УТВЕРЖДАЮ
Директор
_____ Л.В. Суслопарова
(подпись)
«_8_» ____08_____ 2017г.

Положение об обработке и обеспечении безопасности персональных данных в Муниципальном бюджетном общеобразовательном учреждении «Биотехнологический лицей № 21»

Сокращения, условные обозначения
ИСПДн – информационная система персональных данных
НСД – несанкционированный доступ
ПДн – персональные данные
Термины и определения

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

Персональные данные работника – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника.

Персональные данные обучающихся – информация, необходимая образовательному учреждению в связи с отношениями, возникающими между обучающимся, его родителями (законными представителями) и образовательным учреждением.

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.

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.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Несанкционированный доступ–доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

1. Назначение и область применения

Настоящее Положение об обработке и обеспечении безопасности персональных данных (далее - Положение) Муниципального бюджетного общеобразовательного учреждения «Биотехнологический лицей № 21» (далее - Организация) разработано в соответствии с Конституцией Российской Федерации, Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»,постановлениями Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Трудовым кодексом Российской Федерации, иными нормативными правовыми актами, действующими на территории Российской Федерации.

Положение определяет порядок обработки и обеспечения безопасности персональных данных (ПДн) в Организации, устанавливает процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений, определяет права, обязанности и ответственность лиц, допущенных к обработке ПДн и ответственных за организацию обработки ПДн.

Действие настоящего Положения распространяется на все процессы обработки персональных данных в Организации, как с использованием средств автоматизации, так и без использования таких средств, на все структурные подразделения и работников Организации, участвующих в таких процессах, а также на информационные системы Организации, используемые в процессах обработки ПДн.

Настоящее Положение вступает в силу с момента его утверждения директором Организации и действует бессрочно, до замены его новым Положением. Все изменения в Положение вносятся приказом.

Положение обязательно для соблюдения всеми работниками Организации и должно быть доведено до них под роспись.

Контроль над соблюдением настоящего Положения, осуществляется лицом, ответственным за организацию обработки персональных данных в Организации, которое назначается приказом директора Организации.

2. Принципы обработки персональных данных

Обработка персональных данных осуществляется Организацией на законной и справедливой основе и ограничивается достижением конкретных, заранее определенных и законных целей. Организацией не допускается обработка персональных данных, несовместимая с целями сбора персональных данных и объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

Обработке подлежат только персональные данные, которые отвечают целям их обработки. Содержание и объем обрабатываемых Организацией персональных данных соответствуют заявленным целям обработки, избыточность! обрабатываемых данных не допускается.

При обработке персональных данных Организацией обеспечивается точность персональных данных, их достаточность и в необходимых случаях актуальность по отношению к целям обработки персональных данных. Организацией принимаются необходимые меры (обеспечивается их принятие) по удалению или уточнению неполных или неточных персональных данных.

Хранение персональных данных Организацией осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели об-

работки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

При определении состава обрабатываемых персональных данных субъектов персональных данных Организация руководствуется минимально необходимым составом персональных данных для достижения целей получения персональных данных.

3. Условия обработки персональных данных

Обработка персональных данных осуществляется в соответствии с целями, заранее определенными и заявленными при сборе персональных данных, а также полномочиями Организации, определенными действующим законодательством Российской Федерации и договорными отношениями с Организацией.

Получение и обработка персональных данных в случаях, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», осуществляется Организацией с письменного согласия субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного электронной подписью.

Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено Федеральным законом от27 июля 2006 г. № 152-ФЗ «О персональных данных». В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются Организацией.

Организация вправе обрабатывать персональные данные без согласия субъекта персональных данных (или при отзыве субъектом персональных данных согласия на обработку персональных данных) при наличии оснований, указанных в Федеральном законе от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, Организацией не осуществляется.

Сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (биометрические персональные данные) и сведения о состоянии здоровья, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных или иных оснований, предусмотренных федеральным законодательством.

Персональные данные субъекта могут быть получены Организацией от лица, не являющегося субъектом персональных данных, при условии предоставления Организации подтверждения наличия оснований, указанных в Федеральном законе от 27 июля 2006г. №152-ФЗ «О персональных данных» или иных оснований, предусмотренных федеральным законодательством.

Право доступа к персональным данным субъектов персональных данных на бумажных и электронных носителях имеют работники Организации в соответствии с их должностными обязанностями.

