

ПОЛОЖЕНИЕ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения.

1.1. Настоящее Положение разработано в целях защиты персональных данных, обрабатываемых в информационных системах персональных данных «МБДОУ «ЦРР – детский сад №60», от несанкционированного доступа, неправомерного их использования или утраты.

1.2. Положение определяет обеспечение в соответствии с законодательством Российской Федерации обработки, хранения и защиты персональных данных, а также персональных данных, содержащихся в документах, полученных из других организаций, в обращениях граждан и иных субъектов персональных данных.

1.3. Положение разработано на основании ст.24 Конституции РФ, Федерального закона РФ «О персональных данных» № 152-ФЗ от 27.07.2006 г., Закона «Об информации, информатизации и защите информации» № 149-ФЗ от 27.07.2006 г., Постановления Правительства Российской Федерации от 17.11.2007г. №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», нормативно-правовыми актами Российской Федерации в области трудовых отношений.

1.4. Настоящее Положение утверждается заведующим Учреждения и действует до принятия нового..

1.5. В настоящем Положении используются следующие основные понятия:

1.5.1. Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных) – работнику, абитуриенту, обучающемуся, выпускнику;

1.5.2. Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных

1.5.3. 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;

1.5.4. 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;

1.5.5. Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором 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;

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

1.5.7. 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;

1.5.8. Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

1.5.9. Информационная система персональных данных – информационная система, 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;

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

1.5.11. 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.

2. Понятие и содержание персональных данных.

2.1. Персональные данные – информация, необходимая для осуществления основной деятельности «МБДОУ «ЦРР – детский сад №60», и кадрового учета сотрудников.

2.2. Оператором персональных данных является «МБДОУ «ЦРР – детский сад №60».

2.3. Допускается привлекать для обработки персональных данных уполномоченные организации на основе соответствующих договоров и соглашений.

2.4. Персональные данные являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения, соответствующий гриф ограничения на них не ставится.

2.5. Обеспечение конфиденциальности персональных данных не требуется в случае обезличивания и в отношении общедоступных персональных данных.

3. Порядок получения и обработки персональных данных.

3.1. Получение персональных данных осуществляется в соответствии с нормативно-правовыми актами Российской Федерации в области трудовых отношений, защиты персональных данных, нормативными и распорядительными документами «МБДОУ «ЦРР – детский сад №60», на основе согласия субъектов на обработку их персональных данных.

3.2. Оператор не вправе требовать от субъекта персональных данных предоставления информации о его национальной и расовой принадлежности, политических и религиозных убеждениях и о его частной жизни.

3.3. Без согласия субъектов осуществляется обработка общедоступных персональных данных или содержащих только фамилии, имена и отчества, обращений и запросов организаций и физических лиц, регистрация и отправка корреспонденции почтовой связью, оформление разовых пропусков, обработка персональных данных для исполнения трудовых договоров или без использования средств автоматизации, и в иных случаях, предусмотренных законодательством Российской Федерации

3.4. Обработка и использование персональных данных осуществляется в целях, указанных в соглашениях с субъектами персональных данных, а также в случаях, предусмотренных нормативно-правовыми актами Российской Федерации.

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

3.6. В случае увольнения субъекта персональных данных и иного достижения целей обработки персональных данных, зафиксированных в письменном соглашении, Оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами.

3.7. Правила обработки и использования персональных данных устанавливаются отдельными регламентами и инструкциями «МБДОУ «ЦРР – детский сад №60».

3.8. Персональные данные могут храниться в бумажном и(или) электронном виде централизованно или в соответствующих структурных подразделениях с соблюдением предусмотренных нормативно-правовыми актами Российской Федерации мер по защите персональных данных.

3.9. Перечень отдельных должностей, имеющих право на обработку персональных данных, определяется отдельными Приказами, распорядительными документами и иными письменными указаниями уполномоченных сотрудников «МБДОУ «ЦРР – детский сад №60».

