АДМИНИСТРАЦИЯ АЛЕКСАНДРОВСКОГО РАЙОНА
ТОМСКОЙ ОБЛАСТИ

РАСПОРЯЖЕНИЕ

26.12.2012 № 106-р

с. Александровское

Об утверждении Положения о защите персональных данных.

В целях защиты персональных данных, обрабатываемых в информационных системах персональных данных Администрации Александровского района, от несанкционированного доступа, неправомерного их использования или утраты, на основании Федерального закона Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»:

1.Утвердить прилагаемое Положение о защите персональных данных;

2.Контроль за исполнением настоящего распоряжения возложить на первого заместителя Главы района Фисенко А.В.

Глава Александровского района А.П. Жданов

А.П. Харчевников
25565

Приложение к распоряжению Администрации района от 26.12.2012 № 106-р

Положение о защите персональных данных

Глава 1. Общие положения

1. Настоящее Положение разработано в целях защиты персональных данных, обрабатываемых в информационных системах персональных данных (далее по тексту - ИСПДн) Администрации Александровского района, от несанкционированного доступа, неправомерного их использования или утраты.

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.

3. Положение разработано на основании ст. 24 Конституции РФ, Федерального закона РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных», Постановления Правительства РФ от 17.11.2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», нормативно-правовых актов Российской Федерации в области трудовых отношений.

4. В настоящем Положении используются следующие основные понятия:

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных);

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;

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;

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;

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;

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 или в результате которых уничтожаются материальные носители персональных данных;

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

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;

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;

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.

Глава 2. Понятие и содержание персональных данных

5.Персональные данные – информация, необходимая для осуществления основной деятельности Администрации района и кадрового учёта сотрудников.

6.Оператором персональных данных является Администрация Александровского района.

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

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

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

Глава 3. Порядок получения и обработки персональных данных

10.Получение персональных данных осуществляется в соответствии с нормативно-правовыми актами Российской Федерации в области трудовых отношений, защиты персональных данных, нормативными и распорядительными документами Администрации Александровского района на основе согласия субъектов на обработку их персональных данных.

11.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.

12.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.

13.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.

14.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.

15.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 трёх рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами.

16.Правила обработки и использования персональных данных устанавливаются отдельными регламентами и инструкциями Администрации района.

17.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.

18.Перечень структурных подразделений и (или) отдельных должностей, имеющих право на обработку персональных данных предоставляется работникам структурных подразделений и (или) должностным лицам, определённым отдельными распорядительными документами Администрации района.

19.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.

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

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

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;

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;

3) На получение при обращении или при получении запроса информации, касающейся обработки его персональных данных;

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

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

21.Обязанности Оператора при сборе персональных данных.

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 блокировать соответствующие персональные данные по предоставлении субъектом персональных данных или его законным представителем сведений, подтверждающих, что

персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет Оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

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;

3) В случае выявления неправомерных действий с персональными данными Оператор в срок, не превышающий трёх рабочих дней с даты такого выявления, обязан устранить допущенные нарушения;

4) В случае невозможности устранения допущенных нарушений Оператор в срок, не превышающий трёх рабочих дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные;

5) Об устранении допущенных нарушений или об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных или его законного представителя;

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;

7) Об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных.

22.Права Оператора на передачу персональных данных третьим лицам.

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

2) Передача персональных данных субъекта третьим лицам должна производится в соответствии с Регламентом передачи персональных данных третьим лицам.

Глава 5. Особенности обработки персональных данных в ИСПДн с использованием средств автоматизации.

23.Обработка персональных данных в ИСПДн данных с использованием средств автоматизации осуществляется в соответствии с требованиями постановления Правительства РФ от 17.11.2007 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.

24.Информационные системы, предназначенные для обработки персональных данных, должны быть приведены в соответствие с Приказом ФСТЭК от 5.02.2010 г. № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных».

25.Не допускается обработка персональных данных в ИСПДн с использованием средств автоматизации:

1) при отсутствии средств защиты информации;

2) при отсутствии утверждённых организационных документов о порядке эксплуатации ИСПДн.

26.Пользователь ИСПДн обязан соблюдать правила и технологию обработки информации, отражённую в инструкции.

27.Для входа в ИСПДн сотрудник должен ввести имя и пароль. Не допускаются режимы беспарольного доступа к какой-либо информации, содержащейся в информационной системе персональных данных.

Глава 6. Порядок обработки персональных данных без использования средств автоматизации.

28.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 банных) на электронных носителях информации.

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

30.При неавтоматизированной обработке персональных данных на бумажных носителях:

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

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

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

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

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

1) 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;

2) 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;

3) 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;

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

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

33.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.

34.Электронные носители информации, содержащие персональные данные, учитываются в журнале учёта электронных носителей персональных данных, составленном по форме согласно приложению к настоящему Положению.

35.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:

1) 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;

2) 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.

36.Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в надёжно 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).

Глава 7. Основные принципы построения системы комплексной защиты информации.

37.Построение системы обеспечения безопасности персональных данных ИСПДн Администрации района и их функционирование должны осуществляться в соответствии со следующими основными принципами:

Законность. Предполагает осуществление защитных мероприятий и разработку системы защиты персональных данных Администрации района в соответствии с действующим законодательством в области защиты персональных данных и других нормативных актов по безопасности информации. Пользователи и обслуживающий персонал ИСПДн администрации должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за защиту персональных данных.

