

**МИНИСТЕРСТВО СОЦИАЛЬНОГО РАЗВИТИЯ ПЕРМСКОГО КРАЯ**

**ПРИКАЗ**  
от 3 апреля 2014 г. N СЭД-33-01-03-123

**ОБ УТВЕРЖДЕНИИ ПОЛИТИКИ МИНИСТЕРСТВА СОЦИАЛЬНОГО РАЗВИТИЯ  
ПЕРМСКОГО КРАЯ В ОТНОШЕНИИ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ  
ДАННЫХ**

Список изменяющих документов  
(в ред. [Приказа](#) Министерства социального развития Пермского края  
от 18.01.2019 N СЭД-33-01-03-12)

В целях исполнения Федерального [закона](#) от 27 июля 2006 г. N 152-ФЗ "О персональных данных", [Постановления](#) Правительства Российской Федерации от 21 марта 2012 г. N 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" приказываю:

1. Утвердить прилагаемую [Политику](#) Министерства социального развития Пермского края в отношении обработки и защиты персональных данных.

2. Начальнику отдела по управлению персоналом Министерства социального развития Пермского края (далее - Министерство) Крюковских Т.П.:

2.1. ознакомить с настоящим Приказом заместителя министра Фокина П.С., начальника отдела информационных технологий и сопровождения регистра Министерства Косожихину Е.И., руководителей структурных подразделений Министерства;

2.2. обеспечить опубликование настоящего Приказа на сайте Министерства - <http://minsoc.permkrai.ru>.

3. Настоящий Приказ вступает в силу со дня его подписания.

4. Контроль за исполнением настоящего Приказа возложить на заместителя министра Фокина П.С.

Министр  
Т.Ю.АБДУЛЛИНА

УТВЕРЖДЕНА  
Приказом  
Министерства социального  
развития Пермского края  
от 03.04.2014 N СЭД-33-01-03-123

**ПОЛИТИКА  
МИНИСТЕРСТВА СОЦИАЛЬНОГО РАЗВИТИЯ ПЕРМСКОГО КРАЯ В ОТНОШЕНИИ  
ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Список изменяющих документов  
(в ред. Приказа Министерства социального развития Пермского края  
от 18.01.2019 N СЭД-33-01-03-12)

**1. Общие положения**

1.1. Настоящая политика (далее - Политика) разработана в соответствии со [ст. 18.1](#) Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (далее - Закон о ПДн) и является основополагающим внутренним регулятивным документом Министерства социального развития Пермского края (далее - Министерство), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее - ПДн), оператором которых является Министерство.

1.2. Политика направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн в Министерстве, в том числе защиты прав на неприкосновенность частной жизни, личной и семейной тайн.

1.3. Положения Политики распространяются на отношения по обработке и защите ПДн, полученных Министерством как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПДн, полученных до ее утверждения.

1.4. Если в отношениях с Министерством участвуют наследники (правопреемники) и (или) представители субъектов ПДн, то Министерство становится оператором ПДн лиц, представляющих указанных субъектов. Положения Политики и другие внутренние регулятивные документы Министерства распространяются на случаи обработки и защиты ПДн наследников (правопреемников) и (или) представителей субъектов ПДн, даже если эти лица во внутренних регулятивных документах прямо не упоминаются, но фактически участвуют в правоотношениях с Министерством.

**2. Основания обработки и состав персональных данных,  
обрабатываемых в Министерстве**

2.1. Обработка ПДн в Министерстве осуществляется в связи с выполнением законодательно возложенных на Министерство полномочий и функций, определяемых [Положением](#) о Министерстве социального развития Пермского края, утвержденным Постановлением Правительства Пермского края от 24 июля 2006 г. N 7-п.

Кроме того, в Министерстве осуществляется обработка ПДн, связанных с поступлением на государственную гражданскую службу Пермского края и ее прохождением, реализацией трудовых отношений, формированием кадрового резерва на государственную гражданскую службу Пермского края в Министерстве.

2.2. ПДн получают и обрабатываются Министерством на основании федеральных законов и принятых в соответствии с ними нормативными правовыми актами, а в необходимых случаях - при наличии письменного согласия субъекта ПДн.

2.3. В рамках осуществления функции регионального оператора государственного банка данных о детях, оставшихся без попечения родителей, ПДн обрабатываются Министерством:

1) при осуществлении учета детей, оставшихся без попечения родителей, учете детей, оставшихся без попечения родителей;

2) при организации их устройства на воспитание в семьи граждан Российской Федерации, постоянно проживающих на территории Российской Федерации.