3.10. Персональные данные защищаются от несанкционированного доступа в соответствии с нормативно-правовыми актами Российской Федерации, нормативно-распорядительными актами и рекомендациями регулирующих органов в области защиты информации, а также утвержденными регламентами и инструкциями Оператора

4. Права, обязанности и ответственность субъекта персональных данных и Оператора при обработке персональных данных/

4.1. В целях обеспечения защиты своих персональных данных субъект персональных данных в соответствии с Федеральным законом Российской Федерации от 27.06.2006 г. № 152-ФЗ «О персональных данных» за исключением случаев, предусмотренных данным Федеральным законом, имеет право:

4.1.1. На получение сведений об Операторе, о месте его нахождения, о наличии у Оператора персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими персональными данными;

4.1.2. Требовать от Оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

4.1.3. На получение при обращении или при получении запроса информации, касающейся обработки его персональных данных;

4.1.4. На обжалование действий или бездействия Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке;

4.1.5. На защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

4.2. Обязанности Оператора при сборе персональных данных.

4.2.1. Оператор обязан 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 заблокировать соответствующие персональные данные по предоставлению субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет Оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

4.2.2. О внесенных изменениях и предпринятых мерах Оператор обязан уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы.

4.2.3. В случае выявления неправомерных действий с персональными данными Оператор в срок, не превышающий трех рабочих дней с даты такого выявления, обязан устранить допущенные нарушения.

4.2.4. В случае невозможности устранения допущенных нарушений Оператор в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные.

4.2.5. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных или его законного представителя.

4.2.6. 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 трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Оператором и субъектом персональных данных.

4.2.7. Об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных.

4.3. Права Оператора на передачу персональных данных третьим лицам.

4.3.1. Оператор не вправе без письменного согласия субъекта персональных данных передавать обрабатываемые персональные данные третьим лицам, за исключением случаев, предусмотренных законодательством Российской Федерации

4.3.2. Передача персональных данных субъекта третьим лицам должна производиться в соответствии с Регламентом передачи персональных данных третьим лицам.

5. Ответственность за разглашение персональных данных.

5.1. Оператор, а также должностные лица, виновные в нарушении требований Федерального закона РФ «О персональных данных» № 152-ФЗ от 27.07.2006, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

5.2. Ответственность за соблюдение требований законодательства Российской Федерации при обработке и использовании персональных данных возлагается в приказе об утверждении Положения и иных приказах на руководителей структурных подразделений и конкретных должностных лиц Оператора, обрабатывающих персональные данные.

6. Особенности обработки персональных данных в информационных системах персональных данных с использованием средств автоматизации

6.1 Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации осуществляется в соответствии с требованиями 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», нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.

6.2. Информационные системы, предназначенные для обработки персональных данных, должны быть приведены в соответствие с Приказом ФСТЭК № 58 от 5 февраля 2010 г «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных».

6.3. Не допускается обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации:

- при отсутствии установленных и настроенных сертифицированных средств защиты информации;
- при отсутствии утвержденных организационных документов о порядке эксплуатации информационной системы персональных данных.

6.4. Пользователь информационной системы персональных данных обязан соблюдать правила и технологию обработки информации, отраженную в Инструкции пользователя ИСПДн.

6.5. Для входа в информационную систему персональных данных сотрудник должен ввести имя и пароль. Не допускаются режимы безпарольного (гостевого) доступа к какой-либо информации, содержащейся в информационной системе персональных данных.

7. Порядок обработки персональных данных без использования средств автоматизации

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

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

7.3. При неавтоматизированной обработке персональных данных на бумажных носителях:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или

использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

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

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

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).

8. Основные принципы построения системы комплексной защиты информации

Построение системы обеспечения безопасности персональных данных информационных систем персональных данных «МБДОУ «ЦРР – детский сад №60», и их функционирование должны осуществляться в соответствии со следующими основными принципами:

- законность;
- системность;
- комплексность;
- непрерывность;
- персональная ответственность;
- минимизация полномочий;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- простота применения средств защиты;
- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;
- обязательность контроля.

8.1. Законность

Предполагает осуществление защитных мероприятий и разработку системы защиты персональных данных (СЗПДн) «МБДОУ «ЦРР – детский сад №60» в соответствии с действующим законодательством в области защиты персональных данных и других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции.