Организацией не осуществляется трансграничная передача персональных данных и не принимаются решения, основанные исключительно на автоматизированной обработке персональных данных субъекта.

4. Цели обработки персональных данных

В соответствии с принципами и условиями обработки персональных данных, Орга-

низацией определены цели обработки персональных данных:

- организация учебного процесса и контроль качества образования;
- учет и анализ успеваемости учащихся, организация информирования родителей (законных представителей) об успеваемости детей;
- заключении трудовых договоров.

5. Особенности обработки персональных данных

Обработка персональных данных Организацией осуществляется как с использованием средств автоматизации, так и без использования таких средств.

При обработке персональных данных Организация осуществляет следующие действия с персональными данными: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

6. Порядок обработки персональных данных

6.1. Источники получения персональных данных

Организация получает ПДн из следующих источников:

- непосредственно от субъекта ПДн;
- от третьей стороны, в целях исполнения договорных обязательств или исполнения требований нормативных документов РФ.

Если предоставление ПДн является обязательным в соответствии с федеральным законом и субъект ПДн отказывается их предоставить, необходимо разъяснить субъекту ПДн юридические последствия такого отказа.

Если ПДн получены не от субъекта ПДн, то до начала обработки таких ПДн необходимо предоставить субъекту ПДн следующую информацию:

- цель обработки ПДн и ее правовое основание;
- предполагаемые пользователи ПДн;
- установленные законодательством права субъекта ПДн;
- источник получения ПДн.

Указанная информация может не предоставляться в следующих случаях:

- субъект ПДн уже уведомлен об осуществлении обработки его ПДн соответствующим оператором;
- ПДн получены на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн;
- ПДн сделаны общедоступными субъектом ПДн или получены из общедоступного источника;
- предоставление субъекту ПДн указанных сведений нарушает права и законные интересы третьих лиц.

6.2. Перечень процессов и категорий персональных данных, обрабатываемых в Организации

Перечень процессов обработки персональных данных, категории субъектов ПДн, чьи данные обрабатывается в Организации, и состав таких данных закреплены в Перечне процессов и персональных данных, обрабатываемых в Организации.

6.3. Способы обработки персональных данных

Обработка персональных данных в Организации осуществляется как автоматизированным способом, так и без использования средств автоматизации (на бумажных носителях) работниками Организации, доступ которых к персональным данным, необходим для выполнения ими служебных (трудовых) обязанностей.

Документы, содержащие персональные данные, создаются путём:

- копирования оригиналов (паспорт, доверенность, свидетельство ИНН, пенсионное свидетельство и т.д.);
- внесения сведений в учётные формы на бумажных и электронных носите-

лях;

- внесения сведений в информационные системы персональных данных;
- получения оригиналов необходимых документов (трудовая книжка, анкета, и т.д.).

Работники Организации, допущенные к обработке персональных данных в информационных системах персональных данных, несут ответственность за достоверность и полноту введенной информации.

6.4. Порядок обработки отдельных документов (типовых форм), содержащих персональные данные

При использовании внутренних типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее - типовая форма), должны выполняться следующие условия:

- в типовые формы или связанные с ними документы (инструкции по заполнению, карточки, реестры и журналы) включаются следующие сведения:
  - цели обработки ПДн;
  - наименование и адрес Организации;
  - Ф. И. О. адрес места жительства субъекта ПДн;
  - источник получения ПДн (третьи стороны, субъект ПДн и т.п.);
  - сроки обработки ПДн;
  - перечень действий, которые будут совершаться с ПДн;
- в случае необходимости получения согласия на обработку ПДн (например, отсутствует договор, в рамках исполнения которого необходима обработка ПДн), во внутреннюю типовую форму включается поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн;
- внутренняя типовая форма составляется таким образом, чтобы каждый из субъектов, чьи ПДн содержатся в типовой форме, имел возможность ознакомиться со своими ПДн, не нарушая прав и законных интересов иных субъектов ПДн;
- во внутренней типовой форме не допускается объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо , несовместимы.

6.5. Хранение, блокирование и уничтожение персональных данных

Персональные данные, позволяющие определить субъекта, хранятся не дольше, чем этого требуют цели их обработки, и подлежат уничтожению по достижении целей обработки персональных данных, или утраты необходимости в их достижении. Законодательством РФ могут устанавливаться специальные сроки хранения отдельных видов документов, содержащих ПДн. В этом случае указанные документы подлежат уничтожению по истечению установленных сроков хранения.