При этом обрабатываются ПДн:

а) детей, оставшихся без попечения родителей;

б) граждан, желающих принять ребенка в семью.

2.4. В рамках осуществления функции организации предоставления государственной социальной и иной социальной помощи, мер социальной поддержки населению в соответствии с законодательством Российской Федерации и Пермской области, Пермского края, а также формирования, использования и организации ведения регионального регистра лиц, имеющих право на получение мер государственной социальной помощи и поддержки, ПДн обрабатываются Министерством:

1) при предоставлении мер социальной помощи и поддержки;

2) при учете фактов предоставления мер социальной помощи и поддержки.

При этом обрабатываются ПДн:

а) лиц, имеющих право на получение мер социальной помощи и поддержки.

2.4 (1). В рамках осуществления функции в области содействия занятости населения ПДн обрабатываются Министерством:

1) при реализации в Пермском крае единой государственной политики в области содействия занятости населения.

При этом обрабатываются ПДн:

а) получателей государственных услуг в сфере занятости населения (физических лиц и работодателей).

(п. 2.4 (1) введен [Приказом](#) Министерства социального развития Пермского края от 18.01.2019 N СЭД-33-01-03-12)

2.5. В связи с трудовыми и иными непосредственно связанными с ними отношениями, в которых Министерство выступает в качестве работодателя, для обеспечения кадровой работы ПДн обрабатываются Министерством в целях:

- содействия государственным гражданским служащим Пермского края в прохождении государственной гражданской службы Пермского края,

- учета соблюдения государственными гражданскими служащими Пермского края, лицами, замещающими государственные должности Пермского края, установленных ограничений и запретов,

- реализации трудовых отношений;

- противодействия коррупции;

- формирования кадрового резерва на государственную гражданскую службу Пермского края.

При этом обрабатываются ПДн:

а) государственных гражданских служащих Пермского края,

б) лиц, замещающих государственные должности Пермского края,

в) граждан, претендующих на замещение должностей государственной гражданской службы Пермского края, государственных должностей Пермского края,

г) лиц, претендующих на замещение должностей, не являющихся должностями государственной гражданской службы Пермского края, в Министерстве либо замещающих указанные должности (далее - работники);

д) бывших работников Министерства или лиц, замещавших должности государственной гражданской службы Пермского края в Министерстве;

е) граждан, претендующих на включение (включенных) в кадровый резерв на государственную гражданскую службу Пермского края (далее - резерв) в Министерстве.

2.6. Министерством обрабатываются следующие специальные категории ПДн.

2.6.1. Для детей, оставшихся без попечения родителей:

- сведения о состоянии здоровья (физическое развитие, нервно-психическое развитие, группа здоровья, коды болезней по МКБ-10, дата проведения последнего медицинского обследования, инвалидность, дата установки и срок действия инвалидности);

- этническое происхождение.

КонсультантПлюс: примечание.

В официальном тексте документа, видимо, допущена опечатка: имеется в виду пункт 9 части 1 статьи 6 Федерального закона от 27.07.2006 N 152-ФЗ, а не пункт 9 части 2 статьи 6.

Обработка указанных специальных категорий данных осуществляется Министерством в соответствии с п. 9 ч. 2 ст. 6 Закона о ПДн. Перечень обрабатываемых при этом категорий ПДн соответствует требованиям ст. 6 Федерального закона "О государственном банке данных о детях, оставшихся без попечения родителей".

2.6.2. Для лиц, имеющих право на получение мер социальной помощи и поддержки, а также получателей государственных услуг в сфере занятости населения:

- сведения о состоянии здоровья (причина инвалидности, группа инвалидности, диагноз заболевания, ограничения передвижения), обработка осуществляется Министерством в соответствии с п. 2.3 ч. 2 ст. 10 Закона о ПДн;

- сведения о судимости (в части несовершеннолетних, находящихся в социально опасном положении или иной трудной жизненной ситуации, имеющих право на предоставление мер поддержки; граждан, испытывающих трудности в поиске работы), обработка осуществляется Министерством в соответствии с ч. 3 ст. 10 Закона о ПДн.

