Экз.№ 1

УТВЕРЖДАЮ

Исполнительный директор
некоммерческой организации «Фонд
развития индустрии переработки
отходов в Московской области»

Е.Л. Педенюк
«___»_____ 2019 г.

ПОЛОЖЕНИЕ

О ПОРЯДКЕ ОБРАБОТКИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В НЕКОММЕРЧЕСКОЙ ОРГАНИЗАЦИИ «ФОНД РАЗВИТИЯ ИНДУСТРИИ ПЕРЕРАБОТКИ ОТХОДОВ В МОСКОВСКОЙ ОБЛАСТИ»

ОЗНАКОМЛЕН

Ведущий специалист некоммерческой организации
«Фонд развития индустрии переработки отходов
в Московской области»

А.А. Квасов
«___» _____ 2019 г.

г. Москва
2019

ОГЛАВЛЕНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. «Положение о порядке обработки и обеспечении безопасности персональных данных в некоммерческой организации «Фонд развития индустрии переработки отходов в Московской области» (далее – Положение) разработано в соответствии с Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и другими нормативно-правовыми актами в областях обработки и защиты персональных данных (далее – руководящие документы).

1.2. Положение устанавливает единый порядок обработки персональных данных (ПДн) в некоммерческой организации «Фонд развития индустрии переработки отходов в Московской области» (далее – организация, Работодатель) и проведения работ по обеспечению безопасности ПДн работников организации (далее – работник).

1.3. В настоящем Положении используются следующие термины и понятия:

персональные данные работника – любая информация, относящаяся к определенному или определяемому на основании такой информации работнику, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая Работодателю в связи с трудовыми отношениями;

обработка персональных данных – сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в

том числе передача), обезличивание, блокирование, уничтожение персональных данных работников организации;

конфиденциальность персональных данных – обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным работников, требование не допускать их распространения без согласия работника или иного законного основания;

распространение персональных данных – действия, направленные на передачу персональных данных работников определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных работников в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным работников каким-либо иным способом;

использование персональных данных – действия (операции) с персональными данными, совершаемые должностным лицом организации в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении работников либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных работников, в том числе их передачи;

уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных работников или в результате которых уничтожаются материальные носители персональных данных работников;

обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному работнику;

общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия работника или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

2. ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНИЗАЦИИ

2.1. Состав персональных данных

2.1.1. В состав ПДн работников организации входят документы, содержащие информацию о паспортных данных, образовании, отношении к воинской обязанности, семейном положении, месте жительства, а также о предыдущих местах их работы и др.

2.1.2. Информация, представляемая работником при поступлении на работу в организацию, должна иметь документальную форму. При заключении трудового договора в соответствии со ст. 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет Работодателю:

паспорт или иной документ, удостоверяющий личность;

трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства, либо трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;

страховое свидетельство государственного пенсионного страхования;

документы воинского учета – для военнообязанных и лиц, подлежащих воинскому учету;

документ об образовании, о квалификации или наличии специальных знаний – при поступлении на работу, требующую специальных знаний или специальной подготовки;

свидетельство о присвоении ИНН (при его наличии у работника).

2.1.3. При оформлении работника в организацию заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные работника:

общие сведения (Ф.И.О. работника, дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные);

сведения о воинском учете;

данные о приеме на работу.

В дальнейшем в личную карточку вносятся:

сведения о переводах на другую работу;

сведения об аттестации;

сведения о повышении квалификации;

сведения о профессиональной переподготовке;

сведения о наградах (поощрениях), почетных званиях;

сведения об отпусках;

сведения о социальных гарантиях;

сведения о месте жительства и контактных телефонах.

2.1.4. В организации создаются и хранятся следующие группы документов, содержащие данные о работниках в единичном или сводном виде:

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

документация по организации работы структурных подразделений (положения о структурных подразделениях, должностные инструкции работников, приказы, распоряжения, указания руководства организации); документы по планированию, учету, анализу и отчетности в части работы с персоналом организации.

2.2. Сбор, обработка и защита персональных данных

2.2.1. Все ПДн работника организации следует получать у него самого. Если ПДн работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Должностное лицо Работодателя должно сообщить работнику организации о целях, предполагаемых источниках и способах получения ПДн, а также о характере подлежащих получению ПДн и последствиях отказа работника дать письменное согласие на их получение.

2.2.2. Работодатель не имеет права получать и обрабатывать ПДн работника организации о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни. 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.

2.2.3. Обработка указанных ПДн работников Работодателем возможна только с их согласия либо без их согласия в следующих случаях:

ПДн являются общедоступными;

ПДн относятся к состоянию здоровья работника и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия работника невозможно;

по требованию полномочных государственных органов в случаях, предусмотренных федеральным законом.