Документы, содержащие ПДн, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.

Конкретные обязанности по хранению документов возлагаются на лиц, осуществляющих обработку ПДн, в соответствии с их трудовыми функциями и закрепляются в трудовых договорах, должностных инструкциях и иных регламентирующих документах Организации.

Порядок учета материальных носителей ПДн определен в разделе 9.5.настоящего Положения.

Организация блокирует обрабатываемые ПДн при выявлении недостоверности обрабатываемых ПДн или неправомерных действий в отношении субъекта в следующих случаях:

- по требованию субъекта ПДн;
- по требованию уполномоченного органа по защите прав субъектов ПДн (Роскомнадзора);
- по результатам внутренних контрольных мероприятий.

Организация уничтожает персональные данные в следующих случаях:

- по достижению цели обработки персональных данных (в том числе по истечении установленных сроков хранения);
- отзыва субъектом согласия на обработку своих персональных данных, | когда это согласие является обязательным условием обработки ПДн;
- невозможности устранения допущенных при их обработке нарушений;
- получения соответствующего предписания от уполномоченного органа по защите прав субъектов ПДн.

7. Доступ к персональным данным

7.1. Предоставление прав доступа к персональным данным

Персональные данные, обрабатываемые в Организации, относятся к информации ограниченного доступа. Доступ к персональным данным должен быть ограничен, в том числе путем определения перечня лиц, доступ которых к персональным данным, необходим для выполнения ими служебных (трудовых)обязанностей.

При получении доступа к ПДн работники Организации подписывают Соглашение о неразглашении персональных данных. Отсутствие подписанного Соглашения не является основанием для допустимости нарушения работником конфиденциальности персональных данных, снятия или уменьшения его ответственности за нарушение норм, регулирующих обработку и обеспечение безопасности ПДн.

Организация в ходе своей деятельности предоставляет доступ к ПДн третьим сторонам в целях исполнения договорных обязательств перед субъектами ПДн, а также с целью обеспечения своей деятельности или исполнения требований нормативных документов РФ. Такой доступ может быть предоставлен третьим сторонам только после подписания соглашения о неразглашении персональных данных (если обязанность третьего лица по соблюдению конфиденциальности персональных данных заранее не установлена нормативными документами РФ).

Права доступа к персональным данным в Организации предоставляется на постоянной или временной основе.

Право доступа к персональным данным на постоянной основе имеют работники Организации, непосредственно занимающиеся обработкой ПДн.

Основанием для оформления работнику временного (разового) права доступа к ПДн является выполнение производственного задания, в рамках которого работнику объективно необходим доступ к ПДн.

Доступ работников Организации к обработке ПДн осуществляется после:

- ознакомления с положениями законодательства Российской Федерации о персональных данных, документами Организации, устанавливающими порядок обработки и обеспечения безопасности персональных данных, а также об их правах и обязанностях в этой области;
- прохождения внутреннего обучения (инструктажа) по правилам обработки и обеспечения безопасности ПДн;
- ознакомления с эксплуатационной документацией к средствам защиты информации, применяемым в рамках системы защиты персональных данных;
- ознакомления с ответственностью за нарушение установленных в Организации правил обработки и обеспечения безопасности ПДн.

Доступ работников Организации к ИСПДн ограничен системой разграничения прав доступа, реализуемой в рамках системы защиты персональных данных с использованием технических и организационных мероприятий.

Каждый пользователь имеет индивидуальную учетную запись, которая определяет его права и полномочия в ИСПДн. Информация об учетной записи не может быть передана другим лицам. Пользователь несет персональную ответственность за конфиденциальность сведений собственной учетной записи.

Запрещается использование для доступа к ИСПДн учетных записей других пользователей.

Заведение, активацию, блокирование и уничтожение учетных записей пользователей ИСПДн осуществляет Администратор ИСПДн, который назначается приказом директора Организации.

Все работники, допущенные к обработке ПДн, обязаны соблюдать конфиденциальность ПДн как в течение срока действия трудового договора, так и после его прекращения в течение срока, установленного соглашением о неразглашении персональных данных.