(п. 2.6.2 в ред. Приказа Министерства социального развития Пермского края от 18.01.2019 N СЭД-33-01-03-12)

2.6.3. Для граждан, претендующих на замещение должностей государственной гражданской службы Пермского края, государственных должностей Пермского края в Министерстве:

- сведения о состоянии здоровья (медицинское заключение по установленной форме об отсутствии у гражданина заболевания, препятствующего поступлению на государственную гражданскую службу или ее прохождению);

- информация о наличии или отсутствии судимости.

Обработка указанных специальных категорий ПДн осуществляется без согласия указанных лиц в рамках целей, определенных пунктом 2.1 Положения в сфере обработки и защиты персональных данных в связи с прохождением государственной гражданской службы в Министерстве социального развития Пермского края (далее - положение о ПДн), утвержденного Приказом Министерства от 15 августа 2013 г. N СЭД-33-01-03-390, в соответствии с [подпунктом 2.3 п. 2 ч. 2 ст. 10, ч. 3 Закона о ПДн](#) и положениями Трудового [кодекса](#) Российской Федерации.

Запрещается получать, обрабатывать и приобщать к личному делу государственного гражданского служащего Пермского края, работника персональные данные, не предусмотренные пунктами 2.2, 2.3 указанного Положения о ПДн, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

2.7. Министерством обрабатываются биометрические ПДн для следующих категорий субъектов ПДн:

2.7.1. Для детей, оставшихся без попечения родителей:

- вес, рост, фотография.

Перечень обрабатываемых при этом категорий ПДн соответствует требованиям [ст. 6](#) Федерального закона от 16 апреля 2001 г. N 44-ФЗ "О государственном банке данных о детях, оставшихся без попечения родителей".

2.7.2. Для лиц, перечисленных в [п. 2.5](#) настоящей Политики:

- фотография.

Перечень обрабатываемых при этом категорий ПДн соответствует требованиям [п. 16](#) Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела, утвержденного Указом Президента Российской Федерации от 30 мая 2005 г. N 609.

2.8. Обработка иных специальных категорий персональных данных, а также биометрических персональных данных Министерством не ведется.

2.9. В целях исполнения возложенных на Министерство функций Министерство в установленном порядке вправе поручить обработку ПДн третьим лицам.

В договоры с лицами, которым Министерство поручает обработку ПДн, включаются условия, обязывающие таких лиц соблюдать предусмотренные [Законом](#) о ПДн и Политикой правила обработки ПДн.

2.10. Министерство предоставляет обрабатываемые им ПДн государственным органам и организациям, имеющим в соответствии с федеральным законом право на получение соответствующих ПДн.

2.11. В Министерстве не производится обработка ПДн, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПДн в Министерстве, в том числе при достижении целей их обработки или утраты необходимости в

достижении этих целей, обрабатывавшиеся Министерством ПДн уничтожаются или обезличиваются.

2.12. При обработке ПДн обеспечиваются их точность, достаточность, а при необходимости - и актуальность по отношению к целям обработки. Министерство принимает необходимые меры по удалению или уточнению неполных или неточных ПДн.

### **3. Принципы обеспечения безопасности персональных данных**

3.1. Основной задачей обеспечения безопасности ПДн при их обработке в Министерстве является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПДн, разрушения (уничтожения) или искажения их в процессе обработки.

3.2. Для обеспечения безопасности ПДн Министерство руководствуется следующими принципами:

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

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

3) комплексность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Министерства (далее - ИС), и других имеющихся в Министерстве систем и средств защиты;

4) 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;

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

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

7) персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на должностных лиц (государственных служащих и работников) Министерства в пределах их обязанностей, связанных с обработкой и защитой ПДн;

8) минимизация прав доступа: доступ к ПДн предоставляется должностным лицам только в объеме, необходимом для выполнения их должностных обязанностей;

9) гибкость: обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования информационных систем персональных данных Министерства (далее - ИСПДн), а также объема и состава обрабатываемых ПДн;

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

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

12) специализация и профессионализм: реализация мер по обеспечению безопасности ПДн и эксплуатация СЗПДн осуществляются должностными лицами, имеющими необходимые для этого квалификацию и опыт;

13) эффективность процедур отбора кадров и выбора контрагентов: кадровая политика Министерства предусматривает тщательный подбор персонала и мотивацию должностных лиц, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн; минимизация вероятности возникновения угрозы безопасности ПДн, источники которых связаны с человеческим фактором, обеспечивается получением наиболее полной информации о контрагентах Министерства до заключения договоров;

14) 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;

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

#### **4. Доступ к обрабатываемым персональным данным**

4.1. Доступ к обрабатываемым в Министерстве ПДн имеют лица, уполномоченные приказом Министерства, а также лица, чьи ПДн подлежат обработке.

