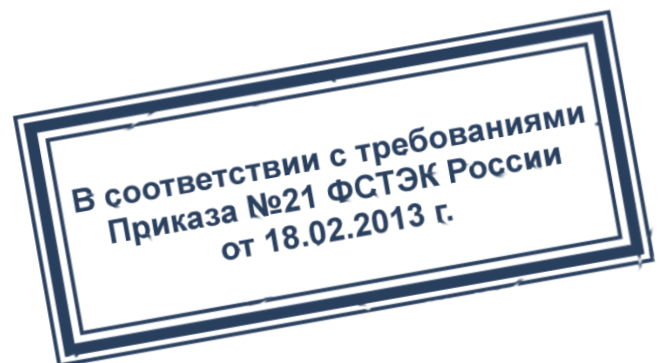


ПОРЯДОК
проведения работ по приведению процессов обработки и
защиты персональных данных в соответствии требованиям
№ 152-ФЗ «О персональных данных»





Оглавление

1.	Введение	4
2.	Цели и задачи работ.....	5
3.	Этапы проведения работ	5
3.1.	Анализ автоматизированной и неавтоматизированной обработки ПДн	6
3.2.	Разработка нормативной и организационно-распорядительной документации	8
3.3.	Определение требований к СЗПДн.....	9
3.4.	Разработка ТП на создание (модернизацию) СЗПДн.....	13
3.5.	Реализация технических и организационных мероприятий по приведению порядка защиты ПДн в соответствие требованиям действующего законодательства.....	15
3.6.	Подготовка ИСПДн к аттестации	15
3.7.	Организация и проведение аттестации на соответствие ИСПДн требованиям по защите информации.....	16
4.	Общая характеристика работ.....	17
	Приложение 1.....	19
	Приложение 2.....	20



Перечень сокращений

ДЛ – должностное лицо

ИБ - информационная безопасность

ИСПДн - информационная система персональных данных

ПДн – персональные данные

СЗПДн - система защиты персональных данных

СМИБ - система менеджмента информационной безопасности

СИБ - система информационной безопасности

ТЗ - техническое задание

ТП - технический проект



1. Введение

Настоящий документ содержит описание методологии и содержание этапов проведения работ по приведению процессов обработки персональных данных (далее – ПДн) в соответствие требованиям действующего законодательства РФ.

Реализация комплекса организационно-технических мероприятий при обработке ПДн различных субъектов (сотрудников, клиентов и пр.) является обязательной в силу требований Федерального закона РФ от 27 июля 2006 г. №152-ФЗ "О персональных данных", Постановления Правительства РФ от 1 ноября 2012 г. №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", Постановления Правительства РФ от 15 сентября 2008 г. №687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", Постановления Правительства РФ от 06 июля 2008 г. №512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных".

Проверки соблюдения обязательных требований в сфере обработки ПДн

Согласно отчету Роскомнадзора за 2012 год, регулятором были рассмотрены 5677 обращений физических и юридических лиц с целью защиты интересов в сфере персональных данных, что на 31 % больше, чем в 2011 году. Были проведены 874 плановые и 663 внеплановые проверки. При этом операторам персональных данных выдано 1370 предписаний об устранении выявленных нарушений, составлено и направлено на рассмотрение в суды 5359 протоколов о нарушении норм КоАП.



Данными документами установлены правила в отношении обработки и обеспечения безопасности ПДн, выполнение которых носит обязательный характер. Кроме того, регуляторами изданы и вступили в силу нормативные правовые акты и иные руководящие документы, регламентирующие порядок технической защиты ПДн.