2.2.4. Работодатель вправе обрабатывать ПДн работников только с их письменного согласия.

Письменное согласие работника на обработку своих ПДн 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 ПДн;

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.

Форма заявления о согласии работника на обработку ПДн приведена в приложении № 1 к настоящему Положению.

2.2.5. Согласие работника не требуется в следующих случаях:

обработка ПДн осуществляется на основании Трудового кодекса РФ или иного федерального закона, устанавливающего ее цель, условия получения ПДн и

круг субъектов, ПДн которых подлежат обработке, а также определяющего полномочия Работодателя;

обработка ПДн осуществляется в целях исполнения трудового договора;

обработка ПДн осуществляется для статистических или иных научных целей при условии обязательного обезличивания ПДн;

обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов работника, если получение его согласия невозможно.

2.2.6. Порядок обработки, передачи и хранения ПДн.

2.2.6.1. Работник организации предоставляет достоверные сведения о себе. Работник кадрового органа проверяет достоверность сведений, сверяя данные, предоставленные работником, с имеющимися у работника документами.

2.2.6.2. В соответствии со ст. 86 главы 14 Трудового кодекса РФ в целях обеспечения прав и свобод человека и гражданина Работодатель и его представители при обработке ПДн работника должны соблюдать следующие общие требования:

обработка ПДн может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по работе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

при определении объема и содержания, обрабатываемых ПДн, Работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами;

при принятии решений, затрагивающих интересы работника, Работодатель не имеет права основываться на ПДн работника, полученных исключительно в результате их автоматизированной обработки или электронного получения;

защита ПДн работника от неправомерного их использования или утраты обеспечивается Работодателем за счет его средств в порядке, установленном федеральным законом.

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

2.3. Передача и хранение персональных данных

2.3.1. При передаче ПДн работника Работодатель должен соблюдать

следующие требования:

не сообщать ПДн 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 ПДн работника в коммерческих целях без его письменного согласия. Обработка ПДн работников в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с его предварительного согласия;

предупредить лиц, получивших ПДн 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, получившие ПДн работника, обязаны соблюдать режим конфиденциальности;

осуществлять передачу ПДн работников в пределах организации в соответствии с настоящим Положением;

разрешать доступ к ПДн работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те ПДн работника, которые необходимы для выполнения конкретной функции.

2.4. Хранение и использование персональных данных работников

2.4.1. ПДн работников обрабатываются соответствующим должностным лицом и хранятся в организации.

2.4.2. ПДн работников могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде в информационных системах (далее – ИС).

2.4.3. При получении ПДн не от работника (за исключением случаев, если ПДн были предоставлены Работодателю на основании федерального закона или если ПДн являются общедоступными) Работодатель до начала обработки таких ПДн обязан предоставить работнику следующую информацию:

наименование (фамилия, имя, отчество) и адрес оператора или его представителя;

цель обработки ПДн и ее правовое основание;

предполагаемые пользователи ПДн;

установленные федеральными законами права субъекта ПДн.

2.4.4. Обработка ПДн в ИС с использованием средств автоматизации

осуществляется в соответствии с требованиями постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2.4.5. При получении, обработке, хранении и ПДн работников организации должны соблюдаться следующие требования:

обработка ПДн работника осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации, содействия работнику в работе, в обучении и должностном росте, обеспечения личной безопасности и членов его семьи, а также в целях обеспечения сохранности принадлежащего ему имущества и имущества организации, учета результатов исполнения им должностных обязанностей;

ПДн следует получать лично у работника. В случае возникновения необходимости получения ПДн работника у третьей стороны следует известить об этом работника заранее, получить его письменное согласие и сообщить работнику о целях, предполагаемых источниках и способах получения ПДн;

запрещается получать, обрабатывать и приобщать к личному делу работника не установленные федеральными законами ПДн о его политических, религиозных и иных убеждениях, частной жизни, членстве в общественных объединениях, в том числе в профессиональных союзах;

при принятии решений, затрагивающих интересы работника, запрещается основываться на ПДн работника, полученных исключительно в результате их автоматизированной обработки или с использованием электронных носителей;

защита ПДн работника от неправомерного их использования или утраты обеспечивается за счет средств организации в порядке, установленном федеральными законами;

передача ПДн работника третьей стороне не допускается без письменного согласия работника, за исключением случаев, установленных федеральным законом.

