Д Е П А Р Т А М Е Н Т О Б Р А З О В А Н И Я
М Э Р И И Г О Р О Д А Я Р О С Л А В Л Я

П Р И К А З

(в редакции приказа департамента образования мэрии города Ярославля от 29.11.2019 № 01-05/1071)

07.12.2012 № 01-05/989

Об утверждении Положения о порядке организации и проведения работ по созданию и эксплуатации информационных систем персональных данных и системы защиты персональных данных в департаменте образования мэрии города Ярославля

В целях обеспечения защиты персональных данных при их обработке в информационных системах департамента образования мэрии города Ярославля, руководствуясь Федеральным законом от 27.07.2006 N 152-ФЗ «О персональных данных»,

ПРИКАЗЫВАЮ:

1. Утвердить Положение об о порядке организации и проведения работ по созданию и эксплуатации информационных систем персональных данных и системы защиты персональных данных в департаменте образования мэрии города Ярославля (Приложение).

2. Контроль исполнения приказа оставляю за собой.

Директор департамента образования С.В.Терех

Приложение
к приказу департамента образования мэрии города
Ярославля от 07.12.2012 № 01-05/989

ПОЛОЖЕНИЕ

о порядке организации и проведения работ
по созданию и эксплуатации информационных систем персональных данных и системы защиты персональных данных в департаменте образования мэрии города Ярославля

1 Основные положения

1.1 Настоящее Положение определяет последовательность действий при организации работ по созданию и эксплуатации информационных систем персональных данных (далее – ИСПДн) и системы защиты персональных данных (далее – СЗПДн) в департаменте образования мэрии города Ярославля (далее – Департамент), порядок взаимодействия работников Департамента, а также сторонних организаций при проведении указанных работ, их основные функции по обеспечению безопасности персональных данных (далее – ПДн), обрабатываемых в Департаменте.

1.2 Настоящее Положение разработано в соответствии с требованиями законодательства Российской Федерации по обеспечению безопасности персональных данных.

1.3 Действие настоящего Положения распространяется на все процессы по сбору, записи, систематизации, накоплению, хранению, уточнению (обновлению, изменению), извлечению, использованию, передаче (распространению, предоставлению, доступу), блокированию, удалению, уничтожению ПДн, осуществляемые в ИСПДн Департамента.

1.4 Настоящее Положение вступает в силу с даты его утверждения и действует до его отмены либо замены новым Положением.

2 Основные понятия

2.1 Основные понятия, используемые в Положении:

Администратор информационной безопасности – лицо, ответственное за защиту информационной системы персональных данных от несанкционированного доступа к информации.

Безопасность информации (данных) – состояние защищенности информации (данных), при котором обеспечиваются её (их) конфиденциальность, доступность и целостность.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Доступ к информации – возможность получения информации и ее использования.

Доступность информации (ресурсов информационной системы персональных данных) – состояние информации (ресурсов информационной системы персональных данных), при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

Защищаемые информационные (программные) ресурсы - файлы и базы данных, содержащие ПДн; программные средства, используемые для обработки ПДн; программные средства защиты ПДн;

Защита информации от несанкционированного доступа – защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами

(актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

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

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

Инцидент информационной безопасности – нарушение заданных характеристик безопасности ПДн, обрабатываемых в ИСПДн.

Контролируемая зона - помещения с установленными техническими средствами, участвующими в обработке ПДн, а также помещения, где хранятся материальные носители ПДн, дистрибутивы и документация к средствам защиты информации, в которых исключено неконтролируемое пребывание граждан.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к такой информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Несанкционированный доступ (к информации / ресурсам информационной системы персональных данных) – доступ к информации (ресурсам информационной системы персональных данных), осуществляемый с нарушением установленных прав и (или) правил доступа к информации (ресурсам информационной информационной системы персональных данных).

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных.

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Угроза (безопасности информации) – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения конфиденциальности, доступности и (или) целостности информации.

Целостность информации — состояние защищённости информации, характеризуемое способностью обеспечивать сохранность и неизменность информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки и хранения.

