Приложение №1
к приказу от ____ 2015 г. №____

ПОЛИТИКА
В ОТНОШЕНИИ ОБРАБОТКИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящая Политика защиты персональных данных (далее – Политика) разработана на основании ст. 24 Конституции РФ, главы 14 Трудового Кодекса РФ, Закона «Об информации, информатизации и защите информации» № 149-ФЗ от 27.07.2006 г., Федерального закона РФ «О персональных данных» № 152-ФЗ от 27.07.2006 г.

1.2. Настоящая Политика утверждается приказом начальника Департамента.

1.3. Настоящая Политика определяет:

- порядок обработки (сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления доступа), обезличивания, блокирования, удаления, уничтожения) персональных данных в Департаменте;

- порядок обеспечения защиты прав и свобод субъектов персональных данных при обработке их персональных данных с использованием средств автоматизации или без использования таких средств, а также устанавливает ответственность лиц, имеющих доступ к персональным данным, за невыполнение требований, регулирующих обработку и защиту персональных данных.

Целью настоящей Политики является обеспечение безопасности объектов защиты Департамента от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональных данных.

1.4. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

1.5. Для целей настоящей Политики используются следующие основные понятия:

1) персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2) оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

3) 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;

4) автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

5) распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

6) предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

7) блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

8) уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

9) обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

10) информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

1.6. В настоящей Политике используются следующие обозначения и сокращения:

АРМ – автоматизированное рабочее место

ИСПДн – информационная система персональных данных

НСД – несанкционированный доступ

ПДн – персональные данные

СЗИ – средства защиты информации

СЗПДн – система (подсистема) защиты персональных данных

2 ОБЛАСТЬ ДЕЙСТВИЯ

Требования настоящей Политики распространяются на всех работников Департамента, а также всех прочих лиц (имеющих санкционированный доступ информационным системам и ресурсам Департамента (сотрудников контролирующих органов, аудиторы и т.п.).

3 ОСНОВНЫЕ ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Основной целью обеспечения безопасности персональных данных является минимизация ущерба (как непосредственного, так и опосредованного), возникающего вследствие возможной реализации угроз безопасности персональных данных.

Непосредственный ущерб связан с причинением материального, финансового или морального вреда непосредственно субъекту персональных данных и может проявляться в виде:

- незапланированных и (или) непроизводительных финансовых или материальных затрат субъекта;
- потери субъектом свободы действий вследствие шантажа и угроз, осуществляемых с использованием персональных данных;
- нарушения конституционных прав субъекта вследствие вмешательства в его личную жизнь.

Основной задачей обеспечения безопасности персональных данных, при их обработке в Департаменте, является предотвращение утечки персональных данных по техническим каналам, несанкционированного доступа к ним, предупреждение преднамеренных программно-технических воздействий с целью их разрушения (уничтожения) или искажения в процессе обработки, передачи и хранения

4 ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ОБРАБАТЫВАЕМЫЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

4.1. Состав персональных данных

Состав персональных данных и ИСПДн, подлежащих защите, определяется в ходе проведения обследования информационных потоков в Департаменте и отражается в «Сводном перечне персональных данных, подлежащих защите».

4.2.Категории субъектов персональных данных

В Департаменте обрабатываются персональные данные следующих субъектов:

1) Сотрудники Департамента, обработка персональных данных которых осуществляется в целях выполнения положений Трудового Кодекса РФ.

2) Граждане, желающие принять ребёнка в семью на основании Федерального закона от 16 апреля 2001 г. № 44-ФЗ «О государственном банке данных о детях, оставшихся без попечения родителей».

3) Дети, оставшиеся без попечения родителей на основании Федерального закона от 16 апреля 2001 г. № 44-ФЗ «О государственном банке данных о детях, оставшихся без попечения родителей».

4.3. Цели обработки персональных данных

В основе определения целей обработки персональных данных лежит принцип законности их обработки.

Целями обработки персональных данных сотрудников являются содействие в трудоустройстве, обучение и продвижение по службе, обеспечение личной безопасности сотрудников, контроль количества и качества выполняемой работы и обеспечение сохранности имущества.

Целями обработки персональных данных граждан является исполнение Федерального закона от 16 апреля 2001 г. № 44-ФЗ «О государственном банке данных о детях, оставшихся без попечения родителей».

При определении целей обработки персональных данных иных категорий субъектов персональных данных, необходимо соблюдать законы и иные нормативно-правовые акты.

4.4. Состав персональных данных субъектов персональных данных

Состав персональных данных должен соответствовать принципу их достаточности для достижения целей обработки (персональные данные не должны быть избыточными по отношению к целям обработки).

4.5. Характеристики безопасности персональных данных

Персональные данные, обрабатываемые в информационных системах Департамента, обладают как минимум свойствами конфиденциальности, целостности, доступности.

Для обеспечения заданных характеристик безопасности персональных данных в Департаменте реализован базовый и достаточный набор организационно-технических мер.

5 ОБЩИЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПД И ИСПДн

Построение СЗПДн в Департамаенте и ее функционирование осуществляется в соответствии со следующими основными принципами:

- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- разумная достаточность и адекватность;
- персональная ответственность;
- минимизация полномочий;
- гибкость;
- открытость алгоритмов и механизмов защиты;
- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;
- наблюдаемость и оцениваемость;
- обязательность контроля и оценки.

5.1. Законность

Защита ПДн в ИСПДн Департаменте основывается на положениях и требованиях существующих законов, стандартов и нормативно-методических документов по защите ПДн и учитывает лучшие мировые практики.

5.2. Системность

Системный подход к построению СЗПДн предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов,

условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ПДн Департамаента.

5.3. Комплексность

Безопасность ПДн обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер, реализованных в Департаменте.

Применение различных средств и технологий защиты информации обеспечивает предотвращение всех существенных (значимых) каналов реализации угроз безопасности ПДн.

СЗПДн строится с учетом не только всех известных каналов проникновения и несанкционированного доступа (далее – НСД) к ПДн, но и с учетом возможности повышения уровня защиты по мере выявления новых источников УБПДн, развития способов и средств их реализации в ИСПДн.

СЗПДн Департамента строится на основе использования сертифицированных средств защиты информации. При создании СЗПДн могут использоваться системы и средства защиты информации, используемые в организации для обеспечения безопасности иной конфиденциальной информации.

5.4. Непрерывность

Защита ПДн обеспечивается на всех технологических этапах обработки ПДн и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

5.5. Своевременность

Принимаемые меры по обеспечению безопасности ПДн носят упреждающий характер.

Департамент принимает необходимые меры по защите ПДн до начала обработки ПДн, которые должны обеспечить надлежащий уровень безопасности ПДн.

СЗПДн разрабатывается одновременно с разработкой и развитием ИСПДн Департамента, что позволяет учитывать требования по безопасности ПДн при проектировании и модернизации ИСПДн.

5.6. Преемственность и непрерывность совершенствования

Предполагают постоянное совершенствование мер и средств защиты ПДн на основе результатов анализа функционирования ИСПДн и СЗПДн с учетом выявления новых способов и средств реализации УБПДн, отечественного и зарубежного положительного опыта в сфере защиты информации.

Департамент определяет действия, необходимые для устранения причин потенциальных несоответствий требованиям по безопасности ПДн с целью предотвратить их повторное появление.

5.7. Разумная достаточность и адекватность

Состояние и стоимость реализации мер защиты должно быть соизмеримы с рисками, связанными с обработкой и характером защищаемых ПДн.