Невыполнение требований нормативных правовых актов по вопросам обработки и защиты ПДн может грозить:

- предупреждением или наложением административного штрафа (КоАП РФ, статьи 13.11, 13.14, 5.39);
- приостановлением или прекращением обработки персональных данных в организации (№152-ФЗ, статья 23, п.4);
- гражданскими исками со стороны субъектов персональных данных (№152-ФЗ, Статья 23, п.5);
- приостановлением действия или аннулированием лицензии на ведение основных видов деятельности (№152-ФЗ, статья. 23, п.6);
- привлечением организации и (или) ее руководителя к административной, уголовной, гражданской, дисциплинарной и иным



видам ответственности (№152-ФЗ, статьи 23, п.7, п.9; УК РФ, статьи 137,140, 272).

2. Цели и задачи работ

Выполнение работ по приведению процессов обработки ПДн в соответствие действующим требованиям законодательства в сфере обработки и защиты ПДн, имеет своей целью максимальную адаптацию бизнес-процессов, в рамках которых осуществляется автоматизированная и неавтоматизированная обработка ПДн различных категорий субъектов, к данным требованиям с наименьшими затратами.

Реализация работ по приведению процессов обработки ПДн в соответствие действующим требованиям законодательства в сфере обработки и защиты ПДн (далее – Работы) позволит:

- определить текущую степень соответствия процессов обработки и защиты ПДн действующим требованиям законодательства;
- определить перечень мероприятий и ресурсов, необходимых для приведения процессов обработки и защиты ПДн в соответствие действующим требованиям законодательства;
- реализовать необходимые технические и организационные меры по приведению процессов обработки и защиты ПДн в соответствие действующим требованиям законодательства;
- подготовить необходимые регламентирующие и организационно-распорядительные документы;
- подтвердить соответствие ИСПДн требованиям по защите информации для соответствующего уровня защищенности.

3. Этапы проведения работ

Реализация работ по приведению процессов обработки и защиты ПДн в соответствие действующим требованиям законодательства РФ осуществляется в несколько этапов:

Этап 1. Анализ автоматизированной и неавтоматизированной обработки ПДн.

Этап 2. Разработка нормативной и организационно-распорядительной документации.

Этап 3. Разработка модели угроз и нарушителя информационной безопасности. Определение необходимого уровня защищенности. Определение требований к СЗПДн. Разработка ТЗ на создание (модернизацию) СЗПДн.

Этап 4. Разработка ТП на создание (модернизацию) СЗПДн.

Этап 5. Реализация технических и организационных мероприятий по приведению процессов обработки и защиты ПДн в соответствие требованиям действующего законодательства.



Этап 6*. Подготовка ИСПДн к аттестации.

Этап 7*. Организация и проведение аттестации соответствия ИСПДн требованиям по защите информации.

3.1. Анализ автоматизированной и неавтоматизированной обработки ПДн

Цель этапа:

Сбор исходных данных для дальнейшего проведения Работ.

На данном этапе выполняются следующие работы:

1. Анализ технологических и бизнес-процессов Заказчика:

- анализ организационно-штатной структуры Заказчика;
- выделение бизнес-процессов, связанных с обработкой ПДн;
- определение состава ПДн, обрабатываемых Заказчиком, оснований, целей и сроков их обработки;
- анализ порядка реагирования на запросы субъектов ПДн.

2. Анализ нормативной и организационно-распорядительной документации Заказчика, регламентирующей порядок и правила обработки и защиты ПДн:

- анализ имеющихся концепций, политик, регламентов, инструкций и иной документации в области обработки и защиты ПДн;
- изучение степени вовлеченности сотрудников в процессы обеспечения ИБ ПДн, в том числе распределения обязанностей и ответственности за обеспечение ИБ ПДн (наличие подразделения по защите информации, администраторов безопасности информации и прочих ответственных лиц).

3. Анализ информационных систем Заказчика:

- изучение и анализ топологии информационных систем;
- анализ применяемого серверного и сетевого оборудования;
- анализ перечня используемых программных средств (в том числе на рабочих местах);

Формирование плана работ и предварительная оценка затрат

В целях формирования плана работ по приведению Вашего предприятия или организации к соответствию требованиям 152-ФЗ «О персональных данных» Вы можете воспользоваться результатами экспресс-оценки, которая формируется специалистами КонсалтИнфоМенеджмент на основании заполненной Вами специальной анкеты. Анкету для формирования экспресс-оценки Вы можете получить, обратившись к нашим специалистам.