3 Организационная структура Департамента в области обеспечения безопасности персональных данных

3.1 Директор Департамента в рамках обеспечения безопасности ПДн выполняет следующие функции:

– осуществляет общую координацию действий в области защиты ПДн;

– обеспечивает реализацию планов в области защиты ПДн;

– организует обучение работников по вопросам обеспечения безопасности ПДн;

– принимает решения о необходимости привлечения сторонних организаций на этапах инвентаризации информационных ресурсов, предпроектного обследования, проектирования ИСПДн и СЗПДн, внедрения ИСПДн и СЗПДн в эксплуатацию и поддержания работоспособности ИСПДн и СЗПДн при их эксплуатации.

3.2 Лицо, ответственное за организацию обработки ПДн, назначается приказом Департамента и в рамках обеспечения безопасности ПДн выполняет следующие функции:

– обеспечивает контроль соблюдения в Департаменте требований законодательства РФ о ПДн;

– организует (в том числе, осуществляет) разработку и представление на утверждение проектов организационно-распорядительных документов по вопросам обработки и защиты ПДн, поддерживает данные документы в актуальном состоянии;

– обеспечивает опубликование документов, определяющих политику Департамента в отношении обработки ПДн;

– доводит до сведения работников Департамента положения законодательства РФ о ПДн и внутренних документов Департамента по вопросам обработки и защиты ПДн;

– организует прием и обработку обращений и запросов субъектов ПДн или их представителей, а также иных органов и организаций по вопросам, связанным с обработкой, передачей или защитой ПДн;

– участвует в выборе методов и способов защиты ПДн, в формировании требований по обеспечению безопасности ПДн;

– обеспечивает физическую защиту помещений, относящихся к контролируемой зоне;

– контролирует соответствие договоров и соглашений, заключаемых Департаментом с третьими лицами и связанных с передачей, совместной обработкой или поручением обработки персональных данных, требованиям законодательства РФ о ПДн;

– обеспечивает уведомление уполномоченного органа по защите прав субъектов ПДн об обработке (намерении осуществлять обработку) ПДн, изменениях, связанных с обработкой ПДн, за исключением случаев, установленных законодательстом Российской Федерации;

– разрабатывает и представляет на утверждение директору Департамента планы работ в области защиты ПДн.

3.3 Администратор информационной безопасности назначается приказом Департамента и в рамках обеспечения безопасности ПДн выполняет следующие функции:

– проводит оценку угроз безопасности ПДн, обрабатываемых в ИСПДн Департамента, и их источников, разрабатывает модели угроз безопасности ПДн, обрабатываемых в ИСПДн;

– разрабатывает и поддерживает в актуальном состоянии матрицу доступа к защищаемым информационным (программным) ресурсам;

– обеспечивает предоставление доступа к защищаемым информационным (программным) ресурсам в соответствии с матрицей доступа;

– участвует в выборе методов и способов защиты ПДн, обрабатываемых в ИСПДн, формирует требования по обеспечению безопасности ПДн с помощью инженерно-технических методов защиты;

– участвует в проектировании СЗПДн и внедрении средств защиты информации, взаимодействует с подрядными организациями, привлеченными для выполнения данных работ[1];

– обеспечивает безотказную работу и восстановление работоспособности ИСПДн в случае сбоя;

– осуществляет мониторинг функционирования средств защиты информации;

– проводит расследование инцидентов информационной безопасности;

– проводит инструктаж работников Департамента по вопросам обеспечения безопасности ПДн;

– обеспечивает соблюдение требований по безопасности информации при эксплуатации средств вычислительной техники, а также при выводе средств вычислительной техники или их элементов из эксплуатации, в том числе при передаче в ремонт.

3.4 Комиссия по подготовке и организации работ по защите ПДн утверждается приказом Департамента и в рамках обеспечения безопасности ПДн выполняет следующие функции:

– проводит внутреннее обследование в целях выявления фактов обработки ПДн в Департаменте;

– разрабатывает и представляет на утверждение директору Департамента:

- перечень ИСПДн;
- перечень ПДн, обрабатываемых в ИСПДн Департамента;
- перечень нормативных правовых актов, в соответствии с которыми производится обработка ПДн в ИСПДн Департамента, с указанием целей и сроков обработки ПДн (обоснование обработки ПД в ИСПДн Департамента);
- акт классификации ИСПДн Департамента;

– разрабатывает и представляет на утверждение директору Департамента планы работ в области защиты ПДн.