Анализ рисков нарушения безопасности ПДн проводится в целях определения влияния системы защиты информации на вероятность реализации угроз безопасности ПДн с учетом уязвимостей (дефектов) ИТ-инфраструктуры Департамента.

Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики и производительность ИСПДн Департамента.

5.8. Персональная ответственность

Ответственность за обеспечение безопасности ПДн и ИСПДн Департамента возлагается на каждого сотрудника, допущенного к обработке персональных данных, в пределах его полномочий.

Распределение обязанностей и полномочий сотрудников Департамента позволяет обеспечить выявление виновных лиц в случаях нарушения безопасности ПДн.

Роли и обязанности сотрудников Департамента определены и документально подтверждены в соответствии с организационной политикой в области защиты информации.

5.9. Минимизация полномочий

Предоставление и использование прав доступа к ПДн ограничено и управляемо.

Пользователям предоставляются минимально необходимые права доступа к ПДн и ИСПДн только в соответствии с производственной необходимостью.

Доступ к ПДн предоставляется только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

Сотруднику запрещены все операции с ПДн за исключением тех, которые разрешены явно.

5.10. Гибкость

В процессе функционирования ИСПДн могут меняться ее характеристики, а также объем и категория обрабатываемых Департаменте ПДн.

Для обеспечения возможности варьирования уровня защищенности ПДн, СЗПДн Департамента обладает определенной гибкостью.

5.11. Открытость алгоритмов и механизмов защиты

Защита ПДн не должна осуществляться только за счет сокрытия структуры, технологий и алгоритмов функционирования СЗПДн.

Знание указанных характеристик СЗПДн не должно давать возможности преодоления защиты возможными нарушителями безопасности ПДн, включая разработчиков средств защиты.

5.12. Научная обоснованность и техническая реализуемость

Уровень рекомендаций и требований по защите ПДн соответствует имеющемуся уровню развития информационных технологий и средств защиты информации.

При создании и эксплуатации СЗПДн используются лучшие современные отечественные и зарубежные технические решения и практику защиты информации.

5.13. Специализация и профессионализм

Реализация мер по обеспечению безопасности ПДн и эксплуатация СЗПДн осуществляется профессионально подготовленными специалистами Департамента

5.14. Знание своих работников

Департамент реализует кадровую политику (тщательный подбор персонала и мотивация сотрудников), позволяющую исключить или минимизировать возможность нарушения безопасности ПДн своими сотрудниками.

5.15. Наблюдаемость и оцениваемость обеспечения безопасности персональных данных

Предлагаемые Департаментом меры по обеспечению безопасности ПДн спланированы так, чтобы результат их применения был явно наблюдаем (прозрачен)

и мог быть оценен федеральными органами исполнительной власти, осуществляющими функции по контролю и надзору в пределах своих полномочий.

5.16. Обязательность контроля и оценки

Неотъемлемой частью работ по защите ПДн является оценка эффективности системы защиты.

С целью своевременного выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПДн в Департаменте определены процедуры для постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются.

6 ОБЩИЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Классификация методов обеспечения безопасности персональных данных

Методы обеспечения безопасности ПДн разделяются на:

- административно-правовые;
- организационно-технические;
- физические.

По времени применения методы обеспечения безопасности ПДн разделяются на:

- превентивные;
- восстановительные.

6.2. Административно-правовые методы

К административно-правовым методам защиты относятся нормы действующего законодательства и внутренние организационно-распорядительные документы Департамента, регламентирующие правила обращения с ПДн, закрепляющие права и обязанности участников информационных отношений в процессе обработки и использования ПДн, а также устанавливающие ответственность за нарушения этих правил, препятствуя неправомерному использованию ПДн и являющиеся сдерживающим фактором для реализации угроз безопасности потенциальными нарушителями.

Основными направлениями этой деятельности Департамента являются:

- разработка, внесение изменений и дополнений в политику информационной безопасности в части защиты ПДн и поддерживающие ее документы;
- регламентация процессов обработки ПДн;
- определение ответственности за нарушения в области обеспечения безопасности ПДн;
- назначение и подготовка должностных лиц (работников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности ПДн;
- закрепление в должностных инструкциях установленного разграничения полномочий в области обеспечения безопасности ПДн;
- разработка и принятие документов, устанавливающих ответственность структурных подразделений и сотрудников, а также взаимодействующих юридических лиц, за несанкционированный доступ к ПДн, противоправное копирование, искажение и противозаконное использование, преднамеренное распространение недостоверных ПДн, противоправное их раскрытие или использование в преступных и корыстных целях;

- контроль знания и соблюдения пользователями ИСПДн, требований организационно-распорядительных документов по вопросам обеспечения безопасности ПДн;
- проведение постоянного анализа эффективности и достаточности принимаемых мер и применяемых средств защиты ПДн, разработка и реализация предложений по совершенствованию СЗПДн.

6.3. Организационно-технические методы

Организационно-технические методы защиты основаны на использовании организационных мер, различных программных, аппаратных и программно - аппаратных средств, входящих в состав СЗПДн и выполняющих функции защиты информации, направленных на решение следующих задач:

- строгий учет всех подлежащих защите ресурсов (персональных данных, сервисов, каналов связи, серверов, автоматизированных рабочих мест и т.д.);
- предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременного обнаружения фактов НСД к ПДн;
- недопущения воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;
- возможности незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие НСД к ним;
- постоянного контроля за обеспечением уровня защищенности ПДн.

6.4. Физические методы

Физические методы защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

6.5. Превентивные методы

Превентивные методы противодействия угрозам безопасности ПДн осуществляются на основе эффективного применения в процессе эксплуатации ИСПДн комплекса организационных, технических и технологических мероприятий, а также методов и средств обеспечения функциональной устойчивости и безопасности работы ИСПДн.

Организационные мероприятия по обеспечению безопасности ПДн являются мероприятиями общего характера по организации деятельности персонала, эксплуатирующего ИСПДн, порядку применения информационных технологий в зданиях и сооружениях, систематическому применению мер по недопущению вывода ИСПДн из строя.

Технические мероприятия по обеспечению безопасности ПДн заключаются в обслуживании, поддержании и управлении требуемым составом технических средств, обеспечивающих обработку ПДн в защищенном режиме.

Технологические мероприятия по обеспечению безопасности ПДн направлены на правильную реализацию функций и заданных алгоритмов работы ИСПДн,

технологий обработки ПДн и защиту программ и ПДн от преднамеренных и непреднамеренных нарушений.

6.6. Восстановительные методы

Планирование восстановительных методов определяется системой документов, устанавливающих требования к обязательным мероприятиям, проводимым заблаговременно и после возникновения нарушений, угрожающих штатному функционированию ИСПДн.

6.7. Основные этапы работ по обеспечению безопасности персональных данных

В число основных этапов работ по обеспечению безопасности персональных данных входят, в частности, следующие:

- определение объектов защиты;
- установление целей защиты объектов защиты;
- определение угроз объектам защиты;
- установление требований к системе защиты персональных данных;
- определение порядка контроля и надзора.

Основным объектом защиты являются персональные данные.

Персональные данные могут иметь различные формы представления (бумажная, файлы, записи и поля записей баз данных, электромагнитные волны и поля, излучения и т.д.), каждая из которых является объектом защиты.

Формы представления персональных данных связаны с различными ресурсами информационной системы персональных данных, которые в свою очередь могут порождать объекты защиты.

Используемые в информационной системе персональных данных средства защиты информации являются объектами защиты.

