информационные технологии
КЕЙСИСТЕМС

ЭТАПЫ ПРОВЕДЕНИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ:

КОМПЛЕКСНОЕ ОБСЛЕДОВАНИЕ И РАЗРАБОТКА КОМПЛЕКТА ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНЫХ ДОКУМЕНТОВ, ПОСТРОЕНИЕ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ, АТТЕСТАЦИЯ

Сорокин Максим Александрович,
Старший инженер по безопасности информации ООО «Кейсистемс»

www.keysystems.ru

428000, Чувашская Республика, г.Чебоксары, пр. И.Яковлева, 3
тел./факс: (8352) 57-27-57

ОБЩИЕ СВЕДЕНИЯ

Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» - это унифицированный нормативный правовой акт, создающий правовую основу обращения с персональными данными граждан, осуществляемой органами государственной власти, юридическими и физическими лицами, в целях реализации конституционных прав человека.

Статья 23

1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.

Статья 24

1. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

2. Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Более ранние нормативно-правовые акты, определяющие порядок обработки персональных данных работников:

Трудовой Кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ст.85-90)

Указ Президента РФ от 30.05.2005 № 609

«Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»

ОБЩИЕ СВЕДЕНИЯ

Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» - это унифицированный нормативный правовой акт, создающий правовую основу обращения с персональными данными граждан, осуществляемой органами государственной власти, юридическими и физическими лицами, в целях реализации конституционных прав человека.

Статья 23

1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.

Статья 24

1. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

2. Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Более ранние нормативно-правовые акты, определяющие порядок обработки персональных данных работников:

Трудовой Кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ст.85-90)

Указ Президента РФ от 30.05.2005 № 609

«Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»

ОБЩИЕ СВЕДЕНИЯ

Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» определяет:

1. Основные понятия, связанные с обработкой персональных данных;
2. Принципы и условия обработки персональных данных;
3. Обязанности оператора;
4. Права субъекта персональных данных;
5. Виды ответственности за нарушение требований, установленных Федеральным законом № 152-ФЗ;
6. Государственные органы, осуществляющие контроль и надзор за соблюдением требований, установленных Федеральным законом № 152-ФЗ.

ОСНОВНЫЕ ПОНЯТИЯ

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

ОПЕРАТОР - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных

ОСНОВНЫЕ ПОНЯТИЯ

ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных

ИНФОРМАЦИОННАЯ СИСТЕМА ПЕРСОНАЛЬНЫХ ДАННЫХ (ИСПДн) - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств

ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Цель и способы обработки персональных данных должны быть законными.

2. Цель обработки персональных данных должна соответствовать цели, заявленной при сборе персональных данных, а также полномочиям оператора;

3. Объем, характер и способы обработки персональных данных должны соответствовать целям обработки персональных данных;

4. Обрабатываемые персональные данные должны быть достоверными, достаточными для заявленных целей обработки, но не избыточными;

5. Объединение созданных для несовместимых между собой целей баз данных информационных систем персональных данных **недопустимо**.

ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Предоставление и отзыв в письменной форме согласия на обработку персональных данных (ч.1 ст.9):

Согласие на обработку персональных данных должно содержать:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
2) наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;
3) цель обработки персональных данных;
4) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
5) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
6) срок, в течение которого действует согласие, а также порядок его отзыва.

2. Получение по письменному запросу доступа к своим персональным данным (ч.1 ст.14):

- получение сведений об операторе, о месте его нахождения, о наличии у оператора относящихся к нему персональных данных в доступной форме;
- ознакомление со своими персональными данными:

1) подтверждение факта обработки персональных данных оператором, а также цель такой обработки;
2) способы обработки персональных данных, применяемые оператором;
3) сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
4) перечень обрабатываемых персональных данных и источник их получения;
5) сроки обработки персональных данных, в том числе сроки их хранения;
6) сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

3. Требование от оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принятия предусмотренные законом меры по защите своих прав (ч.1,2 ст.14).

4.Обжалование действий или бездействия оператора в уполномоченном органе по защите прав субъектов персональных данных (Роскомнадзор) или в судебном порядке, если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований настоящего Федерального закона или иным образом нарушает его права и свободы (ч.1 ст.17);

5. Защита своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке (ч.2 ст.17).