7.2. Изменение прав доступа к персональным данным

Основанием для изменения прав доступа работника к ПДн является:

- перевод работника на должность, функциональные обязанности которой требуют расширения или сокращения прав доступа к ПДн;
- изменение процесса (процессов) обработки ПДн в Организации и/или требований законодательства РФ в области обработки и обеспечения безопасности ПДн, при которых расширяются или сокращаются права доступа к ПДн, закрепленные за определенными должностями работников;
- изменения в организационно-штатной структуре Организации;
- служебная необходимость, в рамках которой работнику требуется временное (разовое) расширение прав на обработку ПДн;
- проведение в отношении работника служебного расследования, в рамках которого такому работнику необходимо ограничить права доступа к ПДн.

7.3. Прекращение прав доступа к персональным данным

Основанием для прекращения прав доступа работника к ПДн является:

- нарушение работником требований законодательства Российской Федерации о персональных данных, локальных актов Организации в области обработки и обеспечения безопасности ПДн;
- перевод работника на другую должность или в другое структурное подразделение, не требующих участия в процессах обработки ПДн;
- достижение заявленных целей, для которых работнику предоставлялся временный (разовый) доступ к ПДн;
- прекращение трудовых отношений с работником.

8. Предоставление персональных данных третьей стороне

Предоставление ПДн третьим сторонам осуществляется только с предварительного письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных законодательством Российской Федерации, в частности Федеральным законом «Об обязательном пенсионном страховании в Российской Федерации, Федеральным законом «Об основах обязательного социального страхования, Федеральным законом «Об обязательном медицинском страховании в Российской Федерации».

Существенным условием договоров с третьими сторонами, в рамках исполнения которых передаются ПДн, является обязанность соблюдения сторонами мер обеспечения безопасности ПДн при их обработке. Кроме того, в договорах в обязательном порядке определяется порядок передачи ПДн.

Организация с согласия субъекта может поручать обработку ПДн третьим сторонам, а также выступать в роли лица, осуществляющего обработку ПДн по поручению других операторов ПДн.

В случае если Организация поручает обработку третьей стороне, в поручении на обработку ПДн должны быть в обязательном порядке определены:

- перечень действий (операций) с персональными данными, которые будут совершаться третьей стороной;
- цели обработки (цели не должны противоречить целям, заявленным перед субъектом - в договоре с оператором, в согласии и т. д.);
- обязанность третьей стороны соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке;

- требования к защите ПДн.

При обработке ПДн по поручению третьих сторон Организацией соблюдаются установленные соответствующими поручениями (договорами) требования к обеспечению безопасности ПДн.

Федеральным законом может устанавливаться обязанность Организации непосредственно направлять информацию, содержащую ПДн, третьим лицам (отчетность, налоговые декларации и т.д.) либо право третьих лиц запрашивать указанную информацию в пределах их полномочий.

В последнем случае передача информации осуществляется на основании письменных мотивированных запросов, оформленных на официальных бланках за подписью уполномоченного должностного лица. Запрос должен содержать цели и правовые основания затребования информации, срок предоставления такой информации, если иное не установлено законом.

Ответы на запросы направляются законным получателям ПДн только в письменном виде и только в затребованном объеме.

Получателями ПДн на законном основании, в том числе являются:

- Фонд социального страхования РФ;
- Пенсионный фонд РФ;
- Федеральная Налоговая Служба;
- Федеральная инспекция труда;
- иные органы надзора и контроля за соблюдением законодательства о
- труде;
- правоохранительные и судебные органы.

Организация обязано предоставить персональные данные по письменному запросу субъекта персональных данных или его законного представителя.

Копии документов, содержащих ПДн, выдаются Организацией в срок не позднее тридцати дней со дня подачи письменного заявления об их выдаче.

При выдаче документов для ознакомления, а также запрашиваемых копий и справок, работник, занимающийся обработкой ПДн, обязан удостовериться в личности запрашивающего (или его представителя) и потребовать предоставление документа, подтверждающего соответствующие полномочия.

9. Обращение с материальными носителями персональныхданных

9.1. Виды носителей

Персональные данные в Организации хранятся на материальных носителяхдвух видов:

- машинные (электронные) носители персональных данных
- бумажные носители персональных данных.

Организация обработки поступивших и создаваемых документов, содержащих персональные данные, осуществляется в соответствии с принятыми в Организации нормами документооборота.