Информация о методах и средствах обеспечения безопасности персональных данных содержит сведения, которые являются объектами защиты, в частности, к таким объектам могут быть обнесены парольная и аутентифицирующая информация, ключевая информация

Установление целей защиты объектов защиты связано с установлением характеристик безопасности для каждого из определенных объектов защиты.

Определение угроз объектам защиты проводится путем формирования модели угроз и модели нарушителя. При этом модель нарушителя формируется как составная часть модели угроз, определяющая возможные специфические угрозы – атаки.

Установление требований к системе защиты персональных данных основано на формировании моделей угроз и нарушителя.

В первую очередь устанавливаются общие требования к организационным мерам.

Далее на основе моделей угроз и нарушителя, сформированных в соответствии с нормативными и методическими документами ФСТЭК России и ФСБ России, определяются требования к средствам защиты информации, а также требования к поддерживающим эти средства организационным мерам.

Процесс формирования требований к системе защиты персональных данных заканчивается, если выполнение установленных требований нейтрализует все угрозы, перечисленные в моделях угроз и нарушителя.

7. ОСНОВНЫЕ МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Для разработки и осуществления мероприятий по организации и обеспечению безопасности ПДн при их обработке в ИСПДн Департамента назначается должностное лицо, ответственное за обеспечение безопасности ПДн.

Основными мероприятиями по организации и техническому обеспечению безопасности ПДн в ИСПДн являются:

- мероприятия по организации обеспечения безопасности ПДн, включая классификацию ИСПДн;
- мероприятия по техническому обеспечению безопасности ПДн при их обработке в ИСПДн, включающие мероприятия по размещению, специальному оборудованию, охране и организации режима допуска в помещения, где ведется работа с ПДн;
- мероприятия по защите ПДн от несанкционированного доступа и определению порядка выбора средств защиты ПДн при их обработке в ИСПДн.

Обеспечение безопасности ПДн осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках создаваемой СЗПДн. Структура, состав и основные функции СЗПДн определяются с учетом класса ИСПДн.

Перечень реализуемых мероприятий по защите ПДн при их обработке в специальных ИСПДн определяется на основании анализа актуальности угроз, рисков безопасности ПДн, в соответствии с нормативными и методическим документами ФСБ России и ФСТЭК России.

ИСПДн по своим характеристикам и номенклатуре угроз безопасности ПДн близки к наиболее распространенным информационным системам, поэтому целесообразно при их защите максимально использовать традиционные подходы к технической защите информации в автоматизированных системах.

Методы и способы защиты информации в информационных системах устанавливаются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

В соответствии с нормативными документами Федеральной службы по техническому и экспортному контролю:

- осуществляется обеспечение защиты (некриптографическими методами) информации;
- проводятся мероприятия по предотвращению утечки информации по техническим каналам;
- проводятся мероприятия по предотвращению несанкционированного доступа к информации, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения, и блокирования доступа к ней.

В соответствии с нормативными документами Федеральной службы безопасности Российской Федерации:

- устанавливаются особенности разработки, производства, реализации и эксплуатации шифровальных (криптографических) средств защиты

информации и предоставления услуг по шифрованию персональных данных при их обработке в информационных системах;
- проводятся мероприятия по обнаружению компьютерных атак.

Мероприятия по обеспечению безопасности ПДн включают в себя:
- управление доступом:
  - идентификация и аутентификация;
  - физическая защита;
- регистрацию и учет;
- обеспечение конфиденциальности;
- обеспечение целостности;
- обеспечение доступности;
- обеспечение достоверности (аутентичности);
- антивирусную защиту;
- обеспечение безопасного межсетевого взаимодействия;
- анализ защищенности;
- обнаружение вторжений;
- обеспечение безопасного доступа к сетям международного информационного обмена.

7.1. Идентификация и аутентификация

Управление доступом к ПДн осуществляется на основе принципа минимизации полномочий. Стандартным методом доступа является ролевой доступ, для чего определяются совокупности типов доступа - групповых прав и полномочий доступа пользователей (ролей), предоставляемых пользователям. Количество таких ролей ограниченно и подразумевает возможность эффективного управления. Назначение прав и полномочий конкретным пользователям осуществляется путем назначения им соответствующих ролей.

Каждый пользователь для получения соответствующих прав доступа при подключении к ИСПДн проходит процедуру идентификации, при этом используются уникальные признаки и имена. Стандартное средство проверки подлинности (аутентификации) – пароль. Для обеспечения более высокой надежности аутентификации возможно использование таких средств как токены, смарт-карты и другие носители аутентифицирующей информации.

7.2. Физическая защита

Физическая защита зданий, помещений, объектов и средств информатизации осуществляется с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации.

Размещение, специальное оборудование, охрана и организация режима в помещениях исключает возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

7.3. Регистрация и учет

В ИСПДн ведутся контрольные журналы, регистрирующие действия пользователей с ПДн. Установлены процедуры применения мониторинга действий с ПДн, а результаты действий пользователей регулярно просматриваются.

В целях повышения эффективности контроля действий возможных нарушителей возможно использование средств и методов активного мониторинга и аудита, направленных на выявление и регистрацию подозрительных действий в реальном масштабе времени.

7.4. Обеспечение целостности

В Департаменте обеспечивается целостность программных средств защиты в составе СЗПДн, а также неизменность программной среды. При этом целостность средств защиты проверяется при загрузке системы по наличию имен (идентификаторов) компонентов СЗПДн, целостность программной среды обеспечивается отсутствием в ИСПДн средств разработки и отладки программ.

Обеспечение целостности реализуется преимущественно операционными системами и системами управления базами данных. Средства повышения достоверности и обеспечения целостности передаваемых данных и надежности транзакций, встраиваемые в операционные системы и системы управления базами данных, основаны на расчете контрольных сумм, уведомлении о сбое в передаче пакета сообщения, повторе передачи не принятого пакета.

7.5. Антивирусная защита

Для обеспечения безопасности ПДн и программно-аппаратной среды ИСПДн, осуществляющей обработку этой информации, применяются специальные средства антивирусной защиты, выполняющие:

- обнаружение и (или) блокирование деструктивных вирусных воздействий на общесистемное и прикладное программное обеспечение, реализующее обработку ПДн, а также на ПДн;
- обнаружение и удаление неизвестных вирусов;
- обеспечение самоконтроля (предотвращение инфицирования) данного антивирусного средства при его запуске.

7.6. Обеспечение безопасного межсетевого взаимодействия

Для осуществления разграничения доступа к ресурсам ИСПДн при межсетевом взаимодействии применяется межсетевое экранирование, которое реализуется программными и программно-аппаратными межсетевыми экранами. Межсетевой экран устанавливается между защищаемой сетью, называемой внутренней, и внешней сетью. Межсетевой экран входит в состав защищаемой сети. Для него путем настроек отдельно задаются правила, ограничивающие доступ из внутренней сети во внешнюю и наоборот.

Межсетевое экранирование обеспечивает:

- скрытие внутренней сетевой структуры ИСПДн;
- разрешение только такого входящего и исходящего трафика, который является необходимым для работы ИСПДн;
- блокирование любого входящего и исходящего трафика, не разрешенного явно.

7.7. Анализ защищенности

Анализ защищенности реализуется на основе использования средств тестирования (анализа защищенности) и контроля (аудита) безопасности информации.