2.4.6. В целях обеспечения защиты ПДн, хранящихся в личных делах работников, работники имеют право:

получать полную информацию о своих ПДн и обработке этих данных (в том числе автоматизированной);

осуществлять свободный бесплатный доступ к своим ПДн, включая право получать копии любой записи, содержащей ПДн работника, за исключением случаев, предусмотренных федеральным законом;

требовать исключения или исправления неверных, или неполных ПДн, а также данных, обработанных с нарушением федерального закона. Работник при отказе Работодателя исключить или исправить ПДн работника имеет право заявить в письменной форме Работодателю о своем несогласии, обосновав соответствующим образом такое несогласие. ПДн оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;

требовать от Работодателя уведомления всех лиц, которым ранее были сообщены неверные или неполные ПДн работника, обо всех произведенных в них изменениях или исключениях из них;

обжаловать в суд любые неправомерные действия или бездействие Работодателя при обработке и защите ПДн работника.

2.4.7. Лица, допущенные к обработке ПДн, в обязательном порядке под роспись знакомятся с настоящим Положением и подписывают обязательство о неразглашение информации, содержащей ПДн, по форме согласно приложению № 2 к настоящему Положению.

3. ПОРЯДОК ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Основные требования к защите персональных данных

3.1.1. Для обеспечения безопасности ПДн организация руководствуется следующими принципами:

законность: защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПДн;

системность: обработка ПДн в организации осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;

комплексность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных, систем и средств защиты в ИС;

непрерывность: защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;

своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;

преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в организации с учетом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного опыта в сфере защиты информации;

персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на работников организации в пределах их обязанностей, связанных с обработкой и защитой ПДн;

минимизация прав доступа: доступ к ПДн предоставляется работникам организации только в объеме, необходимом для выполнения их должностных обязанностей;

гибкость: обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования ИС, а также объема и состава обрабатываемых ПДн;

открытость алгоритмов и механизмов защиты: структура, технологии и алгоритмы функционирования системы защиты ПДн (далее - СЗПДн) не дают возможности преодоления имеющихся в организации систем защиты возможными нарушителями безопасности ПДн;

обоснованность и техническая реализуемость: уровень мер по защите ПДн определяется современным уровнем развития информационных технологий и средств защиты информации;

специализация и профессионализм: реализация мер по обеспечению безопасности ПДн и эксплуатация СЗПДн осуществляются работниками организации, имеющими необходимые для этого квалификацию и опыт;

эффективность процедур отбора кадров и выбора контрагентов: кадровая политика организации предусматривает тщательный подбор персонала и мотивацию работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн; минимизация вероятности возникновения угрозы безопасности ПДн;

наблюдаемость и прозрачность: меры по обеспечению безопасности ПДн должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;

непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются.

3.1.2. Организация принимает правовые, организационные и технические меры (или обеспечивает их принятие), необходимые и достаточные для обеспечения исполнения обязанностей, предусмотренных руководящими документами для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

3.1.3. При обработке ПДн с использованием средств автоматизации организацией, в частности, применяются следующие меры:

назначается ответственный за организацию обработки ПДн в организации, определяется его компетенция;

утверждаются (издаются) внутренние регулятивные документы по вопросам обработки и защиты ПДн, в том числе устанавливающие процедуры, направленные

на предотвращение и выявление нарушений законодательства, устранение последствий таких нарушений;

осуществляется внутренний контроль и (или) аудит соответствия обработки ПДн требованиям руководящих документов;

проводится оценка вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона «О персональных данных», определяется соотношение указанного вреда и принимаемых мер, направленных на обеспечение исполнения обязанностей, предусмотренных законодательством.

3.1.4. Обеспечение безопасности ПДн при их обработке в ИС достигается путем:

определения угроз безопасности ПДн. Тип актуальных угроз безопасности ПДн и необходимый уровень защищенности ПДн определяются в соответствии с требованиями законодательства и с учетом проведения оценки возможного вреда;

определения в установленном порядке состава и содержания мер по обеспечению безопасности ПДн, выбора средств защиты информации;

применения организационных и технических мер по обеспечению безопасности ПДн, необходимых для выполнения требований к защите ПДн, обеспечивающих определенные уровни защищенности ПДн, включая применение средств защиты информации, прошедших процедуру оценки соответствия, когда применение таких средств необходимо для нейтрализации актуальных угроз.