9.2. Хранение бумажных носителей персональных данных

Бумажные (документальные) носители ПДн должны храниться в Организации в условиях, исключающих несанкционированный доступ в них посторонних лиц, в сейфах или запираемых металлических шкафах (ящиках).

Хранение бумажных (документальных) носителей ПДн вместе с документами общего доступа запрещается, за исключением случаев, когда документы общего доступа являются приложениями к бумажным (документальным) носителям ПДн.

Запрещается совместное хранение бумажных (документальных) носителей ПДн, обработка которых осуществляется в различных целях.

Для каждой категории персональных данных должны быть определены и занесены в Реестр места хранения бумажных носителей этой категории. В Реестре мест хранения носителей персональных данных указывают:

- наименование процесса, цели обработки и категории субъектов персональных данных;
- категории персональных данных;
- место хранения (номер или наименование помещения, в котором хранятся бумажные носители, номер шкафа (сейфа) в котором хранятся бумажные носители);
- перечень документов;
- перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

9.3. Уничтожение бумажных носителей персональных данных

Основанием для уничтожения бумажных (документальных) носителей ПДн является:

- достижение целей обработки, в том числе истечение сроков обязательного хранения, установленных законодательством РФ;
- отзыв согласия субъекта на обработку его ПДн;
- получение соответствующего запроса от субъекта ПДн;

Уничтожение бумажных (документальных) носителей ПДн производится способом, исключающим возможность восстановления информации.

9.4. Использование и обеспечение сохранности машинных носителей персональных данных

Для обработки (хранения) персональных данных в информационных системах персональных данных Организации используются машинные носители в роли которых могут выступать неотчуждаемые носители (жесткие диски) или отчуждаемые (съемные) носители информации (такие как: внешние жесткие диски гибкие магнитные диски, USB флэш-накопители, карты флэш-памяти, оптические носители и др.)

В целях предотвращения нарушения целостности и утери персональных данных, обрабатываемых в информационных системах персональных данных Организации, пользователь ИСПДн должен осуществлять резервное копирование необходимой информации по мере ее обновления на отчуждаемые (съемные) носители информации

Для обеспечения сохранности машинных носителей должен быть организован режим обеспечения безопасности помещений, в которых размещены технические средства информационных систем персональных данных, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

Системные блоки с жесткими дисками, на которых хранятся персональные данные должны быть опечатаны лицом ответственным за организацию обработки персональных данных. Хранение отчуждаемых (съемных) носителей персональных данных должно осуществляться в сейфах или запираемых металлических шкафах (ящиках).

Несанкционированный вынос машинных носителей из Организациизапрещен.

9.5. Учет машинных носителей персональных данных

Все машинные носители, используемые для обработки и хранения персональных данных, регистрируются и учитываются в Журнале учета машинных носителей персональных данных (приложение 1).

В Журнале указывают:

- Ф.И.О. работника;
- дата получения и подпись работника;
- номер машинного носителя;
- тип носителя;
- дата возврата и подпись работника;
- отметка об уничтожении;
- дата уничтожения и подпись Администратора ИСПДн.

Ответственность за ведение Журнала несут Администраторы ИСПДн.

9.6. Уничтожение машинных носителей персональных данных

В случае выхода из строя или принятия решения о прекращении использования машинного носителя в процессах обработки персональных данных такой носитель уничтожается или с него стираются персональные данные (способом исключающим возможность восстановление данных).

10. Защита персональных данных

10.1. Общие положения

Защита персональных данных представляет собой комплекс мер технического, организационного и организационно-технического характера, направленных на обеспечение конфиденциальности, целостности и доступности ПДн

Организация при обработке персональных данных принимает необходимыеправовые, организационные и технические меры или обеспечивает их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления,распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

К таким мерам, в частности, относятся:

- назначение лица, ответственного за организацию обработки персональных данных;
- осуществление внутреннего контроля за соблюдением законодательства Российской Федерации о персональных данных, в том числе требований к защите L персональных данных;
- ознакомление работников Оператора с положениями законодательства Российской Федерации о персональных данных, локальными актами по вопросам I обработки персональных данных, требованиями к защите персональных данных;
- издание локальных актов по вопросам обработки персональных данных и локальных актов, устанавливающих процедуры, направленные на предотвращение и выявления нарушений законодательства РФ;
- определение угроз безопасности персональных данных и необходимого | уровня защищённости персональных данных, при их обработке в информационных системах персональных данных;
- применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;
- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации;
- осуществление оценки эффективности применяемых мер по обеспечению безопасности персональных данных.