Для гарантии того, что СЗИ успешно выполняют свои функции, разрабатываются процедуры контроля изменений конфигураций СЗИ и сетевых

устройств. Для выполнения этих процедур в информационно-телекоммуникационной среде создается система анализа защищенности, выполняющая следующие функции:

- контроль настроек сетевых устройств, СЗИ и программно-технического обеспечения ИСПДн;
- анализ уязвимостей настроек СЗИ, сетевых устройств или уязвимостей операционных систем или прикладного программного обеспечения.

7.8. Обнаружение вторжений

Обнаружение вторжений реализуется с использованием в составе СЗПДн программных и (или) программно-аппаратных средств (систем) обнаружения вторжений, использующих комбинированные методы обнаружения атак, включающие в себя сигнатурные методы и методы выявления аномалий.

7.9. Криптографическая защита

Для зашиты ПДн, передаваемых между ИСПДн по каналам связи, выходящим за пределы контролируемой зоны, используются защищенные каналы связи.

При использовании открытых и неконтролируемых каналов связи для защиты ПДн применяются средства криптографической защиты информации (далее – СКЗИ). Как раздельно, так и комплексно, используются следующие криптографические методы:

- шифрование, как средство обеспечения конфиденциальности информации;
- электронная цифровая подпись, как средство обеспечения подлинности и юридической значимости электронного документа;
- криптографическая аутентификация, как средство подтверждения санкционированности доступа субъекта к объекту;
- управление ключами, как необходимая составная часть систем с СКЗИ, которая применяется в целях изготовления, учета, распределения, хранения и уничтожения ключевых элементов.

7.10. Обеспечение безопасного доступа к сетям международного информационного обмена

Доступ ИСПДн к сетям связи общего пользования и (или) сетям международного информационного обмена, в том числе к международной компьютерной сети «Интернет» допускается только с использованием специально предназначенных для этого средств защиты информации.

8 ПРИНЦИПЫ ОЦЕНКИ И КОНТРОЛЯ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. В соответствии с принципом обязательности контроля выполняются следующие виды контроля эффективности системы защиты персональных данных:

- внутренний контроль;
- государственный контроль.

8.2. Внутренний контроль эффективности системы защиты ПДн осуществляется Департаментом с целью поддержания заданного уровня эффективности СЗПДн, в соответствии с документированными методиками. Внутренний контроль включает:

- мониторинг состояния технических и программных средств, входящих в состав СЗПДн;
- контроль соблюдения требований по обеспечению безопасности ПДн (требований законодательства в области защиты ПДн, требований внутренних нормативно-методических и организационно-

распорядительных документов Департамента, сформулированных на основе анализа рисков нарушения безопасности ПДн, договорных требований).

8.3.Оценка эффективности СЗПДн реализуется в виде аттестации или декларирования соответствия требованиям по безопасности ПДн.

Декларирование производится по факту ввода в эксплуатацию ИСПДн. Ввод в эксплуатацию ИСПДн производится в соответствии с документально оформленными требованиями по безопасности ПДн (техническими условиями), разрабатываемыми Департаментом в соответствии с требованиями законодательства и нормативно-методических документов федеральных органов исполнительной власти, осуществляющими функции по контролю и надзору в пределах своих полномочий.

9 ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ СУБЪЕКТА

9.1. Список работников Департамента, имеющих доступ к персональным данным, утверждается приказом начальника Департамента.

9.2. Передача Персональных данных третьим лицам возможна только с согласия субъекта в письменной форме или без его согласия в случаях, предусмотренных законодательством РФ.

10. СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. Система защиты персональных данных (СЗПДн), строится на основании:

- «Отчета о результатах обследования информационной инфраструктуры»;
- «Перечня персональных данных, подлежащих защите»;
- «Актов классификации информационной системы персональных данных»;
- «Модели угроз безопасности персональных данных»;
- Руководящих документов ФСТЭК России и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн. На основании анализа актуальных угроз безопасности ПДн описанного в «Модели угроз безопасности персональных данных», делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн, составляется «План мероприятий по обеспечению защиты ПДн».

10.2. Для каждой ИСПДн разрабатывается «Разрешительная система допуска» с описанием уровня полномочий доступа пользователей к защищаемым ресурсам и «Технический паспорт ИСПДн», в котором отражается технологический процесс обработки персональных данных, перечень используемых технических средств защиты, а так же программного обеспечения участвующего в обработке ПДн, на всех элементах ИСПДн:

- АРМ пользователей;
- Сервера приложений;
- СУБД.

10.3. В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

- антивирусные средства для рабочих станций пользователей и серверов;
- средства управления доступом;
- средства регистрации и учета;
- средства защиты от НСД;

- средства межсетевого экранирования;
- средства анализа защищенности;
- средства обнаружения вторжений;
- средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

Так же в список включаются функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

- управление и разграничение доступа пользователей;
- регистрацию и учет действий с информацией;
- обеспечение целостности данных;
- осуществление обнаружений вторжений;
- осуществления анализа защищенности;
- обеспечение межсетевого экранирования.

Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения вносятся в «Технический паспорт ИСПДн».

10.4. СЗПДн включает в себя следующие подсистемы:

- управления доступом, регистрации и учета;
- обеспечения целостности и доступности;
- антивирусной защиты;
- межсетевого экранирования;
- анализа защищенности;
- обнаружения вторжений;
- криптографической защиты.

10.5. Настройки применяемых средств защиты информации отражаются в «Акте установки и настройки средств защиты». В случае необходимости внесения изменений настроек СЗИ, эти изменения фиксируются в приложении к указанному Акту с указанием даты внесения изменений.

10.6. С целью учета всех средств защиты информации используемых в Центре ведется «Журнал учета СЗИ, эксплуатационной и технической документации к ним»

10.7. Порядок работы со средствами антивирусной защиты отражается в «Инструкции по антивирусной защите».

10.8. Порядок применения средств криптографической защиты информации отражается в «Инструкции о порядке организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

Средства криптографической защиты учитываются в «Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов».

Перечень лиц допущенных к работе с СКЗИ утверждается приказом начальника Департамента.

10.9. Атрибуты доступа к средствам защиты информации и программным компонентам ИСПДн учитываются в «Журнале учета атрибутов доступа». Периодичность их смены отражается в «Инструкции по парольной защите».

10.10. В Департаменте запрещен вывод информации, содержащей персональные данные, на съемные носители информации, ведется учет всех электронных носителей персональных данных в «Журнале учета носителей информации ПДн».

10.11. Мероприятия и действия пользователей в случае возникновения инцидентов, повлекших нарушение целостности информации регламентированы в «Инструкции по резервному копированию и восстановлению».

10.12. Мероприятия по защите информации, содержащей персональные данные, при ее обработке без использования средств вычислительной техники регламентированы в «Порядке неавтоматизированной обработки персональных данных».

11. ТРЕБОВАНИЯ К ПЕРСОНАЛУ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПДН

11.1. Все сотрудники Департамента, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

11.2. При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Сотрудник должен быть ознакомлен под роспись с положениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

11.3. Сотрудники, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а так же возможность их утери или использования третьими лицами. Сотрудники несут персональную ответственность за сохранность идентификаторов.

11.4. Сотрудники должны следовать установленным процедурам поддержания режима безопасности ПДн при использовании паролей (если не используются технические средства аутентификации).

11.5. Сотрудники должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все сотрудники должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

11.6. Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

11.7. Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами Департамента, третьим лицам.

11.8. При работе с ПДн в ИСПДн сотрудники обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

11.9. При завершении работы с ИСПДн сотрудники обязаны защитить АРМ с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

11.10. Сотрудники Департамента должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

11.11. Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему защиту информации.