4 Порядок проведения работ по созданию системы защиты персональных данных

4.1 Обеспечение безопасности ПДн, обрабатываемых в Департаменте, должно достигаться скоординированным применением различных по своему характеру методов противодействия угрозам безопасности ПДн: правовых, организационных, экономических, инженерно-технических, программно-аппаратных.

4.2 Безопасность ПДн, обрабатываемых с помощью технических средств, обеспечивается системой защиты персональных данных и дополняющими ее мерами нетехнического характера.

4.3 Предусматриваются следующие стадии создания СЗПДн:

– предпроектная стадия;

– стадия проектирования;

– стадия реализации проектных решений;

– стадия ввода СЗПДн в действие;

– стадия сопровождения СЗПДн.

4.4 Предпроектная стадия создания СЗПДн включает в себя:

– обследование ИСПДн (определение перечня обрабатываемых ПДн; перечня технических средств, входящих в состав ИСПДн; круга лиц, имеющих доступ к ИСПДн и техническим средствам ИСПДн; технологического процесса обработки информации в ИСПДн и взаимодействия со сторонними организациями, связанного с передачей

[1] Привлекаемые подрядные организации должны обладать определенным перечнем лицензий.

обрабатываемых ПДн; условий хранения носителей ПДн и размещения технических средств ИСПДн и линий (каналов) связи);

– определение и оценку угроз безопасности обрабатываемых ПДн;

– классификацию ИСПДн;

– выбор методов и способов противодействия угрозам безопасности обрабатываемых ПДн;

– разработку технического задания на создание СЗПДн или общих требований к СЗПДн в соответствии с перечнем угроз безопасности ПДн, для противодействия которым представляется целесообразным применение программно-аппаратных методов.

4.5 Стадия проектирования СЗПДн подразумевает:

– разработку проектных решений по СЗПДн;

– разработку проектной документации на СЗПДн.

4.6 На стадии реализации проектных решений осуществляется:

– закупка, установка и настройка средств защиты информации в соответствии с проектной документацией на СЗПДн;

– разработка эксплуатационной документации на СЗПДн;

– реализация необходимых мероприятий организационного характера.

4.7 Стадия ввода СЗПДн в действие предусматривает:

– опытную эксплуатацию СЗПДн;

– приемо-сдаточные испытания СЗПДн;

– аттестацию ИСПДн по требованиям безопасности информации (оценку соответствия ИСПДн требованиям безопасности информации).

4.8 Стадия сопровождения СЗПДн подразумевает:

– поддержание в актуальном состоянии документов регламентирующих обеспечение безопасности ПДн;

– контроль и сопровождение аттестационных документов;

– поддержание в актуальном состоянии конфигурации средств и систем защиты информации;

– ежегодный инструментальный контроль;

– проведение аттестационных работ в рамках изменения конфигурации оборудования, замены оборудования, изменения основных и второстепенных технических средств и систем.

4.9 Работы на различных этапах создания СЗПДн могут проводиться как силами работников Департамента, так и сторонними организациями. При этом лицензированию подлежат следующие виды работ и услуг:

– контроль защищенности конфиденциальной информации от утечки по техническим каналам;

– контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;

– сертификационные испытания на соответствие требованиям по безопасности информации продукции, используемой в целях защиты конфиденциальной информации;

– аттестационные испытания и аттестация на соответствие требованиям по защите информации;

– проектирование в защищенном исполнении средств и систем информатизации, помещений со средствами (системами) информатизации, подлежащими защите, защищаемых помещений;

– установка, монтаж, испытания, ремонт средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищенности информации).

5 Порядок организации работ по эксплуатации информационных систем персональных данных

5.1 Ввод в эксплуатацию и вывод из эксплуатации ИСПДн осуществляются по акту при непосредственном участии лица, ответственного за эксплуатацию ИСПДн, и администратора информационной безопасности Департамента.