* Подтверждение соответствия ИСПДн требованиям по защите информации в форме аттестации ИСПДн (этапы 6 и 7) для коммерческих организаций не является обязательным. Однако следует учесть, что в таком случае организации необходимо провести подтверждение соответствия ИСПДн в иной форме, что значительно снижает уровень доверия к подобным системам.



- анализ используемых средств защиты информации.

В результате:

1. Определяются и оцениваются на предмет соответствия действующим требованиям:

- наличие и состав уведомления об обработке ПДн уполномоченного органа;
- цели, состав и основания обработки ПДн Заказчиком;
- процедуры обработки ПДн работниками Заказчика (в том числе, процедуры сбора, хранения, передачи третьей стороне, уничтожения и др.);
- порядок организации учета, хранения и обращения электронных и бумажных носителей персональных данных;
- типовые формы документов, содержащих ПДн, в том числе обрабатываемых без использования средств автоматизации;
- порядок реагирования должностных лиц на запросы субъектов ПДн;
- порядок проведения проверок по фактам нарушения требований при обработке ПДн.

2. Выделяются ИСПДн, по каждой из которых определяются:

- перечень обрабатываемых ПДн, категории субъектов ПДн, цели обработки ПДн;
- источники и способы поступления ПДн в ИСПДн и правовое основание для последующей обработки;
- перечень действий, производимых с ПДн;
- режим обработки ПДн в ИСПДн и ее отдельных компонентах;
- сроки обработки ПДн и/или условия прекращения обработки ПДн;
- описание конфигурации и топологии ИСПДн в целом и ее отдельных компонентов, в том числе перечень технических и программных средств, участвующих в обработке ПДн;
- условия расположения ИСПДн (в том числе относительно границ контролируемой зоны), техническое и информационное взаимодействие с другими информационными системами.

3. Формируются рекомендации по:

- доработке и внесению изменений в нормативные и организационно-распорядительные документы;
- доработке и внесению изменений в должностные обязанности (положения о структурных подразделениях, трудовые договора) работников, участвующих в реализации бизнес-процессов, в рамках которых обрабатываются ПДн;
- распределению обязанностей и ответственности за организацию обработки и защиты ПДн между работниками (назначение ответственных должностных лиц, реструктуризации существующих подразделений по ИБ);



- реализации корпоративной политики унификации защищаемых АРМ (использования унифицированных технических средств);
- доработке корпоративной политики ИБ в аспектах обеспечения ИБ ПДн;
- реализации разрешительной системы допуска сотрудников к обработке ПДн (формирование соответствующих списков, выделение и защита помещений);
- организации и проведению работ по обеспечению безопасности ПДн при их обработке в ИСПДн;
- реализации системы проведения проверок по фактам нарушения требований по обработке ПДн и реагирования на инциденты ИБ;
- модификации существующих информационных систем Заказчика в целях реализации мероприятий по обеспечению ИБ ПДн.

3.2. Разработка нормативной и организационно-распорядительной документации

Цель этапа:

На основании исходных данных, полученных в ходе реализации 1-го этапа Работ, разработать проекты нормативных документов, регламентирующих порядок, правила обработки ПДн, обеспечения их ИБ и предложения по их интеграции в существующие бизнес-процессы.

На данном этапе выполняются следующие работы:

1. Разработка проектов нормативных, организационно-распорядительных документов:

- Разработка проектов нормативных и организационно-распорядительных документов осуществляется в соответствии с рекомендациями, полученными в ходе проведения 1-го этапа Работ.
- Создание системы распределения обязанностей и ответственности за обеспечение ИБ ПДн с учетом организационно-штатной структуры Заказчика.