Пользователи и обслуживающий персонал информационных систем персональных данных Администрации должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за защиту ПДн.

8.2. Системность

Системный подход к построению СЗПДн «МБДОУ «ЦРР – детский сад №60» предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности информационной системы персональных данных Администрации.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки персональных данных, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и НСД к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и

НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

8.3. Комплексность

Комплексное использование методов и средств защиты 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. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невязанных областях.

Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одним из наиболее укрепленных рубежей призваны быть средства криптографической защиты, реализованные с использованием технологии VPN. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

8.4. Непрерывность защиты персональных данных

Защита персональных данных – не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла информационной системы персональных данных.

Информационные системы персональных данных должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода информационных систем персональных данных в незащищенное состояние.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, 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 системы защиты после восстановления ее функционирования.

8.5. 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.

8.6. Принцип минимизации полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «все, что не разрешено, запрещено».

Доступ к персональным данным должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

8.7. Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих деятельность информационных систем персональных данных «МБДОУ «ЦРР – детский сад №60», для снижения вероятности возникновения негативных действий связанных с человеческим фактором.

В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности подразделений технической защиты информации.

8.8. Гибкость системы защиты персональных данных

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

8.9. Простота применения средств защиты

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.). Должна достигаться автоматизация максимального числа действий пользователей и администраторов информационной системы персональных данных.

8.10. Научная обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности персональных данных. Система защиты персональных данных должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

8.11. Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности персональных данных, 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 «МБДОУ «ЦРР – детский сад №60».

8.12. Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности персональных данных на основе используемых систем и средств защиты информации 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.

9. Меры, методы и средства обеспечения требуемого уровня защищенности

Обеспечение требуемого уровня защищенности должно достигаться с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности информационных систем персональных данных подразделяются на:

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

Перечень выбранных мер обеспечения безопасности отражается в Плане мероприятий по обеспечению защиты персональных данных.

9.1. 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 ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию персональных данных и являющиеся сдерживающим фактором для потенциальных нарушителей.

Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

9.2. Морально-этические меры защиты

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения ЭВМ в стране или обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписанные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писанные, 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 коллективах подразделений. Морально-этические меры защиты снижают вероятность возникновения негативных действий связанных с человеческим фактором.

9.3. Организационные (административные) меры защиты

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

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

Реализация политики информационной безопасности персональных данных в информационных системах персональных данных состоит из мер административного уровня и организационных (процедурных) мер защиты информации.

К административному уровню относятся решения руководства, которые закрепляются в локальных актах «МБДОУ «ЦРР – детский сад №60». Примером таких решений могут быть:

- формирование, пересмотр, реализация плана работы «МБДОУ «ЦРР – детский сад №60» по обеспечению безопасности персональных данных, определение ответственных за его реализацию;
- формулирование целей, постановка задач, определение направлений деятельности в области безопасности персональных данных;
- обеспечение нормативной (правовой) базы вопросов безопасности и т.п.

Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности персональных данных, определить какими ресурсами (материальные, персонал) они будут достигнуты и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью информационных систем.

На организационном уровне определяются процедуры и правила достижения целей и решения задач политики информационной безопасности персональных данных. Эти правила определяют:

- каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности персональных данных, а так же их установить ответственность;
- кто имеет права доступа к персональным данным;
- какими мерами и средствами обеспечивается защита персональных данных;
- какими мерами и средствами обеспечивается контроль за соблюдением введенного режима безопасности.

Организационные меры должны:

- предусматривать регламент информационных отношений, исключающих возможность несанкционированных действий в отношении объектов защиты;
- определять коалиционные и иерархические принципы и методы разграничения доступа к персональным данным;
- определять порядок работы с программно-математическими и техническими (аппаратные) средствами защиты и криптозащиты и других защитных механизмов;
- организовать меры противодействия НСД пользователями на этапах аутентификации, авторизации, идентификации, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

Организационные меры должны состоять из:

- ограничения доступа в помещения, где расположены информационные системы персональных данных и их отдельные элементы;
- порядка допуска сотрудников к использованию ресурсов информационных систем персональных данных «МБДОУ «ЦРР – детский сад №60»,
- регламента процессов ведения баз данных и осуществления модификации информационных ресурсов;
- регламента процессов обслуживания и осуществления модификации аппаратных и программных ресурсов информационных систем персональных данных;
- инструкций пользователей информационных систем персональных данных (администратора, администратора безопасности, оператора);

9.4. Физические меры защиты

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

Все объекты критичные с точки зрения информационной безопасности ИСПДн (все сервера баз данных, маршрутизаторы, межсетевые экраны) находятся в отдельном помещении, доступ в которое разрешен только сотрудникам, имеющими соответствующее разрешение от руководства организации. Ключевые диски, пароли и прочая конфиденциальная информация хранится в сейфах или металлических шкафах. Вход в помещение осуществляется через дверь, оснащенную замками (не менее двух). Копии ключей находятся у специалиста по кадрам. Помещение оборудовано принудительной вентиляцией и пожарной сигнализацией. Помещение контролируется системой видео наблюдения с выходом на мониторы вахты. Доступ в помещение посторонним лицам запрещен. Технический персонал, осуществляющий уборку помещения, ремонт оборудования и т.п. может находиться в помещении только в присутствии работников, имеющих право находиться в данном помещении в связи с выполнением своих должностных обязанностей. Доступ в помещение в нерабочее время или в выходные и праздничные дни осуществляется с письменного разрешения заведующего МБДОУ «ЦРР – детский сад №60».

Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение

информационных носителей, самих средств информатизации, исключая находящиеся внутри контролируемой (охраняемой) зоны технических средств разведки.

9.5. Аппаратно-программные средства защиты ПДн

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав ИСПДн и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

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

- средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей информационных систем персональных данных;
- средства разграничения доступа зарегистрированных пользователей системы к ресурсам информационных систем персональных данных Администрации;
- средства обеспечения и контроля целостности программных и информационных ресурсов;
- обязательное резервирование всей информации, имеющей конфиденциальный характер;
- дублирование информации с использованием различных физических и аппаратных носителей;
- средства оперативного контроля и регистрации событий безопасности;
- криптографические средства защиты персональных данных.

Успешное применение технических средств защиты на основании представленных выше принципов предполагает, что выполнение перечисленных ниже требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:

- обеспечена физическая целостность всех компонент информационных систем персональных данных;
- каждый работник - пользователь информационных систем персональных данных имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;
- все изменения конфигурации технических и программных средств информационных систем персональных данных производятся строго установленным порядком (регистрируются и контролируются) только на основании распоряжений руководства «МБДОУ «ЦРР – детский сад №60»»;
- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах, и т.п.).
- специалистами «МБДОУ «ЦРР – детский сад №60» осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

ПЕРЕЧЕНЬ
персональных данных, подлежащих защите
в МБДОУ «ЦРР – детский сад №60»

Введение.

Настоящий Перечень персональных данных, подлежащих защите в информационных системах персональных данных (далее ИСПДн) учреждения (далее - Перечень) МБДОУ «ЦРР - детский сад №60» далее (Учреждение).

Перечень разработан в соответствии со списком объектов защиты, изложенных в Концепции информационной безопасности ИСПДн Учреждения.

Перечень содержит полный список категорий данных, безопасность которых должна обеспечиваться системой защиты персональных данных (СЗПДн).

1. Общие положения.

Объектами защиты являются – информация, обрабатываемая в ИСПДн, и технические средства ее обработки и защиты. Перечень объектов защиты определен по итогам отчета о результатах проведения внутренней проверки.

Объекты защиты каждой ИСПДн включают:

- 1) Обрабатываемая информация:
 - персональные данные работников (раздел 2.1.)
 - персональные данные воспитанников, включая персональные данные родителей (законных представителей) воспитанников (раздел 2.1.2)
- 2) Технологическая информация (раздел 2.2)
- 3) Программно – технические средства обработки (раздел 2.3)
- 4) Средства защиты ПДн (раздел 2.4)
- 5) Каналы информационного обмена и телекоммуникации (раздел 2.5)
- 6) Объекты и помещения, в которых размещены компоненты ИСПДн (раздел 2.6)

2. ИСПДн МБДОУ «ЦРР – детский сад №60»

2.1. Обрабатываемая информация.

