Положение по обработке персональных данных в государственном автономном профессиональном образовательном учреждении Свердловской области «Екатеринбургский колледж транспортного строительства»

I. Общие положения

1.1. Настоящее Положение по обработке персональных данных (далее — Положение) в Государственном автономном профессиональном образовательном учреждении Свердловской области «Екатеринбургский колледж транспортного строительства» (далее Организация) разработано в соответствии с Трудовым кодексом Российской Федерации, Конституцией Российской Федерации, Федеральным законом "Об информации, информационных технологиях и о защите информации" N 149-ФЗ от 27.07.2006 г., Федеральным законом "О персональных данных" N 152-ФЗ от 27.07.2006 г., Постановлением Правительства № 1119 от 01.11.2012г. «Об утверждении требований к защите ПДн при обработке в ИСПДн», Приказом № 21 от 18.02.2013г.. «Об утверждении состава и содержания организационных и технических мероприятий по обеспечению безопасности ПДн при обработке в ИСПДн» и иными нормативно-правовыми актами

1.2. Цель разработки Положения — определение порядка обработки персональных данных работников организации (далее – сотрудников) и иных субъектов персональных данных, обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. Порядок ввода в действие и изменения Положения.

1.3.1. Настоящее Положение вступает в силу с момента его утверждения директором организации и действует бессрочно, до замены его новым Положением.

1.3.2. Все изменения в Положение вносятся приказом.

1.4. Режим конфиденциальности персональных данных сотрудника снимается в случаях их обезличивания и по истечении 75 лет срока хранения, или продлевается на основании заключения экспертной комиссии организации, если иное не определено законом.

II. Основные понятия и состав персональных данных

2.1. Для целей настоящего Положения используются следующие основные понятия:

– персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации сотруднику, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая организации для работы

- персональные данные гражданина - любая информация, относящаяся к определенному или определяемому на основании такой информации субъекту – гражданину, в отношении которого имеются записи актов гражданского состояния, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, и ряд других сведений, подлежащих внесению в записи актов гражданского состояния в соответствии с Федеральным законом «Об актах гражданского состояния»;

– обработка персональных данных — сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных;

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

– 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 должностным лицом организации в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъектов либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

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

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

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

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

– информация — сведения (сообщения, данные) независимо от формы их представления.

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

2.2. В состав персональных данных сотрудников и студентов организации (далее субъект) входят документы, содержащие информацию о паспортных данных, образовании, отношении к воинской обязанности, семейном положении, месте жительства, состоянии здоровья, а также о предыдущих местах их работы. В состав персональных данных субъекта входят записи актов гражданского состояния, электронные записи базы данных, содержащие информацию о гражданах.

2.3. Комплекс документов, сопровождающий процесс оформления служебных или иных отношений субъекта в организации при его приеме, переводе и увольнении, зачислении, переводе и отчислении

2.3.1. Информация, представляемая субъектом 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 сотрудник поступает на работу на условиях совместительства, либо трудовая книжка у сотрудника 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 ;

- сведения о доходах, об имуществе

- иные документы, предусмотренные действующим законодательством Российской Федерации и Свердловской области.

2.3.2. Сотрудником, ответственным за ведение кадровой работы заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные сотрудника:

– общие сведения (Ф.И.О. сотрудника, дата рождения, место рождения, гражданство, образование, профессия, стаж работы, семейное положение, паспортные данные);

– сведения о воинском учете;

– данные о приеме на работу;

В дальнейшем в личную карточку вносятся:

– сведения о переводе 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.

2.3.3. В Организации создаются и хранятся следующие группы документов, содержащие данные о сотрудниках в единичном или сводном виде:

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

2.3.3.2. Должностные регламенты и должностные инструкции сотрудников, приказы руководителя организации, документы по планированию, учету, анализу и отчетности в части работы с персоналом организации.

2.4. Документы, сопровождающие составление актов гражданского состояния.