2. Ввод в действие и интеграция разработанных документов в существующие бизнес-процессы Заказчика.

Консалтинг по вводу в действие документов в области обработки ПДн и ознакомление работников Заказчика с ними.

В результате:

1. Формируется комплект документов по обработке и защите ПДн, содержащий процедуры, необходимые для обеспечения соответствия требованиям законодательства. Типовой перечень разрабатываемой в рамках данного этапа документации приведен в Приложении 2.

2. Бизнес-процессы Заказчика модернизируются с учетом требований законодательства в сфере обработки и защиты ПДн.



3.3. Определение требований к СЗПДн

Цель этапа:

- На основании исходных данных, полученных в ходе проведения 1-го этапа Работ, разработать модель угроз и нарушителя информационной безопасности, определить необходимый уровень защищенности ИСПДн и набор мер по обеспечению безопасности ПДн при их обработке в ИСПДн.
- Разработать ТЗ на создание системы защиты ИСПДн.

Описание работ:

В общем виде схема проведения работ по определению требований к СЗПДн и разработки Технического задания представлена на Рисунке 1.



Рисунок 1

На данном этапе выполняются следующие работы:

1. Разработка модели угроз и нарушителя ИБ

1.1. Анализ имеющихся в распоряжении мер и средств защиты ПДн:

- от утечки по техническим каналам утечки информации;
- от несанкционированного доступа к информации, в том числе физического доступа (внешний, внутренний нарушитель);
- от программно-математических воздействий;
- анализ организационных мероприятий.

1.2. Формирование модели угроз ИБ ПДн:

- оценку возможности физического доступа к ИСПДн;
- выявление возможных технических каналов утечки информации;
- анализ возможностей программно-математического воздействия на ИСПДн;
- определение актуальности угроз НДВ системного и прикладного ПО;
- оценка ущерба от реализации угроз;



Порядок проведения работ по приведению процессов обработки и защиты персональных данных в соответствие требованиям № 152-ФЗ «О персональных данных»

- определение степени базовой защищенности ИСПДн;
- определение частоты реализации и опасности угроз ИБ ПДн;
- определение актуальности угроз ИБ ПДн.

1.3. Формирование модели нарушителя ИБ ПДн, с учетом:

- характера нарушителя;
- квалификации нарушителя;
- технической оснащенности нарушителя;
- уровня возможностей (используемым методам и средствам);
- времени действия;
- места действия/воздействия.

1.4. Формирование частных моделей угроз и нарушителя исходя из реальных условий расположения, функциональных и технологических связей конкретных ИСПДн (сегментов, обособленных частей).

Общий порядок проведения работ по разработке модели угроз и нарушителя представлен на Рисунке 2.



Рисунок 2

2. Определение необходимого уровня защищенности ПДн при их обработке в ИСПДн (сегментах, обособленных частях ИСПДн) и мер по защите ПДн.

Определение необходимого уровня защищенности осуществляется в соответствии с Постановлением Правительства РФ от 1 ноября 2012 г. №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

В зависимости от результатов моделирования угроз, категории субъектов ПДн (работники Оператора персональных данных, субъекты, не



являющиеся работниками Оператора персональных данных), категории обрабатываемых ПДн (специальные, биометрические, иные) и количества субъектов ПДн определяется необходимый уровень защищенности ПДн при их обработке в соответствующей ИСПДн.

Результаты проведенных работ оформляются «Актом определения необходимого уровня защищенности ПДн при их обработке в ИСПДн».

Общий порядок проведения работ по определению необходимого уровня защищенности ПДн при их обработке в ИСПДн представлен на Рисунке 3.