4.2. В целях разграничения полномочий при обработке ПДн полномочия по реализации каждой определенной законодательством функции Министерства закрепляются за соответствующими структурными подразделениями Министерства.

4.3. Доступ должностных лиц к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов Министерства. Допуск должностных лиц к обработке ПДн осуществляется согласно перечню типовых полномочий (ролей пользователей), утверждаемых приказом Министерства. Соответствующие полномочия (роль пользователя) вносятся в должностные обязанности указанных должностных лиц.

Допущенные к обработке ПДн должностные лица под роспись знакомятся с документами Министерства, устанавливающими порядок обработки ПДн, включая документы, устанавливающие права и обязанности конкретных должностных лиц.

4.4. Факты получения доступа к ИСПДн, а также факты обработки ПДн регистрируются, в том числе с использованием средств обеспечения информационной безопасности. Информация о фактах обработки ПДн хранится в Министерстве, включая ИС, в течение трех лет.

Порядок доступа субъекта ПДн к его ПДн, обрабатываемым Министерством, осуществляется в соответствии с [Законом](#) о ПДн и определяется внутренними регулятивными документами Министерства.

#### **5. Реализация Политики**

5.1. Министерство принимает необходимые и достаточные меры для защиты обрабатываемых ПДн от неправомерного или случайного доступа к ним, от уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных

действий с ними со стороны третьих лиц.

5.2. Ответственность за организацию обработки ПДн в Министерстве несет должностное лицо Министерства, назначаемое приказом Министерства.

Ответственный за организацию обработки ПДн в Министерстве, в частности, обязан:

1) осуществлять внутренний контроль за соблюдением в Министерстве требований нормативных правовых актов и внутренних регулятивных документов Министерства в области обработки и защиты ПДн;

2) доводить до сведения должностных лиц Министерства положения нормативных правовых актов и внутренних регулятивных документов Министерства в области обработки и защиты ПДн;

3) организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

5.3. Министерство осуществляет обработку ПДн без использования средств автоматизации, а также с использованием таких средств.

5.4. При обработке ПДн без использования средств автоматизации Министерство в соответствии с положениями нормативных правовых актов в области обработки и защиты ПДн реализует комплекс организационных и технических мер, обеспечивающих:

1) обособление ПДн от информации, не содержащей ПДн;

2) отдельную обработку и хранение каждой категории ПДн (фиксация на отдельных материальных носителях ПДн, цели обработки которых заведомо несовместимы);

3) соответствие типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн, установленным требованиям;

4) соблюдение установленных требований при ведении журналов (реестров, книг), содержащих ПДн, необходимые для однократного пропуска субъекта ПДн в помещения, занимаемые Министерством, или в иных аналогичных целях;

5) сохранность материальных носителей ПДн;

6) условия хранения, исключающие несанкционированный доступ к ПДн, а также смешение ПДн (материальных носителей), обработка которых осуществляется в различных целях;

7) надлежащее уточнение, уничтожение или обезличивание ПДн.

5.5. В соответствии с требованиями нормативных правовых актов в области обработки и защиты ПДн, обработки ПДн с использованием средств автоматизации в Министерстве создаются ИСПДн.

Все ИСПДн проходят периодическую классификацию и аттестацию в соответствии с требованиями нормативных правовых актов в области обеспечения безопасности ПДн.

Для каждой ИСПДн формируется модель угроз безопасности ПДн, и на ее основе проводятся мероприятия по обеспечению безопасности информации в соответствии с требованиями, предъявляемыми к установленному классу ИСПДн.

Пересмотр моделей угроз для каждой ИСПДн осуществляется:



а) в плановом порядке для существующих ИСПДн - ежегодно;

б) в случае существенных изменений в инфраструктуре или порядке обработки ПДн в ИСПДн - в течение трех месяцев с даты фиксации изменений;

в) в случае создания новой ИСПДн (выделения части из существующей ИСПДн) - в течение одного месяца с даты создания (выделения) ИСПДн.

5.6. Обработка ПДн в Министерстве с использованием средств автоматизации ведется только в ИСПДн. В Министерстве запрещается обработка ПДн с целями, не соответствующими целям создания ИСПДн, эксплуатация ИСПДн в составе, отличном от указанного при создании ИСПДн.