Системность. Системный подход к построению системы защиты персональных данных Администрации района предполагает учёт всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ИСПДн 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,

пути проникновения в распределенные системы и несанкционированного доступа к информации.

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 невзаимосвязанных областях. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

Непрерывность защиты персональных данных. Защита персональных данных – непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИСПДн. ИСПДн должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода ИСПДн в незащищенное состояние. Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная поддержка. 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.

Своевременность. Предполагает упреждающий характер мер обеспечения безопасности персональных данных, то есть постановку задач по комплексной защите ИСПДн и реализацию мер обеспечения безопасности персональных данных на ранних стадиях разработки ИСПДн в целом и ее системы защиты информации, в частности. Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

Преемственность и совершенствование. Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИСПДн и их системы защиты с учётом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

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 известен или сведен к минимуму.

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.

Взаимодействие и сотрудничество. Предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих деятельность ИСПДн, 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.

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.

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 ИСПДн.

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 Администрации района.

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.

Глава 8. Меры, методы и средства обеспечения требуемого уровня защищенности.

38. Обеспечение требуемого уровня защищенности должности достигаться с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности ИСПДн подразделяются на:

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.

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 неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний.

Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений. Морально-этические меры защиты снижают вероятность возникновения негативных действий связанных с человеческим фактором.

3) Организационные (административные) меры защиты.

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования ИСПДн, использование ресурсов ИСПДн, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с ИСПДн 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 ИСПДн состоят из мер административного уровня и организационных (процедурных) мер защиты информации.

К административному уровню относятся решения руководства, затрагивающие деятельность рассматриваемых в целом. Эти решения закрепляются в локальных актах Администрации района, примером таких решений могут быть:

а) принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности персональных данных, определение ответственных за ее реализацию;

б) формулирование целей, постановка задач, определение направлений деятельности в области безопасности персональных данных;

в) принятие решений по вопросам реализации программы безопасности, которые рассматриваются на уровне Администрации района в целом;

г) обеспечение нормативной (правовой) базы вопросов безопасности и т.п.

Политика верхнего уровня должна 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:

а) каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности персональных данных, а так же их установить ответственность;

б) кто имеет права доступа к персональным данным;

в) какими мерами и средствами обеспечивается защита персональных данных;

г) какими мерами и средствами обеспечивается контроль за соблюдением введенного режима безопасности.

Организационные меры должны:

а) предусматривать регламент информационных отношений, исключающих возможность несанкционированных действий в отношении объектов защиты;

б) определять порядок работы с программно-математическими и техническими (аппаратные) средствами защиты и криптозащиты и других защитных механизмов;

в) организовать меры противодействия несанкционированного доступа пользователями на этапах аутентификации, авторизации, идентификации, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

Организационные меры должны состоять из:

а) ограничение доступа в помещения, где расположены информационные системы персональных данных и их отдельные элементы;

б) порядок допуска сотрудников к использованию ресурсов информационных систем персональных данных;

в) регламента процессов ведения баз данных и осуществления модификации информационных ресурсов;

г) регламента процессов обслуживания и осуществления модификации аппаратных и программных ресурсов информационных систем персональных данных;

д) инструкций пользователей информационных систем персональных данных (администратора, администратора безопасности, оператора).

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.

Ко всем объектам, критичным с точки зрения информационной безопасности (сервер баз данных, маршрутизаторы, межсетевые экраны), доступ должен быть разрешён только сотрудникам, имеющими соответствующее разрешение от руководства администрации. Ключевые дискеты, пароли и прочая конфиденциальная информация хранится в сейфах. 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.

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, исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

5) Аппаратно-программные средства защиты персональных данных.

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав ИСПДн 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 учётом всех требований и принципов обеспечения безопасности персональных данных и информационных системах по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

а) средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей информационных систем персональных данных;

а) средства разграничения доступа зарегистрированных пользователей системы к ресурсам информационных систем персональных данных Администрации района;

б) средства обеспечения и контроля целостности программных и информационных ресурсов;

в) резервирование всей информации, имеющей конфиденциальный характер;

г) дублирование информации с использованием различных физических и аппаратных носителей;

д) средства оперативного контроля и регистрации событий безопасности;

е) 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:

а) обеспечена физическая целостность всех компонент информационных систем персональных данных;

б) каждый сотрудник (пользователь) или группа пользователей информационных систем персональных данных имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;

в) сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних лиц (специальных помещениях, шкафах, и т.п.);

г) специалистами Администрации района осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

Приложение
к Положению «О защите персональных данных»

Администрация Александровского района

ЖУРНАЛ

учёта электронных носителей персональных данных

название информационной система персональных данных

на _____ листах

Журнал начат «____» _____ 20__ г.

Администратор безопасности ИСПДн

Должность _____ /ФИО должностного лица/

Журнал завершён «____» _____ 20__ г.

Администратор безопасности ИСПДн

Должность _____ /ФИО должностного лица/

№ п/п	Регистраци-онный номер	Дата учета	Тип / емкость носителя	Серийный номер	Отметка о постановке на учёт (ФИО, подпись, дата)	Отметка о снятии с учета (ФИО, подпись, дата)	Местополо-жение носителя	Сведения об уничтожении носителя / стирании информации
1	2	3	4	5	6	7	8	9