3.1.5. Обеспечение защиты ПДн при их обработке, осуществляемой без использования средств автоматизации, достигается, в частности, путем:

обособления ПДн от иной информации;

недопущения фиксации на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы;

использования отдельных материальных носителей для обработки каждой категории ПДн;

принятия мер по обеспечению раздельной обработки ПДн при несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн;

соблюдения требований к:

раздельной обработке зафиксированных на одном материальном носителе ПДн и информации, не относящейся к ПДн;

уточнению, уничтожению или обезличиванию части ПДн;

использованию типовых форм документов, характер информации в которых предполагается или допускается включение в них ПДн;

хранению ПДн, в том числе к обеспечению раздельного хранения ПДн (материальных носителей), обработка которых осуществляется в различных целях, и установлению перечня лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

3.2. Определение угроз безопасности персональным данным и мер по обеспечению их безопасности

3.2.1. Угрозы безопасности ПДн определяются по результатам оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, анализа возможных уязвимостей ИС, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

При определении угроз безопасности информации учитываются структурно-функциональные характеристики ИС, включающие структуру и состав ИС, физические, логические, функциональные и технологические взаимосвязи между сегментами ИС, с иными ИС и информационно-телекоммуникационными сетями, режимы обработки информации в ИС и в ее отдельных сегментах, а также иные характеристики ИС, применяемые информационные технологии и особенности ее функционирования.

3.2.2. Модель угроз безопасности информации должна содержать описание ИС и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей ИС, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Для определения угроз безопасности информации и разработки модели угроз безопасности информации применяются методические документы, разработанные и утвержденные ФСТЭК России и ФСБ России:

«Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утверждена заместителем директора ФСТЭК России 14.02.2008);

«Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утверждена заместителем директора ФСТЭК России 15.02.2008).

3.2.3. По результатам определения угроз безопасности информации при необходимости разрабатываются рекомендации по корректировке структурно-функциональных характеристик ИС, применению мер и средств защиты, направленные на блокирование (нейтрализацию) отдельных угроз безопасности ПДн.

Меры и средства защиты определяются в соответствии с документами, разработанными и утверждёнными ФСТЭК России и ФСБ России:

приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

4. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

4.1. Система защиты персональных данных

4.1.1. Для нейтрализации угроз безопасности ПДн, обрабатываемых в ИС, в организации создана СЗПДн. Структура СЗПДн представляет собой совокупность объектов защиты информации, органов защиты информации, используемых ими средств и методов защиты информации, в том числе криптографических, а также организационно-технических мероприятий, проводимых и планируемых в этих целях.

4.1.2. В ИС объектами защиты являются информация, содержащаяся в ИС, технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы передачи данных, технические средства обработки буквенно-цифровой, графической, видео- и речевой информации), общесистемное, прикладное, специальное программное обеспечение (ПО), информационные технологии, а также средства защиты информации (СрЗИ).

4.1.2.1. Технические средства ИС подразделяются на:

основные технические средства и системы (ОТСС) – автоматизированные системы на базе средств вычислительной техники и программные средства (общесистемное, прикладное и специальное ПО), используемые для обработки ПДн;

вспомогательные технические средства и системы (ВТСС) – технические средства и системы, не обрабатывающие непосредственно ПДн, но размещенные в помещениях, где она обрабатывается (циркулирует).

4.1.2.2. К СрЗИ относятся сертифицированные СрЗИ от несанкционированного доступа (НСД), средства защиты криптографической информации (СКЗИ), а также средства контроля эффективности защиты информации.

В качестве средств предотвращения программно-математических воздействий в ИС используются сертифицированные средства антивирусной защиты информации (САВЗ).

4.2. Органы защиты информации, обрабатываемой в ИС

4.2.1. Структуру органов защиты информации, обрабатываемой в ИС, в организации образуют:

исполнительный директор организации;

ведущий специалист организации, ответственный за организацию обработки ПДн в организации;

ответственный за защиту информации и обеспечение безопасности ПДн в ИС;

администратор информационной безопасности ИС;

ответственные за обеспечение сохранности материальных носителей ПДн в организации;

комиссия для определения классов и уровней защищённости ИС;

пользователи ИС.

4.2.2. Ответственные лица и администратор информационной безопасности ИС назначаются приказом исполнительного директора организации.

4.2.3. Исполнительный директор организации осуществляет руководство деятельностью организации по защите ПДн.

Исполнительный директор организации:

изучает и знает фактическое состояние дел по вопросам защиты ПДн;

распределяет обязанности между работниками организации по вопросам обеспечения защиты ПДн;

оценивает деятельность работников организации и эффективность мероприятий по защите информации;

издает правовые акты, утверждает нормативные и организационно-распорядительные документы по вопросам защиты информации в организации;

определяет порядок передачи ПДн контрагентам;

немедленно прекращает работы в ИС, при выявлении нарушений по защите информации;

определяет потребность и порядок финансирования мероприятий по защите ПДн на очередной финансовый год.