В Организации защите подлежат:

- документы на бумажных носителях, содержащие персональные данные;
- персональные данные в электронном виде, обрабатываемые в информационных системах персональных данных.

При обработке ПДн в информационных системах персональных данных их jзащита осуществляется с учетом положений документа «Треоования к защите персональных данных при их обработке в информационных системах персональных данных» (утв. Постановлением Правительства РФ от 1 ноября 2012 г. №1119).

Для каждой ИСПДн Организации должна быть разработана Модель угроз и определен требуемый уровень защищенности персональных данных при их обработке в ИСПДн.

При обработке ПДн без использования средств автоматизации (на бумажных носителях) защита персональных данных осуществляется с учетом требований настоящего Положения и «Положения об особенностях обработки персональных данных, осуществля-

емой без использования средств автоматизации» (утв.1 Постановлением Правительства РФ от 15 сентября 2008 г. №687).

Все работники Организации, участвующие в обработке ПДн, в обязательном порядке должны проходить инструктаж по следующим направлениям:

- общие вопросы обеспечения информационной безопасности в Организации;
- правила обработки ПДн;
- правила использования средств защиты информации;
- ответственность за нарушение правил обработки и обеспечения безопасности ПДн.

10.2. Система защитыперсональных данных

Обеспечение безопасности персональных данных при их обработке в ИСПДн Организации обеспечивается с помощью системы защиты персональных данных (далее - СЗПДн).

Объектами защиты ИСПДн являются персональные данные, содержащиеся в информационной системе, технические средства (в том числе средства вычислительной техники, машинные носители персональных данных, средства и системы связи и передачи данных), общесистемное, прикладное, специальное программное ооеспечение, информационные технологии, а также средства защиты информации.

Целью реализации СЗПДн является защита ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении ПДн.

СЗПДн включает в себя организационные и технические меры, определенные с учетом актуальных для ИСПДн угроз безопасности персональных данных и информационных технологий, используемых в ИСПДн.

Целью реализации в СЗПДн технических мер является обеспечение конфиденциальности, целостности и доступности ПДн в процессе их обработки и хранения в ИСПДн, предотвращение утечки и НСД к ПДн при их обработке в ИСПДн.

В рамках технических мер в составе СЗПДн используются средства защиты информации, сертифицированные по требованиям безопасности информации, в случае когда применение таких средств необходимо для нейтрализации актуальных угроз.

Целями организационных мероприятий по защите ПДн в Организациияявляются:

- исключение непреднамеренных действий работников Организации, приводящих к утечке, искажению, уничтожению ПДн, в том числе ошибки эксплуатации ИСПДн;
- сведение к минимуму возможности нарушения свойств безопасности ПДн с помощью любых средств, не связанных непосредственно с эксплуатацией ИСПДн (физический вынос ПДн на машинных носителях);
- исключение ознакомления работников с ПДн, если это не предусмотрено их должностными обязанностями.

В рамках мер физической защиты, в соответствии с установленным порядком пропускного и внутриобъектового режима в Организации, для обеспечения безопасности ПДн применяются следующие меры и средства:

- организация режима обеспечения безопасности помещений, в которых размещены технические средства ИСПДн, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения
- системы пожарной сигнализации и пожаротушения;
- исключение возможности просмотра неуполномоченными лицами текстовой и графической информации, содержащей персональные данные, с устройств отображения информации (мониторов).

Разработка СЗПДн и ее внедрение (в том числе внедрение средств защиты инфор-

мации) осуществляется в соответствии с положениями Приказа ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Для осуществления мероприятий по разработке и внедрению СЗПДн на договорной основе может привлекаться организация, имеющая лицензию на осуществление деятельности по технической защите конфиденциальной информации.

Результаты разработки СЗПДн отражаются в Описании системы защиты персональных данных.

Результаты внедрения СЗПДн отражаются в Техническом паспорте ИСПДн.

10.3. Оценка эффективности применяемых мер по обеспечению безопасности персональных данных

Оценка эффективности реализованных в рамках СЗПДн мер по обеспечению! безопасности ПДн проводится Организацией самостоятельно или с привлечением на договорной основе организации, имеющей лицензию на осуществление деятельности по технической защите конфиденциальной информации.