5.7. Ввод в эксплуатацию ИСПДн оформляется актом ввода в эксплуатацию и сопровождается аттестацией ИСПДн или декларированием соответствия ИСПДн требованиям по безопасности ПДн.

5.8. В целях обеспечения управления информационной безопасностью ПДн в Министерстве создается СЗПДн.

Объектами защиты СЗПДн являются информация, обрабатываемая Министерством и содержащая ПДн, а также инфраструктура, содержащая и поддерживающая указанную информацию.

5.9. СЗПДн реализуется комплексом правовых, режимных, организационных и программно-технических мер, которые включают:

1) подготовку внутренних регулятивных документов Министерства по вопросам обработки и защиты ПДн, контроль за исполнением в Министерстве требований нормативных правовых актов и внутренних регулятивных документов Министерства в области обработки и защиты ПДн, а также внесение соответствующих изменений в имеющиеся внутренние регулятивные документы;

2) оформление письменных обязательств должностных лиц о неразглашении ПДн;

3) доведение до сведения должностных лиц информации об установленных законодательством Российской Федерации санкциях за нарушения, связанные с обработкой и защитой ПДн;

4) обеспечение наличия в положениях о структурных подразделениях Министерства и должностных обязанностях требований по соблюдению установленного порядка обработки и защиты ПДн;

5) разработку и введение в действие внутренних регулятивных документов Министерства по обеспечению информационной безопасности ИСПДн;

6) регламентацию процедур создания и осуществление документирования действующих инженерных и информационных систем, программных комплексов, порядка внесения в них изменений и своевременной актуализации эксплуатационной документации;

7) ознакомление должностных лиц с положениями нормативных правовых актов и внутренних регулятивных документов Министерства в области обработки и защиты ПДн и (или) организация обучения их правилам обработки и защиты ПДн;

8) проведение мероприятий по регламентации, установлению, поддержанию и осуществлению контроля за состоянием:

а) физической охраны, контрольно-пропускного режима, перемещением технических

средств и носителей информации;

б) защиты технологических процессов, информационных ресурсов, информации и поддерживающей их инфраструктуры от угроз техногенного характера и внешних неинформационных воздействий;

9) регламентацию обработки ПДн, в том числе хранения и передачи информации как внутри Министерства, так и при взаимодействии с контрагентами Министерства, государственными органами и организациями, обращения с документами (включая электронные документы) и носителями, порядка их учета, хранения и уничтожения;

10) установление правил доступа на объекты, в помещения, в ИС, применение в этих целях систем охраны и управления доступом;

11) формирование участков (выделение в отдельные VLAN (виртуальные локальные компьютерные сети) технических средств) администрирования безопасности, мониторинга и аудита, управления доступом к защищаемым ресурсам;

12) организацию технического оснащения объектов и ИСПДн в соответствии с существующими требованиями к информационной безопасности;

13) формирование условий и технологических процессов обработки, хранения и передачи информации в Министерстве (включая условия хранения документов в архивах), обеспечивающих реализацию требований нормативных правовых актов, методических документов уполномоченных государственных органов и внутренних регулятивных документов Министерства в области обработки и защиты ПДн;

14) установление полномочий пользователей и форм представления информации пользователям ИСПДн;

15) организацию непрерывного процесса контроля (мониторинга) событий безопасности для своевременного выявления и пресечения попыток несанкционированного доступа к защищаемой информации;

16) организацию необходимых мероприятий с должностными лицами, а также собеседование с лицами, претендующими на работу в Министерстве, изучение их биографии и проверку предоставляемых сведений; обучение должностных лиц требованиям информационной безопасности;

17) осуществление контроля эффективности организационных мер защиты;

18) разработку защитных технических решений:

а) при стратегическом планировании архитектуры ИС;

б) выборе технических средств обработки информации;

в) разработке и (или) приобретении программного обеспечения;

19) применение следующих компонентов программно-технических мер защиты:

а) защищенных средств (систем) обработки информации, содержащей ПДн;

б) системы криптографической защиты информации при ее передаче по каналам связи;

в) межсетевых экранов для логического разделения подсетей и защиты от несанкционированного доступа из внешних (открытых) информационных систем;

г) аппаратных и программных средств защиты и контроля, устройств, технических систем и средств, используемых для обеспечения информационной безопасности, в том числе для обнаружения и нейтрализации попыток несанкционированного доступа к информации.