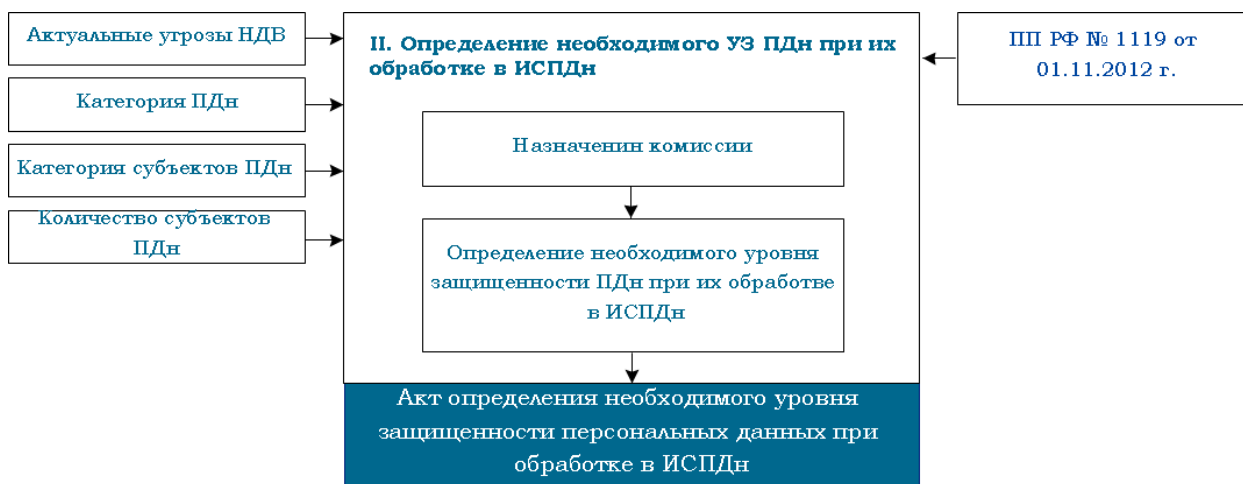


Рисунок 3

3. Определение организационных и технических мер по защите ПДн и разработка ТЗ на создание (модернизацию) СЗПДн.

Определение необходимых мер по обеспечению безопасности ПДн для соответствующего уровня защищенности осуществляется согласно Приказу ФСТЭК №21 от 18 февраля 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. При этом:

1) Для каждой ИСПДн в соответствии с приложением к Приказу ФСТЭК №21 определяется базовый набор организационных и технических мер по обеспечению безопасности ПДн.

2) Базовый набор мер адаптируется с учетом особенностей конкретной информационной системы, в частности, исключаются меры:

- а) связанные с неиспользуемыми технологиями или структурно-функциональными характеристиками, несвойственными конкретной информационной системе;
- б) нереализуемые в рамках конкретной информационной системы;
- в) реализация которых в рамках конкретной информационной системы экономически нецелесообразна.



Порядок проведения работ по приведению процессов обработки и защиты персональных данных в соответствие требованиям № 152-ФЗ «О персональных данных»

3) Адаптированный базовый набор мер уточняется с помощью компенсирующих мер, обеспечивающих нейтрализацию актуальных угроз безопасности ПДн.

4) Уточненный адаптированный базовый набор мер дополняется мерами, обеспечивающими выполнение требований к защите персональных данных, установленными иными нормативными правовыми актами в области обеспечения безопасности персональных данных и защиты информации.

По результатам проведенных работ разрабатывается «Протокол определения организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн».

Общий порядок проведения работ по определению перечня необходимых технических и организационных мер представлен на Рисунке 4.



Рисунок 4

На основе требований, определенных «Протоколом определения организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн», разрабатывается ТЗ на создание (модернизацию) СЗПДн с учетом требований ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы», ГОСТ Р 51624-2000 «Автоматизированные системы в защищенном исполнении. Общие положения» и др. В общем виде ТЗ включает:



- общие сведения (включая оценку соответствия текущих мер и средств защиты ИСПДн требованиям нормативных документов Регуляторов);
- назначение и цели выполнения работ;
- требования к составу и содержанию работ;
- порядок контроля и приемки работ;
- требования к документированию;
- порядок проведения работ.