4.2.4. Ответственный за организацию обработки ПДн в организации отвечает за общее руководство работами по защите ПДн в организации и подготовку пользователей по вопросам защиты ПДн.

Ответственный за организацию обработки ПДн в организации имеет право отстранять пользователей, допустивших грубые нарушения требований по безопасности информации, от работы с использованием технических средств.

Ответственный за обработки ПДн в организации:

устанавливает необходимость обработки (обсуждения) ПДн на объектах информатизации организации;

в соответствии с требованиями нормативно-методических документов ФСТЭК России принимает решение о составе и содержании мероприятий по защите ПДн, а также используемых средствах защиты;

организует контроль за выполнением требований по защите ПДн и эффективностью СЗПДн;

представляет на утверждение исполнительному директору организации документацию по защите информации.

4.2.5. Ответственный за защиту информации и обеспечение безопасности ПДн в ИС.

Организует проведение работ по защите ПДн в организации и отвечает за руководство мероприятиями по защите ПДн в ИС и контроль выполнения требований по безопасности информации.

Ответственный за защиту информации и обеспечение безопасности ПДн в ИС:

ходатайствует перед исполнительным директором организации об отстранении пользователей, допустивших грубые нарушения требований по безопасности информации;

инициирует проведение служебных расследований по фактам нарушения установленных требований по безопасности ПДн;

представляет исполнительному директору организации предложения по совершенствованию принятых мер по безопасности ПДн в организации;

планирует мероприятия по обеспечению требований по безопасности ПДн;

участвует в определении угроз безопасности информации и модели нарушителя;

определяет технические средства и системы, общесистемное и специальное ПО, средства защиты информации, предполагаемые к использованию в ИС;

руководит работой по подготовке исходных данных и документации для проведения аттестационных испытаний ИС и ежегодного контроля эффективности СЗПДн;

организует разработку и контролирует своевременное внесение изменений в разрешительную систему доступа;

организует работы по классификации ИС;

организует проведение с пользователями занятий по изучению нормативных правовых и руководящих документов по вопросам защиты ПДн;

контролирует выполнение комплекса организационно-технических мероприятий по защите ПДн;

обеспечивает проведение проверок выполнения требований руководящих документов по защите ПДн;

контролирует порядок учёта, хранения и обращения с программным и информационным обеспечением, съёмными машинными носителями информации (МНИ);

организует работы по анализу и устранению причин нарушений пользователями требований по безопасности ПДн.

4.2.6. Непосредственное сопровождение СрЗИ в ИС осуществляется администратором информационной безопасности ИС. Администратор информационной безопасности отвечает за соблюдение требований по безопасности информации при эксплуатации ИС и правильность применения СрЗИ.

Администратор информационной безопасности ИС имеет право требовать от пользователей соблюдения требований по безопасности информации при работе в ИС и приостанавливать работу пользователей в случае их нарушения.

Администратор информационной безопасности ИС:

реализует установленные организационно-распорядительной и эксплуатационно-технической документацией способы защиты ПДн;

разрабатывает списки лиц, допущенных к работе в ИС;

разрабатывает предложения по разграничению доступа к информационным ресурсам, программным и техническим средствам ИС (разрешительную систему доступа);

осуществляет допуск пользователей к защищаемым ресурсам ИС в соответствии с разрешительной системой доступа;

осуществляет выполнение мер парольной защиты;

проводит с установленной периодичностью тестирование и анализ работы СрЗИ от НСД;

участвует в проведении аттестационных испытаний ИС;

проводит проверку ИС на наличие компьютерных вирусов, своевременно обновляет базы вирусных сигнатур;

производит установленным порядком резервирование системных файлов, информационных ресурсов пользователей;

принимает меры по недопущению нарушений пользователями требований по безопасности информации;

проводит анализ причин нарушений, выявленных в результате контроля выполнения требований по безопасности информации в ИС.

4.2.7. В целях дифференцированного подхода к защите ПДн проводится классификация ИС и определение уровня защищённости ПДн, обрабатываемых в ИС.

Классификация проводится комиссией, назначаемой приказом исполнительного директора организации. Председателем комиссии назначается заместитель директора по организационным вопросам, ответственный за организацию обработки ПДн в организации.

Акты классификации утверждаются исполнительным директором организации.

4.3. Организационные и технические меры по обеспечению безопасности персональных данных

4.3.1. Комплексная защита информации в ИС обеспечивается применением СрЗИ и выполнением организационных и технических мероприятий, направленных на предотвращение неправомерных доступа, копирования, предоставления или распространения информации (обеспечение конфиденциальности информации), неправомерных уничтожения или модифицирования информации (обеспечение целостности информации) и неправомерного блокирования информации (обеспечение доступности информации).

