Роскомнадзора и ФСТЭК России.

10. Контроль состояния защиты информации

10.1. С целью своевременного выявления и предотвращения НСД к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособность систем информатизации, осуществляется контроль состояния и эффективности СЗИ.

10.2. Контроль заключается в проверке по действующим методикам выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности принятых мер.

10.3. Повседневный контроль выполнения организационных мероприятий, направленных на обеспечение защиты информации, проводится ответственным.

10.4. Плановые и внеплановые проверки за соответствием обработки персональных данных требованиям законодательства могут осуществляться территориальными органами Федеральной службы по надзору в сфере связи и массовых коммуникаций.

10.5. Допуск представителей этих органов для проведения контроля осуществляется в установленном порядке по предъявлению служебных удостоверений и предписаний на право проверки, подписанных руководителем (заместителем) соответствующего органа.

10.6. Ответственный обязан присутствовать при всех проверках по вопросам защиты информации.

10.7. Результаты проверок отражаются в Актах проверок.

10.8. По результатам проверок контролирующими органами ответственный с привлечением заинтересованных должностных лиц в десятидневный срок разрабатывает план устранения выявленных недостатков.

10.9. Защита информации считается эффективной, если принимаемые меры соответствуют установленным требованиям и нормам.

Несоответствие мер установленным требованиям или нормам по защите информации является нарушением.

10.10. При обнаружении нарушений заведующий ДОУ принимает необходимые меры по их устранению в сроки, согласованные с органом или должностным лицом, проводившим проверку.

10.11. Закрепление прав работника, регламентирующих защиту его персональных данных, обеспечивает сохранность полной и точной информации о нем.

10.12. Работники и их представители должны быть ознакомлены под расписку с документами организации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

10.13. В целях защиты персональных данных, хранящихся у работодателя, работник имеет право:

10.13.1. требовать исключения или исправления неверных или неполных персональных данных;

10.13.2. на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;

10.13.3. персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;

10.13.4. определять своих представителей для защиты своих персональных данных;

10.13.5. на сохранение и защиту своей личной и семейной тайны.

10.14. Работник обязан:

10.14.1. передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ;

10.14.2. своевременно сообщать работодателю об изменении своих персональных данных.

10.15. Работники ставят работодателя в известность об изменении фамилии, имени, отчества, даты рождения, что получает отражение в трудовой книжке на основании представленных документов.

При необходимости изменяются данные об образовании, профессии, специальности, присвоении нового разряда и пр.

10.16. В целях защиты частной жизни, личной и семейной тайны работники не должны отказываться от своего права на обработку персональных данных только с их согласия, поскольку это может повлечь причинение морального, материального вреда.

11. Ответственность за разглашение конфиденциальной информации связанной с персональными данными

11.1. Персональная ответственность - одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

11.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

11.3. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

11.4. Каждый сотрудник организации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

11.5. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

11.5.1. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым Кодексом дисциплинарные взыскания.

11.5.2. Должностные лица, в обязанность которых входит ведение персональных данных сотрудника, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации - влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

11.5.3. В соответствии с Гражданским Кодексом лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на работников.

11.5.4. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказывается штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.

Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.