ОБЯЗАННОСТИ ОПЕРАТОРА

1. Получение от субъекта персональных данных **согласия на обработку его персональных данных** и предоставление контролирующим органам доказательства получения согласия субъекта персональных данных на обработку его персональных данных или того, что обрабатываемые персональные данные являются общедоступными **(ч.3,4 ст.9)**;

2. Соблюдение конфиденциальности персональных данных **(ч.10 ст.4)** и, **если оператор на основании договора поручает обработку персональных данных другому лицу**, включение в договор обязанности обеспечения этим лицом конфиденциальности и безопасности персональных данных при их обработке **(ч.4 ст.6)**;

3. Предоставление субъекту персональных данных при сборе персональных данных информации, предусмотренной ч.4 ст.14 Федерального закона № 152-ФЗ **(ч.1 ст.18)**;

4. Принятие необходимых организационных и технических мер, в том числе использование шифровальных (криптографических) средств, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий **(ч.1 ст.19)**;

ОБЯЗАННОСТИ ОПЕРАТОРА

5. **Предоставление субъекту персональных данных, при его обращении или поступлении запроса, информации, предусмотренной ч.4 ст.14 Федерального закона № 152-ФЗ в течение 10 рабочих дней с даты получения запроса (ч.1 ст.20) либо предоставление мотивированного отказа в течение 7 рабочих дней с даты получения запроса (ч.2 ст.20);**

6. **Безвозмездное предоставление субъекту персональных данных возможности ознакомления с персональными данными, а также внесение в них необходимых изменений, уничтожение или блокирование соответствующих персональных данных по предоставлении субъектом персональных данных сведений, подтверждающих, что персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах оператор обязан уведомить субъекта персональных данных (ч.3 ст.20);**

7. **Предоставление в уполномоченный орган по защите прав субъектов персональных данных по его запросу информации, необходимой для осуществления деятельности указанного органа, в течение 7 рабочих дней с даты получения такого запроса (ч.4 ст.20);**

ОБЯЗАННОСТИ ОПЕРАТОРА

8. **В случае выявления недостоверных персональных данных (ч.1,2 ст.21):**
   1) блокирование персональных данных;
   2) уточнение персональных данных;
   3) разблокирование персональных данных.

9. **В случае выявления неправомерных действий с персональными данными (ч.3 ст.21):**
   1) устранение допущенных нарушений в срок, не превышающий 3-х рабочих дней с даты такого выявления, в случае невозможности устранения допущенных нарушений в указанный срок – уничтожить персональные данные;
   2) уведомление субъекта персональных данных.

10. **В случае достижения цели обработки персональных данных (ч.4 ст.21):**
    1) незамедлительное прекращение обработки персональных данных;
    2) уничтожение соответствующих персональных данных в срок, не превышающий 3-х рабочих дней с даты достижения цели обработки персональных данных;
    3) уведомление субъекта персональных данных.

11. **Уведомление уполномоченного органа по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных (ч.1 ст.22).**

ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДн

Требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных устанавливаются Правительством Российской Федерации (ч.1 ст.22).

Постановление Правительства РФ от 17.11.2007 № 781
«Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»

Постановление Правительства РФ от 06.07.2008 № 512
«Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»

Постановление Правительства РФ от 15.09.2008 № 687
«Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

ТРЕБОВАНИЯ ФЗ «О ПЕРСОНАЛЬНЫХ ДАННЫХ»

В соответствии ст.19 Федерального закона «оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий».

В соответствии с ч.3 ст.25 Федерального закона информационные системы персональных данных, созданные до дня вступления в силу настоящего Федерального закона, должны быть приведены в соответствие с требованиями Федерального закона не позднее 1 января 2011 года.

За нарушение требований Федерального закона законодательством Российской Федерации предусмотрена уголовная (статьи 137, 140, 272 УК РФ) и административная (статьи 5.39, 13.11, 13.14 КоАП РФ) ответственность.