11.12. В ИСПДн можно выделить следующие группы сотрудников, участвующих в обработке и хранении ПДн:

- Администратора ИСПДн;
- Администратора безопасности;
- Пользователь ИСПДн.

11.13. Должностные обязанности групп сотрудников отражаются в следующих документах:

- «Инструкция администратора ИСПДн»;
- «Инструкция администратора безопасности ИСПДн»;
- «Инструкция пользователя ИСПДн».

12. ПОРЯДОК РАССМОТРЕНИЯ ЗАПРОСОВ СУБЪЕКТВ ПЕРСОНАЛЬНЫХ ДАННЫХ ИЛИ ИХ ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ

12.1. Рассмотрение запросов субъектов персональных данных или их законных представителей осуществляется в порядке предусмотренном «Регламентом рассмотрения запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных».

13. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ СУБЪЕКТА

13.1. Защита прав Субъекта, установленных настоящей Политикой и законодательством Российской Федерации, осуществляется в целях пресечения неправомерного использования персональных данных, восстановления нарушенных прав и возмещения причиненного ущерба, в том числе морального вреда.

13.2. Сотрудники Департамента, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн, персонально несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством РФ.

14. ЗАКЛЮЧИТЕЛЬНОЕ ПОЛОЖЕНИЕ

14.1. Изменения в настоящую Политику могут быть внесены начальником Департамента.

14.2. Настоящая Политика обязательна для соблюдения всеми сотрудниками Департамента.

14.3. Режим конфиденциальности ПДн снимается в случаях их обезличивания, если иное не определено законодательством РФ.

Приложение №2
к приказу от «__»_____ 2015 г. №___

ПОЛОЖЕНИЕ
о порядке обработки и обеспечения безопасности персональных данных Департамента

1. Общие положения

1.1. Настоящим Положением определяются цели, содержание и порядок обработки персональных данных, меры по обеспечению безопасности персональных данных при их обработке в Департаменте, а также их состав.

1.2. Настоящее Положение разработано во исполнение требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановления Правительства Российской Федерации от 1.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и в соответствии с Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

1.3. Действие настоящего Положения не распространяется на отношения, возникающие при:

- организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;
- обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну;

1.4. В настоящем Положении в соответствии со ст. 3 Федерального закона «О персональных данных» используются следующие основные понятия:

- персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
- 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;

- автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

- распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

- предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

- блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

- уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

- обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

- информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

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

1.5. Требования по соблюдению конфиденциальности персональных данных являются обязательными при допуске сотрудников Департамента к работе с персональными данными.

2. Условия обработки персональных данных

2.1. Состав персональных данных и цели обработки персональных данных.

2.1.1. Персональные данные лиц, состоящих с Департаментом в трудовых отношениях, обеспечения сотруднику Департамента установленных законодательством Российской Федерации условий труда, гарантий и компенсаций, сохранности принадлежащего ему имущества и имущества Департамента.

2.1.2. Персональные данные граждан, желающих принять ребёнка в семью, детей из числа детей-сирот.

2.1.3. Персональные данные различных субъектов персональных данных могут обрабатываться в иных целях, указанных в письменном согласии субъекта персональных данных на обработку его персональных данных.

2.2. Объем персональных данных, подлежащих обработке.

2.2.1. В соответствии со статьей 26 Федерального закона от 27.07.2004 N 79-ФЗ «О государственной гражданской службе Российской Федерации» и Указом Президента РФ от 30.05.2005 N 609 "Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении

его личного дела" в личном деле государственного служащего хранятся:

письменное заявление с просьбой о поступлении на гражданскую службу;

собственноручно заполненная и подписанная гражданином Российской Федерации анкета установленной формы с приложением фотографии;

документы о прохождении конкурса на замещение вакантной должности гражданской службы;

копия паспорта и копии свидетельств о государственной регистрации актов гражданского состояния;

копия трудовой книжки или документа, подтверждающего прохождение военной или иной службы;

копии документов об образовании и о квалификации, документов о квалификации, подтверждающих повышение или присвоение квалификации по результатам дополнительного профессионального образования, документов о присвоении ученой степени, ученого звания;

копии решений о награждении государственными наградами Российской Федерации, Почетной грамотой Президента Российской Федерации, об объявлении благодарности Президента Российской Федерации, присвоении почетных, воинских и специальных званий, присуждении государственных премий (если таковые имеются);

копия акта государственного органа о назначении на должность гражданской службы;

экземпляр служебного контракта, а также экземпляры письменных дополнительных соглашений, которыми оформляются изменения и дополнения, внесенные в служебный контракт;

копии актов государственного органа о переводе гражданского служащего на иную должность гражданской службы, о временном замещении им иной должности гражданской службы;

копии документов воинского учета (для военнообязанных и лиц, подлежащих призыву на военную службу);

копия акта государственного органа об освобождении гражданского служащего от замещаемой должности гражданской службы, о прекращении служебного контракта или его приостановлении;

аттестационный лист гражданского служащего, прошедшего аттестацию, и отзыв об исполнении им должностных обязанностей за аттестационный период;

экзаменационный лист гражданского служащего и отзыв об уровне его знаний, навыков и умений (профессиональном уровне) и о возможности присвоения ему классного чина государственной гражданской службы Российской Федерации;

копии документов о присвоении гражданскому служащему классного чина государственной гражданской службы Российской Федерации (иного классного чина, квалификационного разряда, дипломатического ранга);

копии документов о включении гражданского служащего в кадровый резерв, а также об исключении его из кадрового резерва;

копии решений о поощрении гражданского служащего, а также о наложении на него дисциплинарного взыскания до его снятия или отмены;

копии документов о начале служебной проверки, ее результатах, об отстранении гражданского служащего от замещаемой должности гражданской службы;

документы, связанные с оформлением допуска к сведениям, составляющим

государственную или иную охраняемую законом тайну, если исполнение обязанностей по замещаемой должности гражданской службы связано с использованием таких сведений;

сведения о доходах, имуществе и обязательствах имущественного характера гражданского служащего;

копия страхового свидетельства обязательного пенсионного страхования;

копия свидетельства о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации;

копия страхового медицинского полиса обязательного медицинского страхования граждан;

медицинское заключение установленной формы об отсутствии у гражданина заболевания, препятствующего поступлению на гражданскую службу или ее прохождению;

справка о результатах проверки достоверности и полноты представленных гражданским служащим сведений о доходах, имуществе и обязательствах имущественного характера, а также сведений о соблюдении гражданским служащим ограничений, установленных федеральными законами.

2.2.2. В личное дело гражданского служащего вносятся его персональные данные и иные сведения, связанные с поступлением на гражданскую службу, ее прохождением и увольнением с гражданской службы и необходимые для обеспечения деятельности государственного органа. Личное дело гражданского служащего ведется кадровой службой Департамента.

2.2.3. В отделе правового и кадрового обеспечения Департамента создаются и хранятся следующие группы документов, содержащие данные о сотрудниках в единичном или сводном виде:

2.2.4. Документы, содержащие персональные данные работников:

комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении;

комплекс материалов по анкетированию, тестированию, проведению собеседований с кандидатом на должность;

подлинники и копии приказов (распоряжений) по кадрам;

личные дела и трудовые книжки;

дела, содержащие основания к приказу по личному составу;

дела, содержащие материалы аттестаций работников;

дела, содержащие материалы внутренних расследований;

справочно-информационный банк данных по персоналу (картотеки, журналы);

подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Компании, руководителям структурных подразделений;

копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения.