2.1.1. Перечень персональных данных работников Учреждения.

Персональные данные работников МБДОУ «ЦРР – детский сад №60» включают:

- Фамилия, имя, отчество;
- Место, год и дата рождения;
- Адрес по прописке;
- Адрес проживания (реальный);
- Паспортные данные (серия, номер паспорта, кем и когда выдан);
- Информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающих образование: наименование, номер, дата выдачи, специальность);
- Информация о трудовой деятельности до приема на работу;
- Информация о трудовом стаже (место работы, должность, период работы, причина увольнения);
- Телефонный номер (домашний, рабочий, мобильный);
- Семейное положение и состав семьи (муж/жена, дети);
- Информация о знании иностранных языков;
- Форма допуска;
- оклад
- данные о трудовом договоре (№ трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, длительность дополнительного отпуска за ненормированный рабочий день, обязанности работника, дополнительные социальные льготы и гарантии, № и

число изменения к трудовому договору, характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочей недели, система оплаты);

– Сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета);

– ИНН;

– Данные об аттестации работников;

– Данные о повышении квалификации;

– Данные о наградах, медалях, поощрениях, почетных званиях;

– Информация о приеме на работу, перемещении по должности, увольнении;

– Информация об отпусках;

– Информация о командировках;

– Информация о болезнях;

– Информация о негосударственном пенсионном обеспечении.

2.1.2. Персональные данные воспитанников включают:

– ФИО,

– Дата рождения,

– Свидетельство о рождении,

– Контактный телефон,

– Адрес прописки,

– Фактический адрес проживания,

– Данные о законных представителях (составе семьи, месте работы родителей, образовании, а так же дополнительно запрашиваемых сведениях),

– № путевки,

– № договора с МБДОУ,

– номер группы,

– дата приема (отчисления),

– иные движения воспитанников,

– табель посещаемости,

– медицинская карта воспитанника,

– информацию об отсутствии воспитанника (пропусках, отпусках, летнего - оздоровительного периода, болезни и других причинах).

2.2. Технологическая информация

Технологическая информация, подлежащая защите, включает:

– управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);

– технологическая информация средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);

– информация на съемных носителях информации (бумажные, магнитные, оптические и пр.), содержащие защищаемую технологическую информацию системы управления ресурсами или средств доступа к этим системам управления;

– информация о СЗПДн, их составе и структуре, принципах и технических решениях защиты;

– информационные ресурсы (базы данных, файлы и другие), содержащие информацию о информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;

– служебные данные, появляющиеся при работе программного обеспечения, сообщений и протоколов межсетевое взаимодействия, в результате обработки Обрабатываемой информации.

2.3. Программно-технические средства обработки

Программно-технические средства включают в себя:

- общесистемное и специальное программное обеспечение (операционные системы, серверные приложения и другие);
- резервные копии общесистемного программного обеспечения;
- инструментальные средства и утилиты систем управления ресурсами ИСПДн;
- аппаратные средства обработки ПДн (АРМ и сервера);
- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.).

2.4. Средства защиты ПДн

Средства защиты ПДн состоят из аппаратно-программных средств, включают в себя:

- средства управления и разграничения доступа пользователей;
- средства обеспечения регистрации и учета действий с информацией;
- средства, обеспечивающие целостность данных;
- средства антивирусной защиты;
- средства межсетевого экранирования;
- средства анализа защищенности;
- средства обнаружения вторжений;
- средства криптографической защиты ПДн, при их передачи по каналам связи сетей общего и (или) международного обмена.

2.5. Каналы информационного обмена и телекоммуникации

Каналы информационного обмена и телекоммуникации являются объектами защиты, если по ним передаются обрабатываемая и технологическая информация.

2.6. Объекты и помещения, в которых размещены компоненты ИСПДн

Объекты и помещения являются объектами защиты, если в них происходит обработка обрабатываемой и технологической информации, установлены технические средства обработки и защиты.