2.4.1. Информация, предоставляемая в орган записи актов гражданского состояния гражданами, в виде документов или информация, изложенная в заявлениях:

- заявления от граждан о рождении ребенка, о заключении брака, о расторжении брака, об усыновлении (удочерении), об установлении отцовства, о перемене имени, о смерти;

- заявления граждан о внесении исправлений и (или) изменений в запись акта гражданского состояния, о выдаче повторных свидетельств;

- документы, предусмотренные Федеральным законом «Об актах гражданского состояния»

- сведения в документах, удостоверяющих личность граждан, в том числе их фамилию, имя, отчество, место и дату рождения,

- национальная принадлежность граждан (указывается по желанию).

2.4.2. При составлении записи актов гражданского состояния отражаются следующие данные о гражданах:

- фамилия, имя, отчество, дата и место рождения, пол гражданина, место проживания;

- гражданство и национальность (по желанию) гражданина;

- иные сведения, предусмотренные Федеральным законом «Об актах гражданского состояния».

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

2.4.3.1. Документы, содержащие персональные данные субъекта (комплексы документов, сопровождающие процесс составления записи актов гражданского состояния.

2.4.3.2. Документы по планированию, учету, анализу и отчетности.

III. Сбор, обработка и защита персональных данных субъекта.

3.1. Порядок получения персональных данных.

3.1.1. Все персональные данные субъекта следует получать у него самого. Если персональные данные субъекта возможно получить только у третьей стороны, то субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие на обработку персональных данных. Должностное лицо работодателя должно сообщить субъекту организации о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа сотрудника дать письменное согласие на их получение.

3.1.2. Организация не имеет права получать и обрабатывать персональные данные субъекта 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 сотрудника только с его письменного согласия.

Обработка указанных персональных данных возможна только с согласия субъекта. Обработка персональных данных субъекта без их согласия осуществляется в следующих случаях:

– персональные данные являются общедоступными;

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

3.2. Порядок обработки, передачи и хранения персональных данных.

3.2.1. Сотрудник организации предоставляет сотруднику, ответственному за ведение кадровой работы достоверные сведения о себе. Сотрудник, ответственный за ведение

кадровой работы проверяет достоверность сведений, сверяя предоставленные данные с имеющимися документами.

3.2.2. В соответствии со ст. 86 ТК РФ в целях обеспечения прав и свобод человека и гражданина руководитель организации и его представители при обработке персональных данных должны соблюдать следующие общие требования:

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

3.2.2.2. При определении объема и содержания, обрабатываемых персональных данных должностное лицо организации должно руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами.

3.2.2.3. При принятии решений, затрагивающих интересы субъекта, должностное лицо организации не имеет права основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

3.2.2.4. Защита персональных данных от неправомерного их использования или утраты обеспечивается организацией за счет его средств в порядке, установленном федеральным законом. Мероприятия по обеспечению защиты персональных данных излагаются в положении по обеспечению безопасности персональных данных.

3.2.2.5. Сотрудники должны быть ознакомлены под роспись с документами организации, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

3.2.2.6. Во всех случаях отказ сотрудника от своих прав на сохранение и защиту тайны недействителен.

IV. Передача и хранение персональных данных

4.1. При передаче персональных данных субъекта организации должны соблюдать следующие требования:

4.1.1. Сообщать персональные данные третьей стороне в случаях и в порядке, установленном Федеральным законом «Об актах гражданского состояния».

4.1.2. Не сообщать персональные данные субъекта в коммерческих целях. Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи не допускается.

4.1.3. Осуществлять передачу персональных данных субъекта в пределах организации в соответствии с настоящим Положением.

4.1.4. Разрешать доступ к персональным данным только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретной функции.

4.1.5. Не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

4.1.6. Передавать персональные данные субъекта представителям субъекта в порядке, установленном Трудовым кодексом Российской Федерации или Федеральным законом «Об актах гражданского состояния», и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функции.

4.2. Хранение и использование персональных данных:

4.2.1. Персональные данные субъекта обрабатываются и хранятся в организации в информационной системе и на бумажных носителях.