5.2 Лица, ответственные за эксплуатацию ИСПДн, определяются приказом Департамента.

5.3 Лица, ответственные за эксплуатацию ИСПДн обязаны:

- уведомлять лицо, ответственное за организацию обработки ПДн, о необходимости предоставления доступа работнику Департамента к ПДн, обрабатываемым в ИСПДн Департамента, администратора информационной безопасности Департамента – о необходимости предоставления дополнительных прав доступа к ИСПДн;
- уведомлять лицо, ответственное за организацию обработки персональных данных, об утрате работником Департамента необходимости доступа к ПДн, обрабатываемым в ИСПДн Департамента, (в связи с увольнением, переводом на другую должность);
- осуществлять текущий контроль за соблюдением правил обработки ПДн и требований по обеспечению их безопасности.

5.4 При выводе из эксплуатации (либо передаче сторонним организациям в целях ремонта) отдельных элементов ИСПДн администратор информационной безопасности обеспечивает удаление из запоминающих устройств ПДн и технологической (служебной, конфигурационной, управляющей и т.д.) информации способом, предусмотренным технологией записи в запоминающее устройство.

5.5 Эксплуатация ИСПДн и ее элементов должна осуществляться в соответствии с эксплуатационной документацией, утвержденными инструкциями и правилами.

5.6 По решению директора Департамента обработка ПДн может быть поручена сторонней организации на основании заключенного с данной организацией договора (соглашения) или контракта. Поручение обработки ПДн сторонней организации может происходить либо в форме предоставления доступа к ИСПДн Департамента для выполнения определенных функций по обработке ПДн, либо путем создания сторонней организацией собственной ИСПДн для выполнения переданных ей функций по обработке ПДн.

5.7 При принятии решения о поручении обработки ПДн сторонней организации лицо, ответственное за организацию обработки ПДн в Департаменте, определяет необходимость взимания согласия субъектов ПДн на поручение обработки их ПДн третьему лицу, обеспечивает соответствие формы договора (соглашения) или контракта на поручение обработки ПДн требованиям Федерального закона РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

6 Порядок предоставления доступа работникам Департамента к ИСПДн

6.1 Лицо, ответственное за организацию обработки ПДн в Департаменте, разрабатывает на основании внутреннего обследования, проведенного комиссией по подготовке и организации работ по защите ПДн, и представляет на утверждение директору Департамента:

– перечень лиц, имеющих доступ к ПДн, обрабатываемым в ИСПДн Департамента, в целях выполнения должностных обязанностей;

– перечень лиц, имеющих доступ в помещения[2], относящиеся к контролируемой зоне. Контролируемая зона устанавливается приказом Департамента.

6.2 Администратор информационной безопасности на основании внутреннего обследования, проведенного комиссией по подготовке и организации работ по защите ПДн, и в соответствии с утвержденным перечнем лиц, имеющих доступ к ПДн, обрабатываемым в ИСПДн Департамента, в целях выполнения должностных обязанностей, и перечнем лиц, имеющих доступ в помещения, в которых установлены технические средства ИСПДН либо хранятся материальные носители ПДн :

– разрабатывает и представляет на утверждение директору Департамента:

o перечень лиц, имеющих доступ к техническим средствам ИСПДн Департамента для выполнения технического обслуживания и (или) сопровождения программного обеспечения,

o описание технологического процесса обработки информации;

– разрабатывает матрицу доступа к защищаемым информационным (программным) ресурсам Департамента.

Матрица доступа должна содержать:

– перечень ИСПДн Департамента;

– перечень защищаемых информационных (программных) ресурсов Департамента;

– перечень работников Департамента, допущенных к самостоятельной работе в ИСПДн;

– перечень сотрудников сторонних организаций, имеющих доступ к ИСПДн Департамента в целях обработки ПДн;

– перечень физических и юридических лиц, допущенных к техническим средствам ИСПДн Департамента для выполнения технического обслуживания и (или) сопровождения программного обеспечения;

– права различных категорий лиц, допущенных к ИСПДн, в отношении защищаемых информационных (программных) ресурсов.

Работники Департамента, допущенные к самостоятельной работе в ИСПДн, и сотрудники сторонних организаций, имеющих доступ к ИСПДн Департамента в целях обработки ПДн, являются пользователями ИСПДн.