При необходимости разрабатываются частные ТЗ аналогичной структуры на создание (модернизацию) СЗПДн отдельных ИСПДн.

В результате:

- 1. Для каждой ИСПДн формируются (совершенствуются) модели угроз и нарушителей ИБ ПДн.***
- 2. Определяются необходимые уровни защищенности ПДн при их обработке в ИСПДн.***
- 3. Для каждой ИСПДн определяются технические и организационные меры по защите ПДн.***
- 4. Осуществляется разработка ТЗ на создание (модернизацию) СЗПДн.***

3.4. Разработка ТП на создание (модернизацию) СЗПДн

Цель этапа:

Разработка ТП на создание (модернизацию) СЗПДн в соответствии с ТЗ.

На данном этапе выполняются следующие работы:

- 1. Разработка ТП на создание (модернизацию) СЗПДн в соответствии с ТЗ.***

Порядок оформления и предъявления Заказчику результатов работ по созданию (модернизации) СЗПДн соответствует требованиям комплекса стандартов и руководящих документов на автоматизированные системы и представляется в виде пояснительной записки, с учетом требований:

- ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.
- ГОСТ 34.201-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначения документов при создании автоматизированных систем.



Порядок проведения работ по приведению процессов обработки и защиты персональных данных в соответствие требованиям № 152-ФЗ «О персональных данных»

- ГОСТ 34.601-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы стадии создания.
- ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.
- РД 50-682-89 Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Общие положения.
- РД 50-680-88 Методические указания. Автоматизированные системы. Основные положения.
- РД 50-34.698-90 Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов.
- ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.
- ГОСТ Р 51624-2000 «Автоматизированные системы в защищенном исполнении. Общие положения»

Технический проект на создание (модернизацию) СЗПДн включает в себя:

- ведомость технического проекта;
- ведомость покупных изделий;
- пояснительную записку;
- описание комплекса технических средств.

В результате:

Разрабатывается ТП на создание (модернизацию) СЗПДн в соответствии с требованиями ТЗ.



Стендовые испытания и макетирование СЗПДн

По согласованию с Заказчиком, на стадии технического проектирования могут быть организованы стендовые испытания СЗПДн (ее отдельных компонентов) по разрабатываемой и согласовываемой для этих целей программе.

Стендовые испытания рассматриваются в качестве заключительной фазы процесса разработки и проектирования СЗПДн, характеризующейся возможностью получения доказательств корректности функционирования механизмов защиты и обработки информации в условиях определенной среды функционирования и аппаратного стенда, и соответствия проектируемой СЗПДн установленным требованиям.



3.5. Реализация технических и организационных мероприятий по приведению порядка защиты ПДн в соответствие требованиям действующего законодательства

Цель этапа:

Реализация технических и организационных мероприятий по защите ИСПДн.

На данном этапе выполняются следующие работы:

1. Поставка, пуско-наладка и специальная настройка дополнительных технических средств обработки, передачи и хранения информации в ИСПДн.*

2. Поставка, пуско-наладка и специальная настройка сертифицированных (аппаратных/программных/программно-аппаратных) средств защиты информации.*

3. Реализация разрешительной системы доступа должностных лиц и сотрудников Заказчика к ПДн.

4. Реализация комплекса мероприятий (формирование рекомендаций) по организации охраны и физической защите помещений и технических средств ИСПДн (при необходимости).

5. Опытная эксплуатация внедренной СЗПДн.

6. Утверждение и введение в действие нормативной и организационной структуры СМИБ (ввод в действие документации, реорганизация организационно-штатной структуры Заказчика), разработанной на 2-м этапе.

В результате:

7. Внедряются проектные решения, разработанные на предыдущем этапе Работ.