КОНТРОЛЬ И НАДЗОР

Федеральным законом от 27.07.2008 г. № 152-ФЗ «О персональных данных» установлены 3 органа государственной власти, уполномоченных осуществлять мероприятия по контролю и надзору в отношении операторов, осуществляющих обработку персональных данных:

РОСКОМНАДЗОР
(уполномоченный орган по защите прав субъектов персональных данных)

Контроль и надзор за соответствием обработки персональных данных требованиям Федерального закона № 152-ФЗ

ФСБ РОССИИ
(требования в области криптографии)

ФСТЭК РОССИИ
(требования по защите информации от несанкционированного доступа и утечки техническим каналам)

Контроль и надзор за выполнением требований к обеспечению безопасности ПДн при их обработке в ИСПДн, требований к материальным носителям биометрических ПДн и технологиям хранения таких данных вне ИСПДн

ОБЩАЯ СХЕМА ВЗАИМОДЕЙСТВИЯ

РОСКОМНАДЗОР

Защита прав

СУБЪЕКТ ПЕРСОНАЛЬНЫХ ДАННЫХ
(физическое лицо)

Регистрация, контроль и надзор

ОПЕРАТОР

- государственный орган;
- муниципальный орган;
- юридическое лицо;
- физическое лицо

Обработка персональных данных

ПЕРСОНАЛЬНЫЕ ДАННЫЕ

ОСНОВНЫЕ ПДн

Фамилия, имя, отчество, год, месяц, дата рождения и т.д.

СПЕЦИАЛЬНЫЕ ПДн

Расовая принадлежность, национальная принадлежность, политические взгляды и т.д.

БИОМЕТРИЧЕСКИЕ ПДн

Сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность

Контроль и надзор

ФСБ РОССИИ

ФСТЭК РОССИИ

информационные технологии КЕЙСИСТЕМС

ДОКУМЕНТЫ ФСТЭК РОССИИ

«Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 февраля 2008 года

«Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 февраля 2008 года

Приказ ФСТЭК России от 05.02.2010 № 58 **«Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных»**

Решением ФСТЭК России от 05.03.2010 отменены:

Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных" от 15 февраля 2008 года

Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" от 15 февраля 2008 года

ДОКУМЕНТЫ ФСБ РОССИИ

«Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации»
от 21.02.2008 № 149/54-144

«Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных»
от 21.02.2008 № 149/6/6-622

БЕЗОПАСНОСТЬ ПДн: РЕШЕНИЕ ОТ КОМПАНИИ «КЕЙСИСТЕМС»

Компания «Кейсистемс» предлагает полный спектр услуг, необходимых для реализации положений Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»:

1. **Комплексное обследование информационных систем (инвентаризация и категорирование информационных ресурсов, определение принципов функционирования и используемых технологий обработки информации; определение требований нормативных правовых актов Российской Федерации для обследуемых систем);**
2. **Классификация информационных систем персональных данных (ИСПДн);**
3. **Разработка комплекта организационно-распорядительных документов по защите персональных данных;**

БЕЗОПАСНОСТЬ ПДн: РЕШЕНИЕ ОТ КОМПАНИИ «КЕЙСИСТЕМС»

4. Разработка модели угроз безопасности персональных данных, определение перечня актуальных угроз безопасности персональных данных;

5. Подготовка рекомендаций по обеспечению безопасности информации;

6. Разработка технического задания на систему защиты персональных данных (СЗПДн) и проекта СЗПДн;

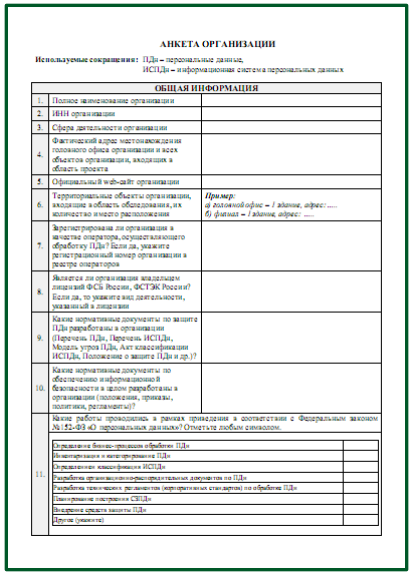
7. Ввод СЗПДн в эксплуатацию: поставка, установка и настройка сертифицированных средств защиты информации;

8. Оценка соответствия ИСПДн требованиям безопасности информации (аттестация);

9. Техническое обслуживание СЗПДн.

С ЧЕГО НАЧАТЬ?