6.3 В случае необходимости предоставления работнику Департамента доступа к ПДн, обрабатываемым в ИСПДн, для выполнения должностных обязанностей, лицо, ответственное за эксплуатацию ИСПДн, обращается к лицу, ответственному за организацию обработки ПДн. При этом лицо, ответственное за организацию обработки ПДн, может запросить подтверждение необходимости предоставления доступа к ПДн данному работнику (в виде ссылки на должностную инструкцию, трудовой договор работника), после чего лицо, ответственное за организацию обработки ПДн, включает работника в перечень лиц, имеющих доступ к ПДн, обрабатываемым в ИСПДн Департамента, в целях выполнения должностных обязанностей, и предоставляет актуализированный перечень на утверждение директору Департамента.

[2] Речь идет обо всех штатных работниках, имеющих право самостоятельного доступа в указанные помещения. Доступ в помещение – возможность посещения помещения без нарушения принятых в организации норм и регламентов, не зависящая от воли других лиц.

6.4 После утверждения актуализированного перечня лиц, имеющих доступ к ПДн, обрабатываемым в ИСПДн Департамента, в целях выполнения должностных обязанностей, лицо, ответственное за организацию обработки ПДн, уведомляет об этом администратора информационной безопасности. Администратор информационной безопасности вносит необходимые изменения в матрицу доступа к защищаемым информационным (программным) ресурсам.

Администратор информационной безопасности обеспечивает создание новой учетной записи пользователя ИСПДн и назначает данной записи права в соответствии с матрицей доступа. Администратор информационной безопасности обеспечивает генерацию необходимой для доступа к ИСПДн аутентификационной (парольной) и ключевой информации, при необходимости обеспечивает подготовку материальных носителей аутентификационной и ключевой информации.

6.5 Обязательным условием предоставления работнику Департамента возможности обработки ПДн в ИСПДн является прохождение им инструктажа по вопросам обеспечения безопасности ПДн и ознакомление с положениями законодательства РФ о ПДн и защите информации и внутренних документов Департамента.

Факт прохождения инструктажа подтверждается росписью работника в листе ознакомления с соответствующими документами (в том числе, Инструкцией пользователя ИСПДн).

После прохождения работником инструктажа администратор информационной безопасности выдает ему под роспись имя учетной записи, материальный носитель аутентификационной и ключевой информации (при необходимости), парольную информацию.

7 Порядок предоставления доступа сотрудникам сторонних организаций к ИСПДн в целях обработки ПДн

7.1 Предоставление доступа сотрудникам сторонних организаций к ИСПДн в целях обработки ПДн осуществляется на основании договора (соглашения) или контракта. Формы договоров (соглашений) или контрактов разрабатывает и согласует лицо, ответственное за организацию обработки ПДн в Департаменте.

7.2 После заключения со сторонней организацией договора (соглашения) или контракта, в соответствии с которым сотрудники сторонней организации могут иметь доступ к ИСПДн Департамента в целях обработки ПДн, директор Департамента уведомляет об этом администратора информационной безопасности и лицо, ответственное за организацию обработки ПДн, и передает им копии соответствующего договора (соглашения) или контракта.

7.3 Руководитель сторонней организации подготавливает список лиц, которым необходим доступ к ИСПДн (с указанием выполняемых ими функций по обработке ПДн) и направляет его директору Департамента.

Список сотрудников сторонней организации, которым должен быть предоставлен доступ к ИСПДн, утвержденный директором Департамента, передается администратору информационной безопасности и лицу, ответственному за организацию обработки ПДн.

7.4 Администратор информационной безопасности вносит необходимые дополнения в матрицу доступа к защищаемым информационным (программным) ресурсам.

Администратор информационной безопасности обеспечивает создание новых учетных записей пользователей ИСПДн и назначает им права в соответствии с матрицей доступа. Администратор информационной безопасности обеспечивает генерацию необходимой для доступа к ИСПДн аутентификационной (парольной) и ключевой информации, при необходимости подготавливает материальные носители аутентификационной и ключевой информации.