4.2.2. Персональные данные субъекта могут быть получены и проходят дальнейшую обработку, передаются на хранение как на бумажных носителях, так и в электронном виде — локальной компьютерной сети и компьютерной программе бухгалтерского и кадрового учета. Персональные данные субъекта могут быть получены и проходят дальнейшую обработку, передаются на хранение как на бумажных носителях, так и в электронном виде — локальной компьютерной сети и компьютерной программе учета записей актов гражданского состояния.

V. Доступ к персональным данным

5.1. Право доступа к персональным данным субъекта имеют: руководитель организации, сотрудники, ответственные за ведение кадровой работы и работы со студентами, сотрудники бухгалтерии.

5.2. Субъект персональных данных имеет право:

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

5.2.2. Требовать уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющихся необходимыми персональных данных.

5.2.4. Получать:

– сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

– перечень обрабатываемых персональных данных и источник их получения;

– сроки обработки персональных данных, в том числе сроки их хранения;

5.2.5. Требовать извещения всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке и защите его персональных данных.

5.3. Копировать и делать выписки персональных данных сотрудника разрешается исключительно в служебных целях с письменного разрешения руководителя организации. Копировать и делать выписки персональных данных граждан разрешается только в случаях, определенных Федеральным законом «Об актах гражданского состояния».

5.4. Передача информации третьей стороне возможна только при письменном согласии субъектов персональных данных или без такового, если такая передача предусмотрена действующими законами.

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

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

ПОЛОЖЕНИЕ
об организации и проведении работ в государственном автономном профессиональном образовательном учреждении Свердловской области «Екатеринбургский колледж транспортного строительства» по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных.

1. Общие положения.

1.1. Данное «Положение об организации и проведению работ в государственном автономном профессиональном образовательном учреждении Свердловской области «Екатеринбургский колледж транспортного строительства» по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных» (далее – Положение) разработано в соответствии с Законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных, Постановлением Правительства № 1119 от 01.11.2012г. «Об утверждении требований к защите ПДн при обработке в ИСПДн», Приказом № 21 от 18.02.2013г. «Об утверждении состава и содержания организационных и технических мероприятий по обеспечению безопасности ПДн при обработке в ИСПДн» в целях обеспечения безопасности персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных (далее – ИСПДн).

1.2. Положение определяет порядок работы персонала ИСПДн в части обеспечения безопасности ПДн при их обработке, порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений, порядок приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления, порядок обучения персонала практике работы в ИСПДн, порядок проверки электронного журнала обращений к ИСПДн, порядок контроля соблюдения условий использования средств защиты информации, предусмотренные эксплуатационной и технической документацией, правила обновления общесистемного и прикладного программного обеспечения, правила организации антивирусной защиты и парольной защиты ИСПДн, порядок охраны и допуска посторонних лиц в защищаемые помещения.

2. Порядок работы персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн.

Настоящий порядок определяет действия персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн.

2.1. Допуск пользователей для работы на компьютерах ИСПДн осуществляется на основании приказа, который издается руководителем Государственного автономного профессионального образовательного учреждения Свердловской области «Екатеринбургский колледж транспортного строительства» (далее руководитель), и в соответствии со списком лиц допущенных к работе в ИСПДн. С целью обеспечения

ответственности за ведение, нормальное функционирование и контроль работы средств защиты информации в ИСПДн руководителем назначается сотрудник, ответственный за за защиту информации; с целью контроля выполнения необходимых мероприятий по обеспечению безопасности ответственный за защиту информации;

2.2. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. Полномочия пользователей к информационным ресурсам определяются в матрице доступа, утверждаемой руководителем организации. При этом для хранения информации, содержащей ПДн, разрешается использовать только машинные носители информации, учтенные в Журнале учета машинных носителей.

2.3. Пользователь несет ответственность за правильность включения и выключения средств вычислительной техники (СВТ), входа в систему и все действия при работе в ИСПДн.

2.4. Вход пользователя в систему может осуществляться по выдаваемому ему электронному идентификатору или по персональному паролю.

2.5. Запись информации, содержащей ПДн может осуществляться пользователем на съемные машинные носители информации, соответствующим образом учтенные в Журнале учета машинных носителей.

2.6. При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов с использованием штатных антивирусных программ, установленных на компьютерах ИСПДн. В случае обнаружения вирусов пользователь обязан немедленно прекратить их использование и действовать в соответствии с требованиями данного Положения.

2.7. Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и ***обязан***:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;
- знать и строго выполнять правила работы со средствами защиты информации, установленными на компьютерах ИСПДн;
- хранить в установленном порядке свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу);
- выполнять требования Положения по организации антивирусной защиты в полном объеме.

Немедленно известить ответственного за защиту информации в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

- нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на составляющих узлах и блоках СВТ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее - НСД) к данным защищаемым СВТ;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию СВТ, выхода из строя или неустойчивого функционирования узлов СВТ или периферийных устройств (сканера, принтера и т.п.), а также перебоев в системе электроснабжения;
- некорректного функционирования установленных на компьютеры технических средств защиты;
- непредусмотренных отводов кабелей и подключенных устройств.

Пользователю категорически ***запрещается***:

- использовать компоненты программного и аппаратного обеспечения ПЭВМ в неслужебных целях;

- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения;

- осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;

- записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных машинных носителях информации (гибких магнитных дисках и т.п.);

- оставлять включенным без присмотра компьютер, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

- оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения);

- размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации.

2.8. Ответственный за защиту информации обязан:

- знать состав основных и вспомогательных технических систем и средств (далее - ОТСС и ВТСС) установленных и смонтированных в ИСПДн, перечень используемого программного обеспечения (далее - ПО) в ИСПДн;

- контролировать целостность печатей (пломб, защитных наклеек) на периферийном оборудовании, защищенных СВТ и других устройствах;

- производить необходимые настройки подсистемы управления доступом установленных в ИСПДн СЗИ от НСД и сопровождать их в процессе эксплуатации, при этом:

- реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру и т.д.);

- вводить описания пользователей ИСПДн в информационную базу СЗИ от НСД;

- своевременно удалять описания пользователей из базы данных СЗИ при изменении списка допущенных к работе лиц;

- проводить инструктаж сотрудников - пользователей компьютеров по правилам работы с используемыми техническими средствами и системами защиты информации;

- обеспечивать постоянный контроль выполнения сотрудниками установленного комплекса мероприятий по обеспечению безопасности информации в ИСПДн;

- осуществлять контроль порядка создания, учета, хранения и использования резервных и архивных копий массивов данных;

- настраивать и сопровождать подсистемы регистрации и учета действий пользователей при работе в ИСПДн;

- вводить в базу данных СЗИ от несанкционированного доступа описания событий, подлежащих регистрации в системном журнале;

- проводить анализ системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам не реже одного раза в 10 дней;

- организовывать печать файлов пользователей на принтере и осуществлять контроль соблюдения установленных правил и параметров регистрации и учета бумажных носителей информации. Сопровождать подсистемы обеспечения целостности информации в ИСПДн;

- периодически тестировать функции СЗИ от НСД, особенно при изменении программной среды и полномочий исполнителей;

- восстанавливать программную среду, программные средства и настройки СЗИ при сбоях;

- вести две копии программных средств СЗИ от НСД и контролировать их работоспособность;
- контролировать отсутствие на магнитных носителях остаточной информации по окончании работы пользователей;
- периодически обновлять антивирусные средства (базы данных), контролировать соблюдение пользователями порядок и правила проведения антивирусного тестирования:
- проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИСПДн и осуществления несанкционированного доступа к информации и техническим средствам вычислительной техники;
- сопровождать подсистему защиты информации от утечки за счет побочных электромагнитных излучений и наводок, контролировать соблюдение требований по размещению и использованию технических средств ИСПДн;
- обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания ИСПДн и отправке его в ремонт (контролировать затирание конфиденциальной информации на магнитных носителях с составлением соответствующего акта);
- присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию ИСПДн;
- поддерживать установленный порядок проведения антивирусного контроля согласно требований настоящего Положений в случае отказа средств и систем защиты информации принимать меры по их восстановлению;
- вести документацию на ИСПДн в соответствии с требованиями нормативных документов.