8. Осуществляется модернизация СЗПДн с учетом требований законодательства.

3.6. Подготовка ИСПДн к аттестации

Цель этапа:

Разработка документации на ИСПДн и СЗПДн. Подготовка необходимых документов для организации и проведения подтверждения соответствия ИСПДн требованиям по защите информации.

* Все работы по поставке, пуско-наладке и настройке технических, программных средств и средств защиты информации осуществляется в соответствии с утвержденным Заказчиком Техническим проектом.



На данном этапе выполняются следующие работы:

- 1. Определение подразделений (ДЛ) Заказчика, ответственных за эксплуатацию СЗПДн.**
- 2. Разработка (уточнение) регламентов действий ДЛ, ответственных за обработку ПДн, на основе организационных документов по защите ПДн.**
- 3. Разработка (уточнение) технической документации на ИСПДн и СЗПДн.**
- 4. Разработка (уточнение) эксплуатационной документации на ИСПДн и СЗПДн.**
- 5. Разработка (уточнение) организационно-распорядительной документации по защите ПДн.**
- 6. Подготовка комплекта документов для аттестации ИСПДн, в том числе разработка и согласование программы-методики аттестационных испытаний.**

В результате:

Формируется полный комплект документации, необходимой для аттестации ИСПДн на соответствие требованиям законодательства.

3.7. Организация и проведение аттестации на соответствие ИСПДн требованиям по защите информации

Цель этапа:

- Проведение аттестации ИСПДн на соответствие требованиям законодательства.
- Подготовка Договора на сопровождение внедренной СЗПДн.

На данном этапе выполняются следующие работы:

- 7. Проведение аттестационных испытаний ИСПДн с выдачей соответствующих документов.**
- 8. Определение порядка сопровождения внедренной СЗПДн.**

В результате:

Заказчик получает выданный лицензиатом ФСТЭК России аттестат соответствия, подтверждающий, что ИСПДн соответствует требованиям по защите информации, предъявляемым к ИСПДн.



4. Общая характеристика работ

Таблица 1. Состав работ по приведению порядка обработки и защиты ПДн в соответствие требованиям законодательства

№ п/п	Наименование этапа	Отчетность по завершении этапа работ
1	Анализ автоматизированной и неавтоматизированной обработки ПДн	1. Отчет по результатам анализа (Приложение 1).
	В зависимости от состава инфраструктуры Заказчика его отраслевой принадлежности возможны различные варианты реализации данного этапа: 1. В виде предпроектного обследования – в случае несложной инфраструктуры (мелкий, средний бизнес, некоторые государственные организации). 2. В стандартной форме анализа автоматизированной и неавтоматизированной обработки ПДн – средний и крупный бизнес, отраслевые и ведомственные предприятий и организации, государственные организации. 3. В виде самостоятельных этапов аудита информационной безопасности предприятия (как один из аспектов аудита), в том числе с разработкой программы-методики проведения аудита - крупный бизнес, отраслевые и ведомственные предприятий и организации, государственные организации	
2	Разработка нормативной и организационно-распорядительной документации	1. Комплект документов (Приложение 2).
3	Разработка моделей угроз и нарушителей информационной безопасности. Определение необходимого уровня защищенности ПДн при обработке в ИСПДн. Определение перечня организационных и технических мер по защите ПДн при их обработке в ИСПДн. Разработка ТЗ на СЗПДн.	1. Модель (модели) угроз; 2. Модель (модели) нарушителей; 3. Проект «Акта (актов) определения необходимого уровня защищенности ПДн при их обработке в ИСПДн»; 3. Проект «Протокола (протоколов) определения организационных и технических мер по обеспечению безопасности ПДн, обрабатываемых в ИСПДн»; 5. ТЗ на создание (модернизацию) СЗПДн.
	В отдельных случаях, по согласованию с Заказчиком, вместо разработки ТЗ на СЗПДн осуществляется разработка Технических требований к системе защиты информации (Плана защиты ИСПДн).	
4	Разработка ТП на СЗПДн	1. ТП на создание СЗПДн.
	Состав и содержание отчетной документации по результатам технического проектирования согласовывается с Заказчиком. Возможна: 1. Разработка основных технических решений (Эскизного проекта) СЗПДн (в составе: пояснительная записка к эскизному проекту; Архитектурная схема системы; Схема информационного взаимодействия компонент системы). 2. Разработка Технического проекта СЗПДн (в составе: пояснительная записка к техническому проекту, ведомость технического проекта, ведомость покупных изделий, описание комплекса технических средств, спецификация оборудования) 3. Разработка Рабочей документации на СЗПДн (в составе: ведомость эксплуатационных	