Имена учетных записей, материальные носители аутентификационной и ключевой информации (при необходимости), парольная информация передается руководителю сторонней организации.

7.5 Ознакомление сотрудников сторонних организаций с положениями законодательства РФ о ПДн и защите информации и инструктаж пользователей по вопросам обеспечения безопасности ПДн, обрабатываемых в ИСПДн, обеспечивает руководитель сторонней организации.

8 Порядок изменения прав пользователей ИСПДН на доступ к ИСПДн

8.1 В случае необходимости предоставления пользователю ИСПДн дополнительных прав в отношении защищаемых информационных (программных) ресурсов, лицо, ответственное за эксплуатацию ИСПДн, обращается к администратору информационной безопасности. Администратор информационной безопасности имеет право запросить у обратившегося лица подтверждение необходимости предоставления дополнительных прав в отношении защищаемых информационных (программных) ресурсов пользователю ИСПДн (в виде ссылки на должностную инструкцию, трудовой договор и т. д.), после чего администратор информационной безопасности вносит необходимые изменения в матрицу доступа к защищаемым информационным (программным) ресурсам.

Администратор информационной безопасности обеспечивает изменение прав учетной записи пользователя ИСПДн в соответствии с матрицей доступа.

8.2 В случае утраты работником Департамента необходимости доступа к ИСПДн (при увольнении работника, переводе его на другую должность) лицо, ответственное за эксплуатацию ИСПДн, уведомляет лицо, ответственное за организацию обработки ПДн, за три дня до наступления указанного события.

Лицо, ответственное за организацию обработки ПДн, исключает работника из перечня лиц, имеющих доступ к ПДн, обрабатываемым в ИСПДн Департамента, в целях выполнения должностных обязанностей, или корректирует указанный перечень (при переводе лица на другую должность), и представляет актуализированный перечень на утверждение директору Департамента.

После утверждения актуализированного перечня лиц, имеющих доступ к ПДн, обрабатываемым в ИСПДн Департамента, в целях выполнения должностных обязанностей, лицо, ответственное за организацию обработки ПДн, уведомляет об этом администратора информационной безопасности. Администратор информационной безопасности вносит необходимые изменения в матрицу доступа к защищаемым информационным (программным) ресурсам.

Администратор информационной безопасности удаляет учетную запись пользователя ИСПДн.

8.3 В случае утраты сотрудником сторонней организации необходимости доступа к ИСПДн в целях обработки ПДн (при увольнении работника, переводе его на другую должность) руководитель сторонней организации сообщает об этом директору Департамента и возвращает материальные носители аутентификационной и ключевой информации пользователя ИСПДн (в случае их использования).

Директор Департамента уведомляет лицо, ответственное за организацию обработки ПДн, и администратора информационной безопасности. Администратор информационной

безопасности вносит необходимые изменения в матрицу доступа к защищаемым информационным (программным) ресурсам. Администратор информационной безопасности удаляет учетную запись пользователя ИСПДн.

9 Порядок организации доступа к ИСПДн и их элементам сторонних организаций в целях обслуживания технических средств ИСПДН и сопровождения программного обеспечения

9.1 При взаимодействии со сторонними организациями в случаях, когда сотрудникам этих организаций предоставляется доступ к ИСПДн или ее элементам, с этими организациями заключается соглашение о соблюдении режима безопасности информации при выполнении работ, предусматривающее процедуру определения прав и условий доступа сотрудникам сторонних организаций к защищаемым объектам, и разграничение между сторонами соглашения зон ответственности за нарушение требований безопасности. Данное соглашение может быть включено в договор, заключаемый со сторонними организациями.

9.2 Доступ сотрудников сторонних организаций к ИСПДн и ее элементам в обязательном порядке осуществляется в присутствии администратора информационной безопасности или (по решению администратора информационной безопасности) лица, ответственного за эксплуатацию ИСПДн. Указанные лица организуют доступ сотрудников сторонних организаций к ИСПДн и ее элементам так, чтобы исключить возможность несанкционированного доступа к ПДн или их носителям, в том числе, возможность хищения носителя ПДн. При невозможности исключить доступ к ПДн, обрабатываемым в ИСПДн, сотрудник сторонней организации, осуществляющий доступ, должн быть под роспись уведомлен о необходимости соблюдать конфиденциальность ПДн и об ответственности за нарушение заданных характеристик безопасности информации.