2.2.5. С целью учёта данных о детях, оставшихся без попечения родителей, и гражданах, желающих принять ребенка на воспитание в свою семью и на основании Федерального закона от 16 апреля 2001 г. № 44-ФЗ «О государственном банке данных о детях, оставшихся без попечения родителей» в Департаменте обрабатываются персональные данные граждан, желающих принять детей на воспитание в свои семьи и детей, оставшихся без попечения родителей:

2.2.6. Персональные данные детей, оставшихся без попечения родителей

включают:

– фамилия, имя, отчество;

– фотография;

– дата рождения;

– место рождения;

– дата первичной регистрации ребёнка;

– дата регистрации в муниципальном модуле;

– дата регистрации в региональном модуле;

– орган опеки и попечительства наблюдающий ребенка;

– пол;

– цвет волос;

– цвет глаз;

– гражданство;

– местонахождение ребёнка;

– этническое происхождение;

– свидетельство о рождении (номер, серия, дата выдачи, место выдачи);

– медицинское заключение 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, вес, рост);

– сведения о биологических родителях (ФИО, дата рождения, гражданство, состояние здоровья, местонахождение, принадлежность к определенной религии и культуре, данные из документа удостоверяющего личность биологического родителя);

– возможная форма устройства ребёнка в семью;

– причины отсутствия родительского попечения;

– данные о несовершеннолетних братьях и сёстрах (ФИО, дата рождения, местонахождение, группа здоровья);

– данные о совершеннолетних родственниках (ФИО, дата рождения, степень родства, местонахождение);

– особенности характера, особые приметы, дополнительная информация;

– дополнительная информация органа опеки и попечительства, регионального оператора.

2.2.7. Персональные данные граждан желающих принять ребёнка в семью:

– фамилия, имя, отчество;

– дата рождения;

– место рождения;

– дата заполнения анкеты;

– гражданство;

– данные из документа удостоверяющего личность гражданина (номер, серия, дата выдачи, кем выдан);

– место жительства;

– номер контактного телефона;

– данные из документа «Заключение о возможности быть усыновителем, опекуном (попечителем), приемным родителем» (каким органом опеки и попечительства или контролирующей организацией выдано заключение, номер заключения, дата выдачи заключения, дата постановки на учёт);

– количество детей, которых возможно усыновить;

– ФИО усыновлённых детей;

– пожелание граждан (текстовая информация о ребёнке, которого гражданин желает принять в семью).

2.3. В случаях, предусмотренных п. 2.1.3 настоящего Положения, обрабатываются персональные данные, указанные в письменном согласии субъекта персональных данных на обработку персональных данных, обрабатываются в целях и объемах, указанных в письменном согласии.

3. Согласие субъекта персональных данных

3.1. Письменное согласие на обработку персональных данных субъекта персональных данных, чьи данные обрабатываются в целях, указанных в п. 2.1.1 настоящего Положения, не требуется при обработке персональных данных в соответствующих целях на основании Трудового кодекса Р Ф, в соответствии с п. 2 ч. 1 ст. 6 Федерального закона «О персональных данных», кроме случаев, предусмотренных п. 3.2 настоящего Положения.

3.2. Необходимо получить согласие субъекта персональных данных на обработку его персональных данных:

при передаче персональных данных третьей стороне (за исключением случаев, предусмотренных федеральными законами);

при принятии решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, на основании исключительно автоматизированной обработки его персональных данных.

3.3. Согласие на обработку персональных данных субъекта необходимо получать непосредственно у субъекта персональных данных в любой форме, позволяющей подтвердить факт его получения, если иное не установлено федеральным законом по наступлению условий, при которых такое согласие становится необходимым.

3.4. Типовая форма согласия субъекта персональных данных и представителя субъекта персональных данных приведена в Приложениях №1 к данному Положению.

3.5. Организация сбора и хранения письменных согласий на обработку персональных данных субъектов персональных обрабатываемых в целях, предусмотренных п. 2.1.1 настоящего Положения, возлагается на отдел правового и кадрового обеспечения.

3.6. Организация сбора и хранения письменных согласий на обработку персональных данных субъектов персональных обрабатываемых в целях, предусмотренных п. 2.1.2 настоящего Положения осуществляется вместе с оформление договоров

4. Действия (операции), совершаемые с персональными данными

4.1. Сбор, запись, систематизация, накопление и уточнение персональных данных.

4.1.1. Сбор, запись, систематизация, накопление и уточнение персональных

данных, обрабатываемых в случаях, предусмотренных п. 2.1.1 настоящего Положения, осуществляется путем:

копирования оригиналов документов;

внесения сведений в учётные формы (на бумажных и электронных носителях) и информационные системы персональных данных;

получения оригиналов необходимых документов (трудовая книжка, автобиография, иные документы, предоставляемые в Департамент);

создания персональных данных в ходе кадровой работы.

4.1.2. Сбор, запись, систематизация, накопление и уточнение персональных данных, обрабатываемых в случаях, предусмотренных п. 2.1.2, 2.1.3 настоящего Положения, осуществляется путем получения персональных данных непосредственно от лиц, давших свое согласие на их обработку, в указанных целях или иным образом, указанным в письменном согласии.

4.2. Предоставление и распространение персональных данных осуществляется в соответствии с федеральными законами, на основании которых они обрабатываются, в порядке, предусмотренном разделом 6 настоящего Положения.

4.3. Использование персональных данных осуществляется в соответствии с федеральными законами, на основании которых они обрабатываются.

Возможность использовать персональные данные имеют исключительно сотрудники, допущенные к персональным данным в порядке, предусмотренном разделом 7 настоящего Положения.

4.4. В зависимости от конкретной цели обработки персональных данных также могут совершаться иные действия, предусмотренные федеральными законами, на основании которых они обрабатываются.

5. Лица, ответственные за организацию обработки персональных данных

5.1. Лицо, ответственное за организацию обработки персональных данных в Департаменте, назначается приказом начальника Департамента.

5.2. В должностные обязанности лица, ответственного за защиту персональных данных, в частности, входит:

осуществление внутреннего контроля за соблюдением сотрудниками Департамента законодательства Российской Федерации о персональных данных и требований по защите персональных данных;

организация мероприятий направленных на выполнение требований законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

организация мероприятий по повышению осведомленности сотрудников Департамента в сфере соблюдения прав субъектов персональных данных и обеспечения безопасности персональных данных (в том числе ознакомление с настоящим Положением);

контроль за приемом и обработкой обращений и запросов субъектов персональных данных или их представителей;

контроль подготовки и организация направления в адрес уполномоченного органа по защите прав субъектов персональных данных уведомления о намерении и (или) об обработке персональных данных по установленной форме, а также

своевременное уведомление об изменении условий обработки.

6. Организация хранения персональных данных

6.1. Персональные данные хранятся на бумажных носителях и в электронном виде в информационных системах персональных данных в структурных подразделениях Департамента, в функции которых входит обработка персональных данных в соответствии с положениями об этих подразделениях.

6.2. Сроки хранения персональных данных на бумажных носителях определяются нормативно-правовыми актами, регламентирующими порядок их сбора и обработки.

6.3. Срок хранения персональных данных на электронных носителях должен соответствовать сроку хранения бумажных оригиналов.

6.4. При хранении персональных данных на электронных носителях обеспечивается регулярное резервное копирование информации с целью недопущения потери персональных данных при выходе из строя носителей персональных данных.

6.5. При хранении материальных носителей персональных данных должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним. Перечень мер, необходимых для обеспечения таких условий, определяется организационно-распорядительными документами Департамента, регламентирующими защиту информации.