Оценка эффективности может проводится в форме декларирования соответствия или в рамках работ по аттестации информационной системы персональных данных в соответствии с национальным стандартом ГОСТ РО 0043-1 003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения».

11. Права субъектов персональных данных

Права субъектов персональных данных (либо их законных представителей) определены в Политике Организации в отношении обработки персональных данных и положениях законодательства Российской Федерации в области; обработки персональных данных.

12. Роли в области организации обработки и обеспечениябезопасности персональных данных

12.1. Перечень ролей

В целях обеспечения законного порядка обработки и обеспечения безопасности ПДн в Организации выделяются следующие роли:

Ответственный за организацию обработки персональных данных - работник Организации, осуществляющий организацию выполнения требований законодательства Российской Федерации при обработке и обеспечении безопасности ПДн в Организации;

Администратор ИСПДн - работник Организации, обеспечивающие бесперебойное функционирование информационной системы персональных данных;

Пользователь - работник Организации, непосредственно осуществляющий обработку ПДн

12.2. Права и обязанности Ответственного за организацию обработки персональных данных

Ответственный за организацию обработки ПДн обязан:

- осуществлять внутренний контроль над соблюдением Организацией и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных (пункт 1 часть 4 ст. 22.1 152- ФЗ);
- доводить до сведения работников Организации положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных (пункт 2 часть 4 ст. 22.1 152-ФЗ);
- организовывать (обеспечивать) прием и обработку обращений и запросов субъектов персональных данных (пункт 3 часть 4 ст. 22.1 152-ФЗ);
- организовывать построение и эксплуатацию СЗПДн Организации и, при необходимости ее модернизацию;
- обеспечивать поддержание в актуальном состоянии организационно-

распорядительных документов Организации по организации обработки и обеспечению безопасности ПДн;

- проводить систематический контроль над выполнением комплекса организационно-технических мероприятий по организации обработки и обеспечению безопасности персональных данных, в том числе за выполнением Администратором ИСПДн своих обязанностей;
- хранить дистрибутивы программного обеспечения средств защиты информации ИСПДн, а также эксплуатационную документацию и сертификаты средств защиты информации;
- организовывать проведение инструктажей и обучения работников Организации по вопросам обработки и обеспечения безопасности персональныхданных;
- осуществлять взаимодействие с регулирующими органами по вопросам обработки и обеспечения безопасности ПДн, в том числе координировать действия работников Организации при проведении проверок регулирующими органами, а также при обработке запросов указанных органов;
- предоставлять консультации и оказывать содействие работникам Организации по вопросам обработки и обеспечения безопасности персональных данных в рамках своей компетенции;
- незамедлительно принимать меры пресечения и уведомлять руководителя Организации в случае обнаружения попыток или фактов несанкционированного доступа к ПДн, а также нарушения требований организационно-распорядительных документов Организации по организации обработки и обеспечению безопасностиПДн.

Ответственный за организацию обработки ПДн имеет право:

- давать указания Администратору ИСПДн и контролировать ихвыполнение;
- вносить предложения по совершенствованию процессов обработки и обеспечения безопасности персональных данных в Организации;
- требовать от работников устранения выявленных нарушений и предоставления письменных объяснений по фактам нарушений требований организационно-распорядительных документов Организации по организации обработки и обеспечению безопасности ПДн;
- запрашивать у работников, участвующих в процессах обработки и| обеспечения безопасности ПДн, информацию и документы, необходимые для выполнения функциональных обязанностей.

12.3. Права и обязанности Администратора ИСПДн

Администратор ИСПДн обязан:

- обеспечивать настройку и бесперебойную эксплуатацию программных и технических средств обработки ПДн, входящих в состав ИСПДн Организации;
- обеспечивать настройку, бесперебойную эксплуатацию и мониторинг! средств защиты информации, входящих в состав СЗПДн Организации;
- настраивать права доступа работников к персональным данным и средствам их обработки в Организации в соответствии с ролевой моделью доступа;
- проводить инструктаж пользователей ИСПДн по правилам эксплуатации программных и технических средств обработки ПДн, входящих в состав ИСПДн Организации и средств защиты информации, входящими в состав СЗПДн Организации;
- контролировать смену паролей пользователями ИСПДн не реже одного! раза в три месяца либо при компрометации паролей;
- организовать учет, хранение и уничтожение машинных носителей! персональных данных;
- хранить дистрибутивы программного обеспечения средств обработки! информации ИСПДн;
- обеспечивать контроль сторонних организаций (подрядчиков), при привлечении последних для обслуживания, настройки и ремонта средств обработки и защиты