1. Анкетирование. (Заказчик заполняет анкету для предварительной оценки объема работ и высылает ее по факсу: **(8352)57-27-57** или e-mail: **sec@keysystems.ru**).

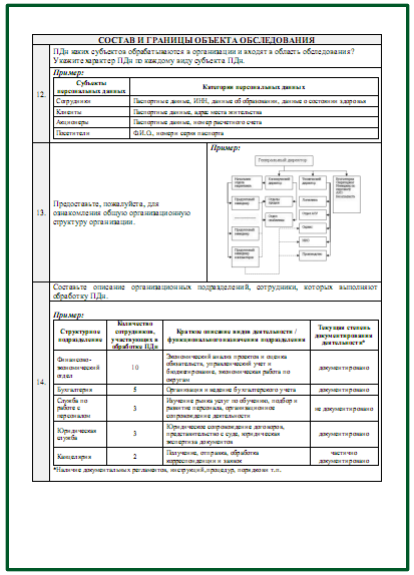


АНКЕТА ОРГАНИЗАЦИИ

Используемые сокращения: ПДн – персональные данные,
ИСПДн – информационная система персональных данных

	ОБЩАЯ ИНФОРМАЦИЯ	
1.	Полное наименование организации	
2.	ИНН организации	
3.	Сфера деятельности организации	
4.	Фактический адрес местонахождения головного офиса организации и всех объектов организации, входящих в область проекта	
5.	Официальный web-сайт организации	
6.	Территориальные объекты организации, входящие в область обследования, их количество и место расположения	*Пример:* *а) головной офис – 1 здание, адрес: ....* *б) филиал – 1 здание, адрес: ....*
7.	Зарегистрирована ли организация в качестве оператора, осуществляющего обработку ПДн? Если да, укажите регистрационный номер организации в реестре операторов	
8.	Является ли организация владельцем лицензий ФСБ России, ФСТЭК России? Если да, то укажите вид деятельности, указанный в лицензии	
9.	Какие нормативные документы по защите ПДн разработаны в организации (Перечень ПДн, Перечень ИСПДн, Модель угроз ПДн, Акт классификации ИСПДн, Положение о защите ПДн и др.)?	
10.	Какие нормативные документы по обеспечению информационной безопасности в целом разработаны в организации (положения, приказы, политики, регламенты)?	
11.	Какие работы проводились в рамках приведения в соответствии с Федеральным законом №152-ФЗ «О персональных данных»? Отметьте любым символом.	

11.	Определение бизнес-процессов обработки ПДн	
	Инвентаризация и категорирование ПДн	
	Определение классификации ИСПДн	
	Разработка организационно-распорядительных документов по ПДн	
	Разработка технических регламентов (корпоративных стандартов) по обработке ПДн	
	Планирование построения СЗПДн	
	Внедрение средств защиты ПДн	
	Другое (укажите)	



СОСТАВ И ГРАНИЦЫ ОБЪЕКТА ОБСЛЕДОВАНИЯ

12.	ПДн каких субъектов обрабатываются в организации и входят в область обследования? Укажите характер ПДн по каждому виду субъекта ПДн.	
	Пример:	

Субъекты персональных данных	Категории персональных данных
Сотрудники	Паспортные данные, ИНН, данные об образовании, данные о состоянии здоровья
Клиенты	Паспортные данные, адрес места жительства
Акционеры	Паспортные данные, номер расчетного счета
Посетители	Ф.И.О., номера серии паспорта

13.	Предоставьте, пожалуйста, для ознакомления общую организационную структуру организации.	*Пример:*
14.	Составьте описание организационных подразделений, сотрудники, которых выполняют обработку ПДн.	
	Пример:	

Структурное подразделение	Количество сотрудников, участвующих в обработке ПДн	Кратко описание видов деятельности / функциональных назначений подразделения	Текущая степень документирования деятельности*
Финансово-экономический отдел	10	Экономический анализ проектов и оценка обязательств, управленческий учет и бюджетирование, экономическая работа по округам	документировано
Бухгалтерия	5	Организация и ведение бухгалтерского учета	документировано
Служба по работе с персоналом	3	Изучение рынка услуг по обучению, подбор и развитие персонала, организационное сопровождение деятельности	не документировано
Юридическая служба	3	Юридическое сопровождение договоров, представительство в суде, юридическая экспертиза документов	документировано
Канцелярия	2	Получение, отправка, обработка корреспонденции и заявок	частично документировано

*Наличие документальных регламентов, инструкций, процедур, порядков и т.п.

СИСТЕМЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

15.	В каких автоматизированных информационных системах, присутствуют ПДн? Укажите наименование, общее назначение, количество и физическое место размещения серверного оборудования и рабочих станций по каждой информационной системе	
	Пример:	

№ п/п	Автоматизированная система	Общее назначение	Кол-во серверов, рабочих мест	Физическое место размещения
1.	АИС «Банк»	Учет расчетов клиентами (абонентами)	1 сервер, 20 АРМ	Головной офис
2.	АИС «Зарплата»	Начисление заработной платы сотрудникам	1 сервер, 5 АРМ	Головной офис
3.	1С-Бухгалтерия	Начисление заплат акционерам	1 сервер, 5 АРМ	Головной офис
4.	«Банк-Клиент»	Взаимодействие с банками	1 АРМ	Удаленный офис №1
5.	Служба каталогов AD (Active Directory)	Ведение основной деятельности организации	2 сервера	Удаленный офис №2
6.	Электронный телефонный справочник домашних телефонов	Ведение основной деятельности организации	3 АРМ	На рабочей станции начальника отдела кадров

16.	Обрабатываются ли в организации ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни? Если да, то какие именно, кем обрабатываются, на основании каких документов и в каких автоматизированных системах?	
17.	Располагаются ли компоненты автоматизированных систем (п. 156) за пределами РФ? Если да, то, какие?	
18.	Какие логические и/или физические схемы сети имеются в организации?	*Пример:* • *Структурная (топологическая) схема с указанием информационных связей между площадками;* • *Структурная (топологическая) схема с указанием информационных связей между устройствами;* • *Схема размещения и расположения основных технических средств и систем на объекте с приемной и границами контролируемой зоны;* • *Схема потоков передачи персональных данных с приемной и границами контролируемой зоны объекта.*
19.	Предоставляется ли сторонним организациям доступ к данным автоматизированных систем (п.16) Обслуживаются ли автоматизированные системы (п.16) сторонними организациями? Если да, то укажите наименование организаций, и какими документами это регламентируется	
20.	Есть ли ограничения по срокам проведения обследования, если есть то какие и чем они вызваны?	

2. Уточнение анкетных данных Заказчика по телефону или в ходе ознакомительного визита .

3. Заключение договора (договоров).

ОБЩИЙ ПОРЯДОК ПРОВЕДЕНИЯ РАБОТ

Работы проводятся в 3 этапа:

Комплексное обследование и подготовка организационно-распорядительных документов

↓

Построение системы защиты персональных данных (СЗПДн)

↓

Проведение оценки соответствия ИСПДн требованиям безопасности информации (аттестация или декларирование)

ЭТАП I. КОМПЛЕКСНОЕ ОБСЛЕДОВАНИЕ ИСПДн

1. **Встреча с сотрудниками, участвующими в обработке ПДн**.
2. **Изучение физических характеристик объекта (планов зданий, помещений).**
3. **Изучение технологических процессов обработки ПДн:**
   - интервьюирование сотрудников;
   - изучение документов (учредительные документы, положения, должностные инструкции, профильные нормативно-правовые акты, договоры и т.д.).
4. **Составление перечня ИСПДн.**
5. **Составление перечня ПДн и сотрудников, участвующих в обработке ПДн (для каждой ИСПДн).**

ЭТАП I. КОМПЛЕКСНОЕ ОБСЛЕДОВАНИЕ ИСПДн

6. Анализ IT-инфраструктуры:

- изучение карты сети;

- изучение используемых прикладных систем;

- компоновка карты сети и приложений;

- изучение дополнительной документации по прикладным системам и техническим средствам.

7. Изучение и инспекция используемых мер и средств защиты:

- составление перечня СЗИ;

- инспекционная проверка мест установки СЗИ;

- изучение документации к СЗИ.

8. Разработка описания технологических процессов обработки ПДн.

9. Разработка паспортов ИСПДн (общие характеристики ИСПДн, описание аппаратного и программного обеспечения АРМ, топологическая схема ИСПДн).