10 Порядок организации внутреннего контроля процесса обработки и обеспечения безопасности персональных данных

10.1 Внутренний контроль процесса обработки и обеспечения безопасности ПДн заключается в проверке выполнения установленных законодательством РФ и внутренними документами Департамента требований по обработке, хранению и обеспечению безопасности ПДн. Целью проведения внутренних проверок является выявление и своевременное устранение нарушений требований по обеспечению безопасности ПДн, в том числе, путем принятия дополнительных мер по обеспечению безопасности ПДн.

10.2 Мероприятия по осуществлению внутреннего контроля процесса обработки и обеспечения безопасности ПДн направлены на решение следующих задач:

– обеспечение соблюдения работниками Департамента требований настоящего Положения и других внутренних документов Департамента, а также нормативных правовых актов, регулирующих сферу обработки ПДн;

– оценка компетентности работников Департамента, задействованных в обработке ПДн, и определение необходимости их обучения по вопросам обработки ПДн и (или) обеспечения безопасности ПДн;

– обеспечение соответствия условий эксплуатации технических средств ИСПДн и средств защиты информации требованиям технической и эксплуатационной документации;

– выявление изменений технологического процесса обработки ПДн, новых угроз безопасности ПДн и их источников, иных факторов, влияющих на оценку угроз безопасности ПДн;

– сбор информации, необходимой для анализа выявленных нарушений требований по обработке, хранению и обеспечению безопасности ПДн, выработки предложений и

принятия решений по совершенствованию порядка обработки и обеспечения безопасности ПДн.

10.3 Лица, ответственные за эксплуатацию ИСПДн, обеспечивают текущий контроль соблюдения лицами, имеющими доступ к ИСПДн, требований по эксплуатации ИСПДн.

10.4 Лицо, ответственное за организацию обработки ПДн, совместно с администратором информационной безопасности проводит регулярные проверки соблюдения требований по обеспечению безопасности ПДн. Порядок, формы и план проведения внутреннего контроля соблюдения требований по обеспечению безопасности ПДн могут быть закреплены отдельными документами, утвержденными директором Департамента, либо определяться лицом, ответственным за организацию обработки ПДн, совместно с администратором информационной безопасности самостоятельно.

10.5 Результаты контрольных мероприятий должны быть документально зафиксированы. Лицо, ответственное за организацию обработки ПДн, представляет директору Департамента отчеты о результатах проведения мероприятий по внутреннему контролю процесса обработки и обеспечения безопасности ПДн.

11 Трансграничная передача персональных данных

11.1 В рамках функционирования ИСПДн Департамента трансграничная передача обрабатываемых ПДн не осуществляется.

11.2 Исключен.

12 Порядок взаимодействия с государственными органами

12.1 По запросу уполномоченного органа по защите прав субъектов ПДн лицо, ответственное за организацию обработки ПДн, оценивает правомерность запроса и обеспечивает подготовку ответа в течение семи рабочих дней с даты получения запроса. Если запрос связан с выявлением не точных ПДн или неправомерной обработки ПДн, то лицо, ответственное за организацию обработки ПДн (при необходимости – совместно с администратором информационной безопасности), обеспечивает блокирование соответствующих ПДн на период проведения проверки.

12.2 При получении правомерного запроса на исправление выявленных нарушений лицо, ответственное за организацию обработки ПДн в Департаменте, устраняет нарушение собственными силами, если нарушение касается содержания таких документов, как согласие на обработку ПДн, уведомления, договоры, соглашения и т. п. В том случае, если нарушения связаны с удалением, уточнением ПДн, а также с техническими вопросами обеспечения безопасности ПДн, обязанность устранения нарушения возлагается на администратора информационной безопасности Департамента.

12.3 В установленных федеральным законодательством случаях Департамент обязан предоставлять информацию, содержащую ПДн, по мотивированному запросу уполномоченных органов государственной власти по вопросам их компетенции либо судебных органов.