4.3.2. Организационные и технические меры по обеспечению безопасности ПДн включают в себя:

4.3.2.1. Определение перечня ПДн, цели их обработки, сроков обработки и хранения ПДн, обрабатываемых в организации.

С этой целью на ИС формируется и утверждается «Перечень персональных данных, подлежащих защите в ИСПДн «Фонд развития индустрии переработки отходов»».

4.3.2.2. Определение ответственных за обеспечение безопасности ПДн.

Для разработки и осуществления мероприятий по организации и обеспечению безопасности ПДн при их обработке в ИС приказом исполнительного директора организации назначаются лица, ответственные за защиту информации и обеспечение безопасности ПДн в ИС.

4.3.2.3. Определение круга лиц, допущенных к обработке ПДн.

Для обеспечения разрешительной системы доступа пользователей к информационным ресурсам ИС ответственным за защиту информации и обеспечение безопасности ПДн разрабатывается перечень лиц, доступ которых к ПДн, обрабатываемым в ИС, необходим для выполнения ими трудовых обязанностей (приложение № 3).

К обработке ПДн допускаются работники, изучившие настоящее Положение, соответствующие руководства и инструкции по порядку обработки информации в ИС организации.

4.3.2.4. Разработка разрешительной системы доступа персонала (пользователей) к информационным ресурсам, программным и техническим средствам ИС.

Разрешительная система доступа пользователей в организации предусматривает установление единого порядка обращения с МНИ, содержащими ПДн, определение ограничений на доступ к ним различных категорий пользователей и степени ответственности за сохранность указанных носителей сведений.

В общем виде разрешительная система доступа может представлять собой матрицу доступа пользователей к информационным ресурсам, программным и техническим средствам ИС (приложение № 4).

4.3.2.5. Организация доступа в блок помещений, где осуществляется обработка ПДн.

Помещения, в которых осуществляется обработка ПДн и (или) установлены технические средства ИС, оборудуются замками, гарантирующими надёжное закрытие помещений в нерабочее время. Дополнительно, помещения могут оборудоваться средствами контроля и управления доступом.

Вход в помещения разрешается постоянно работающим в них лицам по списку, подписанному исполнительным директором организации. Лица, не являющиеся работниками подразделения, но по характеру своей работы обязанные посещать данные помещения, включаются в список отдельно и допускаются в помещения только под контролем ответственного за это помещение.

4.3.2.6. Установление границ контролируемой зоны (КЗ) и размещение технических средств в пределах КЗ.

Границы КЗ ИС устанавливаются приказом исполнительного директора организации и наносятся на план (схему) КЗ.

4.3.2.7. Обеспечение режима безопасности ПДн при обращении с МНИ.

Порядок учёта, хранения, обращения и уничтожения МНИ, содержащих ПДн, приведён в «Инструкции по порядку учета и хранению машинных носителей конфиденциальной информации (персональных данных)» (приложение № 5).

4.3.2.8. Использование в составе ИС сертифицированных по требованиям безопасности информации СрЗИ и лицензионного программного обеспечения.

4.3.2.9. Контроль за принимаемыми мерами по обеспечению безопасности ПДн.

Контроль за принимаемыми мерами по обеспечению безопасности ПДн осуществляется в соответствии с «Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных».

4.3.2.10. Разработка организационно-распорядительной и эксплуатационной документации на ИС (инструкции администратору, пользователям, инструкции по парольной и антивирусной защите и т.д.).

4.3.2.11.Организация и подготовка к проведению аттестации ИС на соответствие требованиям по безопасности информации.

4.3.2.12.Размещение дисплеев видеомониторов, исключающее их несанкционированный просмотр.

4.3.2.13.Предотвращение внедрения в ИС программ-вирусов и программных «закладок».

4.3.2.14.Организация подготовки и повышения квалификации работников организации по вопросам защиты информации, обучение персонала.

Ежегодный инструктаж и доведение под роспись до работников требований по защите ПДн.

Повышение квалификации (переподготовка) работников, обеспечивающих безопасность ПДн, проводится установленным порядком в учебных заведениях, осуществляющих образовательную деятельность, имеющих дополнительные профессиональные программы в области информационной безопасности, согласованные с ФСТЭК России.

4.3.2.15.Установление персональной ответственности за нарушения правил обработки ПДн.

В должностные инструкции работников, допущенных к обработке ПДн, вносятся дополнения в части персональной ответственности за нарушение правил обработки ПДн.

4.4. Порядок резервирования обрабатываемой информации

4.4.1. Резервное копирование ПДн применяется для оперативного восстановления данных.