10. Разработка частных моделей угроз безопасности персональных данных при их обработке в ИСПДн.

КЛАССИФИКАЦИЯ ИСПДн

Совместный приказ ФСТЭК, ФСБ, Мининформсвязи от 13.02.2008 № 55/86/20

«Об утверждении Порядка проведения классификации информационных систем персональных данных»

Типовые информационные системы - информационные системы, в которых требуется обеспечение только конфиденциальности персональных данных.

Специальные информационные системы - информационные системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

Класс специальной информационной системы определяется на основе модели угроз безопасности персональных данных в соответствии с соответствующими методическими документами ФСБ России и ФСТЭК России.

ЭТАП I. КОМПЛЕКСНОЕ ОБСЛЕДОВАНИЕ ИСПДн

Категория ПДн (Хпд)		Объем обрабатываемых в ИСПДн персональных данных (Хнпд)		
		1	2	3
		В информационной системе одновременно обрабатываются ПДн более чем 100 000 субъектов персональных данных или ПДн субъектов персональных данных в пределах субъекта РФ или РФ в целом	В информационной системе одновременно обрабатываются ПДн от 1000 до 100 000 субъектов персональных данных или ПДн субъектов персональных данных, работающих в отрасли экономики РФ, в органе государственной власти, проживающих в пределах муниципального образования	В информационной системе одновременно обрабатываются данные менее чем 1000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации
1	ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни	К1	К1	К1
2	ПДн, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением ПДн, относящихся к категории 1	К1	К2	К3
3	ПДн, позволяющие идентифицировать субъекта персональных данных	К2	К3	К3
4	Обезличенные и (или) общедоступные ПДн	К4	К4	К4

КЛАССИФИКАЦИЯ СПЕЦИАЛЬНОЙ ИСПДн

В соответствии с документами ФСТЭК России Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" от 15 февраля 2008 года и Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных" от 14 февраля 2008 года определяется перечень актуальных угроз безопасности.

Если среди актуальных угроз безопасности ПДн есть :

угрозы низкой опасности (реализация этих угроз может привести к незначительным негативным последствиям для субъектов персональных данных) – это ИСПДн класса 3 (К3);

угрозы средней опасности (реализация этих угроз может привести к негативным последствиям для субъектов персональных данных)) – это ИСПДн класса 2 (К2);

угрозы высокой опасности (реализация этих угроз может привести к значительным негативным последствиям для субъектов персональных данных) – это ИСПДн класса 1 (К1).

ЭТАП I. КОМПЛЕКСНОЕ ОБСЛЕДОВАНИЕ ИСПДн

11. Классификация ИСПДн с учетом моделей угроз безопасности ПДн.

12. Подготовка проектов организационно-распорядительных документов:

- *Положение о защите персональных данных в организации;*
- *Положение по организации и проведению работ по обеспечению безопасности ПДн при их обработке в ИСПДн;*
- *Приказ о назначении администратора безопасности ИСПДн;*
- *Инструкция администратора ИСПДн;*
- *Инструкция пользователя ИСПДн;*
- *Приказ о контролируемой зоне;*
- *Матрица доступа (разрешительная система допуска) и т.д.*

13. Подготовка рекомендаций по принятию организационных мер по защите ПДн.

14. Разработка технического задания на построение системы защиты персональных данных с рекомендациями по применению технических средств защиты информации.

ЭТАП I. КОМПЛЕКСНОЕ ОБСЛЕДОВАНИЕ ИСПДн

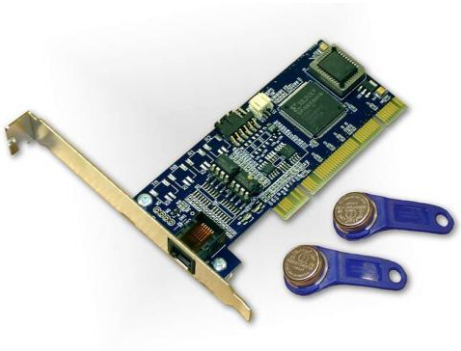
ТЕХНИЧЕСКОЕ ЗАДАНИЕ НА РАЗРАБОТКУ СЗПДн ДОЛЖНО СОДЕРЖАТЬ:

- обоснование разработки СЗПДн;
- исходные данные создаваемой (модернизируемой) ИСПДн в техническом, программном, информационном и организационном аспектах;
- класс ИСПДн;
- ссылку на нормативные документы, с учетом которых будет разрабатываться СЗПДн и приниматься в эксплуатацию ИСПДн;
- конкретизацию мероприятий и требований к СЗПДн;
- перечень предполагаемых к использованию сертифицированных средств защиты информации;
- состав, содержание и сроки проведения работ по этапам разработки и внедрения СЗПДн.