информации ИСПДн;

- предоставлять необходимую информацию при проведении проверок регулирующими органами, а также проведении контрольных мероприятий по обеспечению безопасности ПДн;
- предоставлять консультации и оказывать содействие работникам, участвующим в процессах обработки и обеспечения безопасности ПДн, по! вопросам использования средств обработки информации ИСПДн, в рамках своей компетенции;
- в случае обнаружения попыток или фактов несанкционированного доступа к ПДн, незамедлительно уведомлять о выявленных фактах Ответственного за организацию обработки ПДн.

Администратор ИСПДн имеет право:

- вносить предложения по совершенствованию ИСПДн и СЗПДн Организации, в том числе организационно-распорядительных документов в области обработки и обеспечения безопасности ПДн;
- запрашивать у работников, участвующих в процессах обработки и обеспечения безопасности ПДн, информацию и документы, необходимые для| выполнения функциональных обязанностей.

12.4. Права и обязанности Пользователя

Пользователь обязан:

- строго соблюдать положения законодательства РФ о персональных данных, локальных актов Организации по вопросам обработки персональных данных, требований к защите персональных данных.

Пользователь имеет право:

- запрашивать у лица ответственного за организацию обработки персональных данных разъяснения положений законодательства РФ о персональных данных, локальных актов Организации по вопросам обработки персональных данных, требований к защите персональных данных;
- вносить предложения по совершенствованию процессов обработки и обеспечения безопасности персональных данных в Организации.
- запрашивать у работников, участвующих в процессах обработки и обеспечения безопасности ПДн, информацию и документы, необходимые для выполнения функциональных обязанностей.

13. Ответственность

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

Лица, виновные в нарушении норм, регулирующих обработку ПДн, несут дисциплинарную, административную, гражданскую, уголовную и иную предусмотренную законодательством Российской Федерации ответственность.

Прекращение доступа к персональным данным и/или увольнение не освобождает работника Организации от принятых обязательств по неразглашению персональных данных, ставших доступными при выполнении должностных обязанностей.

К административной ответственности за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах и за нарушение правил защиты информации могут привлекаться как сама Организация и её должностные лица, так и конкретные работники, исполняющие соответствующие трудовые функции.

13.2. Описание видов ответственности

Виды дисциплинарных взысканий, порядок их применения и снятия установлены главой 30 ТК РФ и Правилами внутреннего трудового распорядкаОрганизации.

Порядок защиты нематериальных благ, к числу которых относятся честь и доброе имя, деловая репутация; неприкосновенность частной жизни; личная и семейная тайна определяется Гражданским кодексом РФ и иными законами.

Лица, виновные в нарушении правил работы с ПДн, могут привлекаться к административной ответственности в частности по следующим основаниям:

- неправомерный отказ в предоставлении гражданину собранных в установленном порядке документов, материалов, непосредственно затрагивающих его права и свободы, либо несвоевременное предоставление таких документов и материалов, не предоставление иной информации в случаях, предусмотренных законом, либо предоставление гражданину неполной или заведомо недостоверной информации (ст. 5.39 КоАП);
- нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) (ст. 13.11 КоАП);
- нарушение правил защиты информации (ст. 13.12 КоАП);
- разглашение информации, доступ к которой ограничен федеральным £“ законом (за исключением случаев, когда ее разглашение влечет уголовную Т ответственность), лицом, получившим к ней доступ в связи с исполнением служебных или профессиональных обязанностей (ст. 13.14 КоАП РФ).

Уголовная ответственность за нарушение правил работы с ПДн может, наступить в частности в следующих случаях:

- незаконное собирание или распространение сведений о частной жизни В лица, составляющих его личную или семейную тайну, без его согласия либо в распространении этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, если эти В деяния совершены из корыстной или иной личной заинтересованности и В причинили вред правам и законным интересам граждан (ст. 137 УК РФ);
- неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственной затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан (ст. 140 УК РФ);
- неправомерный доступ к охраняемой законом компьютернойинформации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации (ст. 272 УК РФ);
- нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации причинившее крупный ущерб или повлекшее тяжкие последствия (ст.274 УК РФ).