4.4.2. Резервное копирование ПДн осуществляется администратором информационной безопасности ИС в пределах своих полномочий в соответствии с графиком резервного копирования.

Резервное копирование ПДн производится в соответствии с документацией на используемое ПО.

Носители, на которые осуществляется резервное копирование, не реже 1 раза в полугодие проверяются на отсутствие сбоев.

4.4.3. Резервные копии ПДн хранятся на учтённых МНИ установленным порядком.

4.4.4. Восстановление ПДн из резервной копии производится администратором информационной безопасности в пределах своих полномочий в соответствии с документацией на используемое ПО с составлением акта.

4.4.5. Для обеспечения работоспособности ПО баз данных и СрЗИ в ИС осуществляется резервное копирование специального ПО и конфигурационных настроек программных СрЗИ.

4.4.6. Ответственность за проведение мероприятий по восстановлению работоспособности технических средств и СрЗИ возлагается на администратора информационной безопасности.

4.5. Порядок защиты от программно-математических воздействий

4.5.1. Нейтрализация угроз программно-математических воздействий на ПДн достигается выполнением требований по антивирусной защите ИС.

4.5.2. Мероприятия антивирусной защиты включают в себя:

применение САВЗ;

своевременное обновление баз вирусных сигнатур;

регламентацию действий пользователей при обнаружении заражения программными вирусами;

организация расследования инцидентов заражения ИС компьютерными вирусами.

4.5.3. В качестве САВЗ в ИС допускается использование только лицензированных программных продуктов.

4.5.4. Установку и настройку САВЗ осуществляет администратор информационной безопасности ИС. Автоматическое обновление баз вирусных сигнатур настраивается с серверов производителя САВЗ.

4.5.5. Обязательному входному антивирусному контролю подвергается вся информация, поступающая в ИС по каналам связи или на отчуждаемых МНИ.

Перед передачей ПДн в другие организации файлы, записываемые на МНИ, также проверяются на отсутствие программ-вирусов.

Полная проверка ИС на наличие вредоносного ПО проводится автоматически.

4.5.6. Скачивание из информационно-телекоммуникационных сетей общего пользования (ИТКС ОП) файлов, не имеющих отношения к выполнению функциональных обязанностей пользователя ИС, не допускается.

4.5.7. При возникновении подозрений на наличие компьютерного вируса (нетипичная работа программ, значительное снижение быстродействия ПЭВМ, искажение данных, пропадание файлов и др.), а также при сообщении САВЗ о невозможности выполнить лечение или удаление обнаруженного вируса пользователь приостанавливает работу на ПЭВМ и сообщает администратору информационной безопасности.

В случае подтверждения наличия компьютерного вируса администратор информационной безопасности ИС принимает меры к его лечению (удалению), а также, при необходимости, к локализации последствий заражения ПЭВМ путём отключения их от локальной вычислительной сети.

4.5.8. В случае воздействия на ИС компьютерных вирусов, ответственный за защиту информации и обеспечение безопасности ПДн в ИС организует проведение расследования данного инцидента с привлечением администратора информационной безопасности. По результатам расследования делаются выводы о причинах возникновения компьютерного вируса в ИС и принимаются меры для недопущения подобных происшествий в дальнейшем.

4.5.9. Ответственность за организацию антивирусного контроля в ИС возлагается на администратора информационной безопасности, а за проведение мероприятий антивирусной защиты и соблюдение требований настоящего Положения – на пользователя.

4.6. Политика парольной защиты

4.6.1. Пароли на доступ в систему генерирует, учитывает, хранит и выдаёт пользователям администратор информационной безопасности ИС. В случае отсутствия в СрЗИ встроенных механизмов генерации паролей администратор информационной безопасности составляет комбинации паролей самостоятельно.

4.6.2. К паролям предъявляются следующие требования:

длина паролей пользователей – не менее 6 символов, администраторов – не менее 8;

срок действия паролей – не более 270 суток;

мощность алфавита – не менее 60 (английский алфавит, с использованием верхнего и нижнего регистров, цифры от 0 до 9, и специальные символы [a-zA-Z0-9!@#$%?*];

отличие нового пароля от предыдущего должен отличаться не менее чем в одной позиции;

пароль не должен включать в себя легко вычисляемые сочетания символов, а также общепринятые сокращения, фамилия, имя пользователя, номер АРМ и т.д.;

периодический повтор парольных комбинаций не допускается;

количество попыток неуспешной аутентификации (неправильного ввода пароля) – 5;

время блокировки учётной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации – 15 мин.

4.6.3. Хранение паролей должно осуществляться с учётом следующих требований:

сгенерированные пароли учитываются в журнале учёта и выдачи паролей (приложение № 6);

журнал учёта и выдачи паролей хранится у администратора информационной безопасности ИС в недоступном для посторонних лиц месте;

пользователи ИС получают пароли на доступ под роспись в журнале учёта и выдачи паролей и хранят полученные пароли в тайне;

пользователям запрещается хранить пароли в виде текстовых файлов на АРМ, записанными на бумагу на рабочих столах и на элементах АРМ (монитор, клавиатура и пр.).

4.6.4. В случае необходимости доступа к защищаемым ресурсам

пользователя ИС, отсутствующего на рабочем месте, администратор информационной безопасности с разрешения исполнительного директора организации осуществляет вход в систему с идентификационными данными данного пользователя.

В отсутствие администратора информационной безопасности ИС допускается, с разрешения ответственного за организацию обработки ПДн комиссионное вскрытие сейфа с журналом учёта и выдачи паролей для последующего доступа в систему.

В этом случае администратор информационной безопасности обязан в кратчайшие сроки произвести внеплановую смену своих паролей и паролей всех пользователей для исключения их компрометации.

4.6.5. Внеплановая смена личного пароля пользователя или блокирование учётной записи пользователя в случае прекращения его полномочий (увольнение, переход на другое место работы) должна выполняться незамедлительно после окончания последнего сеанса работы данного пользователя.

Полная внеплановая смена паролей должна производиться в случае смены администратора информационной безопасности ИС.

4.6.6. Повседневный контроль за действиями пользователей при работе с паролями возлагается на администратора информационной безопасности ИС.

4.7. Правила обновления системного и прикладного программного обеспечения, технического обслуживания ИС

4.7.1. Обновление системного и прикладного программного обеспечения (СПО и ППО) проводится администратором информационной безопасности ИС.

Изменение состава программных и технических средств ИС допускается только с разрешения организации, проводившей аттестацию данной ИС, с внесением изменений в технический паспорт ИС.

4.7.2. Техническое обслуживание и ремонтные работы на технических средствах ИС проводятся специалистами подрядных организаций только под контролем администратора информационной безопасности ИС. При необходимости администратор создаёт временные учётные записи для входа в систему этих специалистов. После выполнения работ администратор обязан немедленно удалить такие учётные записи.

4.7.3. Ответственность за соблюдение требований по обеспечению безопасности ПДн при проведении технического обслуживания и ремонтных работ

на технических средствах ИС возлагается на администратора информационной безопасности ИС.

4.8. Порядок вывода ИС из эксплуатации

4.8.1. Обеспечение защиты ПДн при выводе ИС из эксплуатации или после принятия решения об окончании обработки информации осуществляется в соответствии с эксплуатационной документацией на СрЗИ ИС и организационно-распорядительными документами по защите информации и в том числе включает:

архивирование информации, содержащейся в ИС;

уничтожение (стирание) данных и остаточной информации с МНИ и (или) уничтожение МНИ.

4.8.2. Архивирование информации, содержащейся в ИС, должно осуществляться при необходимости дальнейшего использования информации в деятельности организации.

4.8.3. Уничтожение (стирание) данных и остаточной информации с МНИ производится при необходимости передачи его в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения.

4.8.4. При выводе из эксплуатации МНИ, на которых осуществлялись хранение и обработка ПДн, осуществляется физическое уничтожение этих МНИ.

5. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

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

5.1.1. Обработка ПДн считается осуществленной без использования средств автоматизации (неавтоматизированной), если их обработка производится без использования средств вычислительной техники.

5.1.2. ПДн при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях ПДн (далее – материальные носители), в специальных разделах или на полях форм (бланков).

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

5.1.4. Лица, осуществляющие обработку ПДн без использования средств автоматизации, должны быть проинформированы о факте обработки ими ПДн.

5.1.5. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее – типовая форма), должны соблюдаться следующие условия:

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

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

типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со

своими ПДн, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн;

типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

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

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

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

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

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

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

5.2.1. Обработка ПДн, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (материальных

носителей) и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

5.2.2. Необходимо обеспечивать раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.

5.2.3. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер устанавливаются приказом «Об утверждении мест хранения ПДн и лицах, ответственных за соблюдение конфиденциальности ПДн при их хранении».

ЛИСТ

ознакомления работников некоммерческой организации «Фонд развития индустрии переработки отходов в Московской области» с «Положением о порядке обработки и обеспечении безопасности персональных данных в некоммерческой организации «Фонд развития индустрии переработки отходов в Московской области»

№ п/п	Занимаемая должность	Фамилия, Инициалы	Дата ознакомления	Подпись