ЭТАП II. ПОСТРОЕНИЕ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Разработка технического проекта СЗПДн.

2. Приобретение, установка и настройка сертифицированных технических, программных и программно-технических средств защиты информации.



3. Реализация разрешительной системы доступа пользователей ИСПДн к обрабатываемой на ИСПДн информации.

ЭТАП II. ПОСТРОЕНИЕ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

4. Определение подразделений и назначение лиц, ответственных за эксплуатацию средств защиты информации.

5. Корректировка (дополнение) организационно-распорядительной документации в части защиты информации (положений, приказов, паспортов ИСПДн, топологических схем, инструкций и других документов).

6. Приобретение, установка и настройка антивирусного программного обеспечения.

7. Приобретение, установка и настройка системы резервного копирования.

8. Организация охраны и физической защиты помещений ИСПДн (исключение несанкционированного доступа к техническим средствам ИСПДн)

МЕТОДЫ СНИЖЕНИЯ ЗАТРАТ НА СОЗДАНИЕ СЗПДн:

1. Максимальное использование возможностей имеющихся в наличии средств защиты информации, операционных систем и прикладного программного обеспечения.
2. Сокращение числа сотрудников, обрабатывающих ПДн.
3. Частичное исключение ПДн.
4. Частичное обезличивание ПДн.
5. Сегментация ИСПДн (разделение информационной системы на части сертифицированными межсетевыми экранами (МЭ).
6. Организация терминального доступа к ИСПДн.
7. Частичная обработка ПДн вне ИСПДн (на бумажных носителях).

ЭТАП III. АТТЕСТАЦИЯ ИСПДн

В соответствии с п.3.11 нормативного документа ФСТЭК России «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» **(отменен)** оценка соответствия ИСПДн требованиям безопасности ПДн проводится в виде:

для ИСПДн 1 и 2 классов – обязательной сертификации (аттестации) по требованиям безопасности информации;

для ИСПДн 3 класса – декларирования соответствия требованиям безопасности информации.

Для ИСПДн 4 класса оценка соответствия проводится по решению оператора.

ЭТАП III. АТТЕСТАЦИЯ ИСПДн

1. **Разработка программы и методики аттестационных испытаний.**
2. **Оценка эффективности защищенности информации от несанкционированного доступа (с применением специализированного программного обеспечения).**
3. **Объектовые специсследования ИСПДн.**
4. **Разработка комплекта документов по аттестации ИСПДн:**
   - Предписание на эксплуатацию ИСПДн;
   - Протокол оценки защищенности информации от утечки по каналу НСД;
   - Протоколы оценки защищенности информации от утечки по техническим каналам;
   - Заключение по результатам аттестационных испытаний ИСПДн;
   - Аттестат соответствия ИСПДн требованиям по защите информации.

ЭТАП III. АТТЕСТАЦИЯ ИСПДн

Оборудование для аттестации

Автоматизированная система оценки защищенности технических средств от утечки информации по каналу ПЭМИН «Сигурд»

Автоматизированная система оценки защищённости от утечки информации по вибрационному и акустическому каналам «Шепот»

Автоматизированная система измерения действующих высот случайных антенн и коэффициентов затухания электромагнитных сигналов «Стентор»

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

На официальном сайте компании «Кейсистемс»

www.keysystems.ru

в разделе «Защита персональных данных» можно:

- получить дополнительную информацию об услугах в сфере защиты персональных данных, оказываемых компанией «Кейсистемс»;

- скачать анкету для проведения обследования и аттестации ИСПДн;

- ознакомиться с актуальной нормативной базой в сфере обработки персональных данных.

Контактная информация:

многоканальный тел./факс: **(8352) 57-27-57,**

e-mail: **sec@keysystems.ru**

СПАСИБО ЗА ВНИМАНИЕ!