5.10. Для всех критичных в отношении обеспечения целостности и доступности ПДн функций ИСПДн разрабатываются соответствующие планы обеспечения непрерывной работы и восстановления при авариях и стихийных бедствиях, которые не реже одного раза в квартал проходят актуализацию. Должностные лица проходят обучение необходимым действиям по обеспечению целостности и доступности ПДн в нестандартных ситуациях.

## **6. Основные мероприятия по обеспечению безопасности персональных данных**

6.1. Мероприятия по защите ПДн реализуются в Министерстве в следующих направлениях:

1) предотвращение утечки информации, содержащей ПДн, по техническим каналам связи и иными способами;

2) предотвращение несанкционированного доступа к содержащей ПДн информации, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней;

3) защита от вредоносных программ;

4) обеспечение безопасного межсетевого взаимодействия;

5) обеспечение безопасного доступа к сетям международного информационного обмена;

6) анализ защищенности ИСПДн;

7) обеспечение защиты информации с использованием шифровальных (криптографических) средств при передаче ПДн по каналам связи;

8) обнаружение вторжений и компьютерных атак;

9) осуществление контроля за реализацией системы защиты ПДн.

6.2. Мероприятия по обеспечению безопасности ПДн включают в себя:

1) реализацию разрешительной системы допуска пользователей к информационным ресурсам ИС и связанным с их использованием работам, документам;

2) разграничение доступа пользователей ИСПДн и обслуживающих ИСПДн специалистов к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

3) регистрацию действий пользователей и обслуживающих ИСПДн специалистов, контроль несанкционированного доступа и действий пользователей и обслуживающих специалистов, а также третьих лиц;

4) использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

5) предотвращение внедрения в ИС вредоносных программ и программных закладок, анализ принимаемой по информационно-телекоммуникационным сетям (сетям связи общего пользования) информации, в том числе на наличие компьютерных вирусов;

6) ограничение доступа в помещения, где размещены технические средства, позволяющие осуществлять обработку ПДн, а также хранятся носители информации, содержащие ПДн;

7) размещение технических средств, позволяющих осуществлять обработку ПДн, в пределах охраняемой территории;

8) организацию физической защиты помещений и технических средств, позволяющих осуществлять обработку ПДн;

9) учет и хранение съемных носителей информации и их обращение, исключаящее хищение, подмену и уничтожение;

10) резервирование технических средств, дублирование массивов и носителей информации;

11) реализацию требований по безопасному межсетевому взаимодействию ИС;

12) использование защищенных каналов связи, защиту информации при ее передаче по каналам связи;

13) межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры ИС;

14) обнаружение вторжений в ИС, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности ПДн;

15) периодический анализ безопасности установленных межсетевых экранов на основе имитации внешних атак на ИС;

16) активный аудит безопасности ИС на предмет обнаружения в режиме реального времени несанкционированной сетевой активности;

17) анализ защищенности ИС с применением специализированных программных средств (сканеров безопасности);

18) централизованное управление системой защиты ПДн в ИС.

6.3. В целях организации работ по обеспечению информационной безопасности ПДн в Министерстве определяется должностное лицо (структурные подразделения), на которое возлагаются задачи:

1) по классификации, паспортизации и аттестации ИСПДн;

2) организации разработки модели угроз для каждой ИСПДн;

3) организации разработки технического проекта системы защиты информации для каждой ИСПДн;

4) закупке, установке, эксплуатации и администрированию средств защиты информации;

5) организации разрешительной системы допуска к информации, содержащей ПДн, и разработке внутренних регулятивных документов Министерства по этому вопросу;

6) организации реагирования на события безопасности;

7) контролю состояния системы защиты информации и планирования соответствующих мероприятий.

6.4. С целью поддержания состояния защиты ПДн на надлежащем уровне в Министерстве

осуществляется внутренний контроль за эффективностью системы защиты ПДн и соответствием порядка и условий обработки и защиты ПДн установленным требованиям.

Внутренний контроль включает:

1) мониторинг состояния технических и программных средств, входящих в состав СЗПДн;

2) контроль соблюдения требований по обеспечению безопасности ПДн (требований нормативных правовых актов и внутренних регулятивных документов в области обработки и защиты ПДн, требований договоров).

6.5. В целях осуществления внутреннего контроля в Министерстве проводятся периодические проверки условий обработки ПДн. Такие проверки осуществляются ответственным за организацию обработки ПДн в Министерстве либо комиссией, образуемой по приказу Министерства.

6.6. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, докладывается министру.

---