2.9. Ответственный за защиту информации имеют право:

- требовать от сотрудников - пользователей ИСПДн соблюдения установленной технологии обработки информации и выполнения инструкций по обеспечению безопасности и защите информации в ИСПДн;
- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, модификации, порчи защищаемой информации и технических компонентов ИСПДн;
- требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;
- участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

3. Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных, защищаемой информации и средств защиты информации.

3.1. Настоящий порядок определяет организацию резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации.

3.2. Ответственный за защиту информации ***обязан*** осуществлять периодическое резервное копирование конфиденциальной информации.

3.3. Еженедельно, по окончанию работы с конфиденциальными документами (содержащими персональные данные) на компьютере, пользователь, при отсутствии ответственного за защиту информации, обязан создавать резервную копию конфиденциальных документов на зарегистрированный носитель, создавая тем самым резервный электронный архив конфиденциальных документов.

3.4. Перед резервным копированием пользователь или ответственный за защиту информации обязан проверить электронный носитель на отсутствие вирусов.

3.5. Запрещается запись посторонней информации на электронные носители резервной копии.

3.6. Порядок создания резервной копии:

- вставить в компьютер зарегистрированный электронный носитель (ЖМД, ГМД, CD-ROM, USB накопитель, другие) для резервного копирования;
- выбрать необходимый каталог (файл) для создания резервного архива;
- при использовании систем управления базами данных необходимо создать файл с резервной копией защищаемой информации с помощью встроенных средств системы;
- выполнить процедуру создания резервной копии;
- произвести копирование на отчуждаемый носитель;
- произвести отключение отчуждаемого носителя и, создав не обходимые записи в журналах убрать носитель в хранилище.

3.7. Хранение отчуждаемого носителя с резервной копией защищаемой информации осуществляется в специальном металлическом хранилище совместно с ключевой и аутентифицирующей информацией.

3.8. При восстановлении работоспособности программного обеспечения сначала осуществляется резервное копирование защищаемой информации, затем производится полная деинсталляция некорректно работающего программного обеспечения.

3.9. Восстановление программного обеспечения производится путем его инсталляции с использованием эталонных дистрибутивов, хранение которых осуществляется ответственным за защиту информации в специальном хранилище.

3.10. При необходимости ремонта технических средств, с них удаляются опечатывающие пломбы и по согласованию с ответственным за защиту информации и, при условии проведенной аттестации информационной системы, представителем организации, проводившей аттестацию, оборудование передается в сервисный центр производителя. Ремонт носителей защищаемой информации не допускается. Неисправные носители с защищаемой информацией подлежат уничтожению в соответствии с порядком уничтожения носителей защищаемой информации. Работа с использованием неисправных технических средств запрещается.

3.11. При работе на компьютерах ИСПДн рекомендуется использовать источники бесперебойного питания, с целью предотвращения повреждения технических средств и(или) защищаемой информации в результате сбоев в сети электропитания.

3.12. При восстановлении работоспособности средств защиты информации следует выполнить их настройку в соответствии с требованиями безопасности информации, изложенными в техническом задании на создание системы защиты персональных данных. Настройку данных средств должен выполнять сотрудник организации, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

3.13. Восстановление средств защиты информации производится с использованием эталонных сертифицированных дистрибутивов, которые хранятся в хранилище. После успешной настройки средств защиты информации необходимо выполнить резервное копирование настроек данных средств с помощью встроенных в них функций на зарегистрированный носитель.

3.14. Ответственность за проведение резервного копирования в ИСПДн в соответствии с требованиями настоящего Положения возлагается на ответственного за защиту информации

3.15. Ответственность за проведение мероприятий по восстановлению работоспособности технических средств и программного обеспечения баз данных возлагается на ответственного за защиту информации.

3.16. Ответственность за проведение мероприятий по восстановлению средств

защиты информации (далее – СЗИ) возлагается на ответственного за защиту информации