Порядок проведения работ по приведению процессов обработки и защиты персональных данных в соответствие требованиям № 152-ФЗ «О персональных данных»

	документов, схема структурная комплекса технических средств, таблица соединений и подключений, схема соединений внешних проводов, программа и методика испытаний, программа опытной эксплуатации, инструкции по установке и настройке, инструкции по эксплуатации, руководство администратора безопасности, руководство пользователя.)	
5	Реализация технических и организационных мер по защите ИСПДн и приведению порядка и правил обработки ПДн в соответствии требованиям действующего законодательства в данной сфере.	1. Комплекс программно-аппаратных средств. 2. Акты установки технических и программных средств.
6	Подготовка ИСПДн к аттестации.	1. Комплект документов (Приложение 2).
7	Организация и проведение аттестации соответствия ИСПДн требованиям по защите информации	1. Аттестат соответствия 2. Комплект документов (Приложение 2) 3. Проект Договора на сопровождение системы защиты ПДн



Приложение 1

СТРУКТУРА ТИПОВОГО ОТЧЕТА по результатам проведения анализа процессов обработки и защиты персональных данных и оценке их соответствия требованиям законодательства Российской Федерации

1. Общие положения

- 1.1. Введение
- 1.2. Цель работ
- 1.3. Область проведения работ
- 1.4. Методика проведения анализа
- 1.5. Исходные данные

2. Анализ бизнес-процессов связанных с обработкой ПДн

- 2.1. Общие сведения об обрабатываемых ПДн и субъектах ПДн
- 2.2. Структурные единицы, осуществляющие обработку ПДн
- 2.3. Анализ общих требований бизнеса к технологиям обработки ПДн
- 2.4. Анализ технологических процессов неавтоматизированной обработки ПДн
- 2.5. Анализ технологий автоматизированной обработки ПДн

3. Общие характеристики ИСПДн

- 3.1. Параметры ИСПДн
- 3.2. Структура ИСПДн
- 3.3. Анализ реализованных организационных и технических мер по защите информации

4. Заключение и рекомендации

- 4.1. Заключение о степени соответствия требованиям к организации порядка обработки ПДн
- 4.2. Заключение о степени соответствия требованиям к защите ПДн при их обработке в ИСПДн
- 4.3. Рекомендации по приведению порядка обработки ПДн в соответствие требованиям законодательства РФ
- 4.4. Рекомендации по созданию/модернизации системы защиты персональных данных

Приложение 1. Перечень предоставленных исходных данных и документации

Приложение 2. Перечень обрабатываемых ПДн

Приложение 3. Рекомендуемая структура системы нормативных документов по обработке ПДн

Приложение 4. Общая схема ИСПДн

Приложение 5. Проект плана мероприятий по приведению обработки ПДн в соответствие требованиям законодательства

Примечание. Область проведения и состав работ определяются на этапе согласования договоров на проведение анализа процессов обработки и защиты персональных данных с Заказчиком.



Приложение 2

Типовая структура документации, разрабатываемой в ходе проведения работ по приведению порядка и правил обработки ПДн в соответствие требованиям законодательства Российской Федерации