6.6. Необходимо обеспечивать раздельное хранение персональных данных (на разных материальных носителях), обработка которых осуществляется в различных целях, определенных настоящим Положением, без использования средств вычислительной техники (без использования средств автоматизации).

6.7. За хранением и использованием носителей персональных данных устанавливается контроль, не допускающий несанкционированное использование, уточнение, распространение и уничтожение персональных данных, находящихся на этих носителях.

6.8. Корректировка, уточнение персональных данных при осуществлении их обработки без использования средств вычислительной техники (без использования средств автоматизации) может производиться путем обновления (в том числе частичного) или изменения данных на материальном носителе. Если это не допускается техническими особенностями материального носителя — путем фиксации на том же материальном носителе сведений об изменениях, вносимых в персональные данные, либо путем изготовления нового материального носителя с уточненными персональными данными.

6.9. Уничтожение по окончании срока обработки персональных данных на электронных носителях производится путем механического нарушения целостности носителя, не позволяющего произвести считывание персональных данных, или методами и средствами гарантированного удаления остаточной информации.

6.10. Отчуждаемые носители электронной информации, содержащей персональные данные, в Департаменте не используются. Вывод информации на отчуждаемые электронные носители не производится.

6.11. Вывод на печать документов, содержащих персональные данные, допускается в связи с исполнением служебных обязанностей, в том числе в целях

передачи печатных копий субъектам персональных данных либо лицам, допущенным в соответствии с п. 7.1 настоящего Положения, к ознакомлению с передаваемыми персональными данными.

6.12. Все базы данных информации, содержащей персональные данные граждан РФ, размещены в России.

7. Доступ к персональным данным

7.1. Доступ к персональным данным имеет ограниченный круг сотрудников Департамента, перечень которых утверждается начальником Департамента.

7.2. Сотрудники, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

7.3. Лица, допущенные к обработке персональных данных, подписывают соглашение о неразглашении (Приложение №2).

7.3. Лица, допущенные к обработке персональных данных, должны быть проинформированы о факте обработки ими персональных данных, характере обработки, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных настоящим Положением.

7.4. При осуществлении доступа к персональным данным, обрабатываемым в автоматизированных системах персональных данных, должна применяться система разграничения прав доступа на основе утвержденных администратором безопасности правил разграничения доступа к информации, обрабатываемой в автоматизированной системе.

7.5. При осуществлении доступа к персональным данным, обрабатываемым в автоматизированных системах персональных данных, должна применяться система регистрации и учета всех действий, совершаемых с персональными данными. Работы по администрированию такой системы и анализ регистрационной информации возлагается на администратора безопасности. Об инцидентах, связанных с попытками нарушения правил разграничения доступа и несанкционированным доступом, докладывается лицу, ответственному за организацию обработки персональных данных. Срок хранения регистрационной информации должен составлять не менее 10 дней.

8. Порядок предоставления персональных данных

8.1. Не допускается предоставление баз, банков данных, списков, содержащих персональные данные, государственному органу, его территориальному органу, органу местного самоуправления или организации, подведомственной государственному органу, органу местного самоуправления, а также физическому или юридическому лицу, за исключением случаев, предусмотренных федеральными законами.

8.2. Передача персональных данных, в том числе в целях обеспечения общественного интереса, на договорной основе допускается в рамках соглашения (договора) об информационном обмене между контрагентом и Департаментом при соблюдении следующих условий:

в соглашении (договоре) указаны обязательства сторон по соблюдению конфиденциальности и обеспечению заданного уровня безопасности персональных данных;

соглашением (договором) определены цели, порядок и условия передачи персональных данных в соответствии с федеральными законами и настоящим положением;

имеется согласие субъекта персональных данных на передачу персональных данных.

8.3 Департамент передает персональные данные государственному органу, его территориального органу, органу местного самоуправления или организации, подведомственной государственному органу, органу местного самоуправления, а также физическому или юридическому лицу на основании запроса о предоставлении персональных данных (далее — запрос).

8.4. Запрос оформляется в письменном виде на бланках и направляется фельдсвязью, почтовыми отправлениями, с нарочными или в электронном виде по информационно-телекоммуникационным сетям с реквизитами, позволяющими идентифицировать факт обращения в Департамент.

8.7. Запрос должен быть подписан уполномоченным должностным лицом, содержать указание цели и правового основания затребования персональных данных и срок предоставления этой информации, если иное не установлено федеральными законами.

8.8. При направлении запроса по информационно-телекоммуникационным сетям, стандарт, формат и процедуру информационного взаимодействия с контрагентом определяет Департамент в соответствии с действующим законодательством. Подпись должностного лица подтверждается квалифицированной электронной подписью.

8.9. Запрос физического лица о предоставлении персональных данных оформляется на листе бумаги с указанием фамилии, имени, отчества, реквизитов документа, удостоверяющего личность, места жительства или места пребывания и направляется почтовыми отправлениями, с нарочными или доставляется лично.

8.10. Основанием для рассмотрения запроса в Департаменте является ссылка на положение федерального закона, устанавливающее право обратившегося государственного органа, его территориального органа, органа местного самоуправления или организации, подведомственной государственному органу, органу местного самоуправления, а также физического или юридического лица на получение персональных данных или заключение договора (соглашения) об информационном взаимодействии с Департаментом.

8.11. Обоснованием (мотивом) запроса является конкретная цель, связанная с реализацией гражданином своих прав или исполнением субъектом обращения определенных федеральным законом обязанностей, для достижения которых ему необходимо использовать запрашиваемые персональные данные. Запросы, по форме и содержанию не отвечающие требованиям п.п. 8.6.- 8.10. настоящего Положения, исполнению не подлежат.

9. Порядок обследования информационных систем персональных данных и учета персональных данных

9.1. В целях определения исходных данных и полного учета информационных систем персональных данных проводится общее обследование информационных систем персональных данных на объекте информатизации.

9.2. Лица, проводящие обследование, допускаются непосредственно к ознакомлению с персональными данными исключительно в рамках своих полномочий, определенных настоящим Положением.

9.3. Обследованию подлежат помещения, в которых ведется обработка информации.

9.4. В ходе обследования проводится опрос сотрудников структурного подразделения, осмотр рабочих мест и изучение рабочего процесса отдельного работника и подразделения в целом.

9.5. Анализ исходных данных заключается в изучении перечня персональных данных, идентификации отдельных информационных систем персональных данных, выявлении фактов обработки персональных данных в неустановленных целях, в неустановленных объемах и режимах.

9.6. По результатам анализа данных обследования утверждаются перечни персональных данных и информационных систем персональных данных.

9.7. Перечни подлежат актуализации по мере перемещения информационных ресурсов, содержащих персональные данные, изменения характера обработки персональных данных в информационных системах персональных данных, появления новых информационных систем персональных данных.

10. Организация защиты персональных данных при их обработке без использования средств вычислительной техники

10.1. Обработка персональных данных без использования средств вычислительной техники (без использования средств автоматизации) осуществляется сотрудниками Департамента в соответствии с Порядком неавтоматизированной обработки персональных данных в Департаменте.

10.2. Печатная копия документа, созданная в целях передачи определенному субъекту, не должна содержать персональные данные других субъектов, за исключением случаев, определенных действующим законодательством.

10.3. Запрещается использовать печатные копии документов, содержащих персональные данные, для повторной печати (в качестве черновиков).

10.4. Типовые формы документов, характер информации в которых предполагает или допускает включение в них персональных данных, утверждаются в Департаменте с соблюдением условий, предусмотренных п. 7 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15.09.2008 № 687.

11. Меры по обеспечению безопасности персональных данных

11.1 Меры по обеспечению безопасности персональных данных должны обеспечить надлежащий уровень безопасности с учетом соразмерности затрат на их реализацию и опасности угроз, обусловленных природой защищаемых данных и условиями их обработки.

11.2 Работы по обеспечению безопасности персональных данных являются цикличными и включают в себя следующие этапы.

11.2.1 Определение угроз безопасности персональных данных.

Департамент определяет угрозы безопасности персональных данных с составлением модели угроз — документа, описывающего актуальные угрозы безопасности персональных данных, обрабатываемых в информационных системах. В модели угроз должны учитываться как прямые, так и косвенные угрозы.

Модель угроз разрабатываться подразделением, ответственным за обеспечение безопасности, в соответствии с нормативными документами, государственными стандартами, а также методическими рекомендациями ФСТЭК России и ФСБ России.

Актуальность угрозы определяется путем анализа совокупности опасности, уязвимостей информационной системы персональных данных, вероятности реализации и категории потенциального нарушителя, инициирующего угрозу.

11.2.2. Деятельность по обработке угроз (устранение уязвимостей).

Обработка угроз заключается в применении организационных и технических мер, направленных на снижение вероятностей и возможностей реализации угрозы. Также на этом этапе принимаются организационные и технические меры, необходимые для обеспечения установленного правительством Российской Федерации уровня защищенности персональных данных.

11.2.3. Выбор и реализация методов и способов защиты персональных данных.

Выбор методов и способов защиты информации для обеспечения необходимого уровня защищенности осуществляется в соответствии с требованиями ФСТЭК России и ФСБ России.

11.2.4. Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных и контроль за принимаемыми мерами по обеспечению безопасности персональных данных.

До ввода в эксплуатацию информационной системы персональных данных лицом, ответственным за организацию обработки персональных данных в Департаменте, организуются мероприятия по оценке и дается заключение об эффективности принимаемых мер по обеспечению безопасности персональных данных. В дальнейшем оценка проводится в рамках контроля за принимаемыми мерами не реже одного раза в 3 года.

12. Заключительные положения

12.1. При создании новых баз данных, реестров, таблиц, анкет, книг, журналов, предусматривающих занесение в них персональных данных, их использование согласуется лицом, ответственным за организацию обработки персональных данных в Департаменте.

12.2. При создании новых информационных систем персональных данных, изменении состава, порядка и целей обработки персональных данных, лицо, ответственное организацию обработки персональных данных в Департаменте, инициирует внесение изменений в уведомление уполномоченного органа по защите прав субъектов персональных данных об обработке персональных данных в Департаменте.

12.3. Руководители структурных подразделений, в котором обрабатываются персональные данные, осуществляют контроль за соблюдением правил

разграничения доступа к персональным данным и требований по обеспечению конфиденциальности персональных данных в рамках своих полномочий.

12.4. Сотрудники Департамента, допущенные в установленном порядке к обработке персональных данных, несут персональную ответственность за нарушения требований по обработке персональных данных в соответствии со ст. 24 Федерального закона «О персональных данных».

12.5. Методическое руководство по выполнению предусмотренных мер защиты персональных данных возлагается на ответственного за организацию обработки персональных данных в Департаменте.

12.6. Контроль за выполнением предусмотренных мер защиты персональных данных возлагается на лиц, ответственных за защиту персональных данных в Департаменте.

Приложение №1

Форма утверждена постановлением Администрации Смоленской области от 15.09.2009 № 547 «Об утверждении Положения о порядке обработки персональных данных в органах исполнительной власти Смоленской области и подведомственных им учреждениях»

СОГЛАСИЕ
на обработку персональных данных

г. Смоленск «___» _____ __ г.

Я, _____
(Ф.И.О)

паспорт серия _____ № _____ выдан _____
(вид документа, удостоверяющего личность) (когда и кем выдан)

_____,

проживающий (ая) по адресу: _____

_____,

настоящим даю свое согласие на обработку **Департаменту Смоленской области по образованию, науке и делам молодежи**
(наименование и адрес оператора (органа исполнительной власти Смоленской области, областного государственного учреждения))

моих персональных данных и подтверждаю, что, давая такое согласие, я действую своей волей и в своих интересах.

Согласие дается мною для целей: **исполнение обязанностей работодателя перед своими сотрудниками**
(цель обработки персональных данных)

и распространяется на следующую информацию: **фамилия, имя, отчество, год, месяц, дата и**
(перечень персональных данных)

место рождения, адрес, образование, профессия, сведения о составе семьи, перемене фамилии, наличии детей и иждивенцев, номер пенсионного страхового свидетельства, идентификационный номер о постановке на учет физического лица в налоговом органе на территории Российской Федерации, номера зарплатных карт

Настоящее согласие предоставляется на осуществление любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных выше целей, включая (без ограничения) сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), блокирование, уничтожение, а также осуществление любых иных действий с моими персональными данными с учетом федерального законодательства.

В случае неправомерного использования предоставленных мною персональных данных согласие отзывается моим письменным заявлением.

Данное согласие действует с **« »** **г.** по _____.

_____ _____
(подпись лица, давшего согласие на обработку ПДн) (расшифровка фамилии)

Приложение №2

(Форма)

ОБЯЗАТЕЛЬСТВО

о неразглашении информации, содержащей персональные данные

Я,_____ ,
(Ф.И.О.)
исполняющий (ая) должностные обязанности по

_____

_____ ,
(должность, наименование структурного подразделения)

предупрежден (а) о том, что на период исполнения должностных обязанностей мне будет предоставлен допуск к информации, содержащей персональные данные. Настоящим добровольно принимаю на себя обязательства:

1. Не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.

2. В случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать непосредственному начальнику.

3. Не использовать информацию, содержащую персональные данные, с целью получения выгоды.

4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.

5. В течение года после прекращения права на допуск к информации, содержащей персональные данные, не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

Я предупрежден (а) о том, что в случае нарушения данного обязательства буду привлечен (а) к дисциплинарной ответственности и/или иной ответственности в соответствии с законодательством Российской Федерации.

_____ _____
(фамилия, инициалы) (подпись)

«_____»_____ ____г.

Приложение №3
к приказу
от «__» _____ 2015 г. №___

Порядок
неавтоматизированной обработки персональных данных
в Департаменте

1. Настоящий Порядок разработан в соответствии с Положением об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15.09.2008 № 687.

2. Настоящей Порядок распространяется на всех сотрудников Департамента, осуществляющих обработку персональных данных без использования средств автоматизации.

3. Обработка персональных данных без использования средств автоматизации (далее – неавтоматизированная обработка персональных данных) осуществляется в виде документов на бумажных носителях.

4. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами.

5. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

6. При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;

- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;

- дела с документами, содержащими персональные данные, должны иметь внутренние описи;

7. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень

действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

8. Документы, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность. Ключи от шкафов (сейфов) нумеруются и выдаются сотрудникам под расписку. Дубликат ключей хранится в сейфе у руководителя организации. Печати нумеруются, учитываются и выдаются сотрудникам под расписку.

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

10. В случае невозможности уничтожения части персональных данных, уничтожению подлежит носитель, содержащий персональные данные.

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

12. Запрещается:

- передавать документы лицам, недопущенным к обработке персональных данных.

- хранить документы с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам.

- выносить документы с персональными данными из служебных помещений для работы с ними на дому и т.д.

- осуществлять обработку персональных в присутствии посторонних лиц.

Лист ознакомления: