

**Памятка по выполнению требований
ФЗ №152
«О персональных данных»**

ЗАКОНОДАТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

- Федеральный закон 152-ФЗ «О персональных данных»
- Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ
- ПП № 1119 «Требования к защите персональных данных при их обработке в информационных системах персональных данных»
- ПП № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
- Приказ ФСТЭК России 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

Контроль соблюдения требований по обработке персональных данных



Роскомнадзор (Федеральная служба по надзору в сфере связи и массовых коммуникаций) - осуществляет контроль и надзор за соответствием обработки ПД требованиям законодательства

ФСТЭК России (Федеральная служба по техническому и экспортному контролю) - осуществляет контроль и надзор за методами и способами защиты информации в информационных системах с использованием технических средств



ФСБ России (Федеральная служба безопасности РФ) - осуществляет контроль и надзор за методами и способами защиты информации в информационных системах с использованием криптографических средств защиты информации

Основные термины

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.

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

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.

Что такое персональные данные?

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

- фамилия, имя, отчество;
- должность;
- контактные данные;
- паспортные данные;
- фотография;
- и т.д.

ПРИМЕРЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

- Иванов Иван Иванович
- Иванов И.И. 01.01.1999
- 01.01.1999
- +7(911) 111-11-11
- Паспорт 1234 567890
- IvanovII@yandex.ru

Какие компании должны в первую очередь обратить внимание на выполнение требований Закона

В первую очередь под действие ФЗ 152 «О персональных данных» попадают организации (Операторы) работающие в следующих сферах:

- медицина (поликлиники, больницы и т.д.);
- финансы (банки, микрокредитные организации, страховые компании и т.д.);
- образование (дошкольные образовательные учреждения, школы, ВУЗы и т.д.);
- юриспруденция (адвокаты, нотариусы и т.д.);
- торговля;
- On-line площадки осуществляющие взаимодействие с пользователями (интернет магазины и т.д.).

В каких информационных системах осуществляется обработка ПДн?

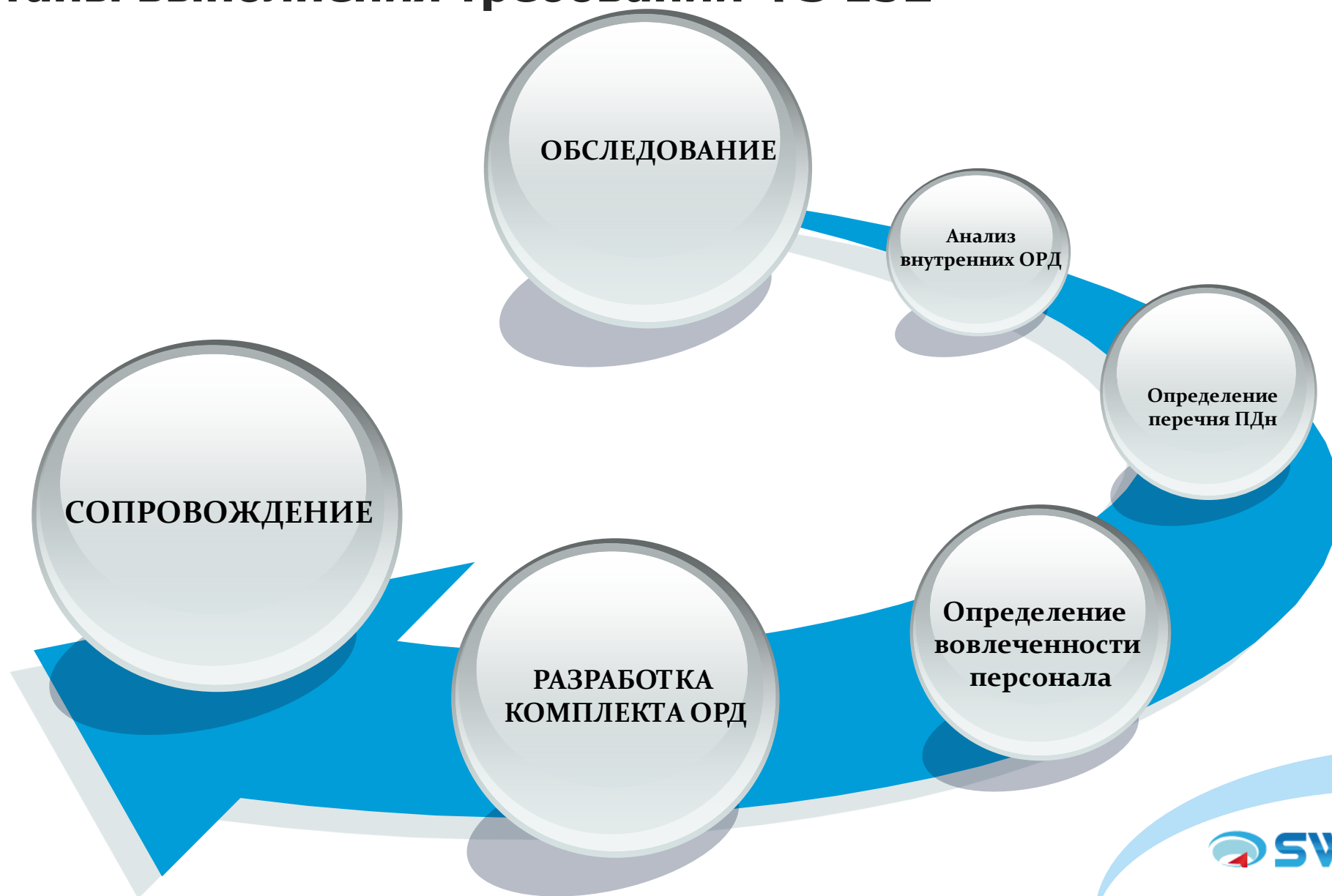
Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

- Бухгалтерские программы
- Программы кадрового учета
- CRM-системы с информацией о действующих и потенциальных клиентах
- Системы биллинга
- ERP-системы, обрабатывающие персональные данные
- и др.

Обязанности оператора

- Назначить ответственного за обработку персональных данных.
- Издать документы, определяющие политику в отношении обработки персональных данных, и локальных актов (<http://www.swrit.ru/dokumenty-po-personalnym-dannym.html>).
- Привести процессы обработки ПДн в соответствии с требованиями ФЗ 152 «О персональных данных».
 - Организовать хранение/уничтожение документов, содержащих персональные данные.
 - Регламентировать доступ к персональным данным.
 - Организовать сбор согласий на обработку ПДн.
 - Скорректировать договора с контрагентами (если договором предусмотрен обмен ПДн).
- Подать уведомление об обработке ПДн в Роскомнадзор (<https://rkn.gov.ru/personal-data/forms/>).

Этапы выполнения требований ФЗ 152



Документы, которые должен иметь Оператор ПДн

- Положение по обработке персональных данных (включая необходимые формы)
- Приказ об организации работ по защите персональных данных
- Политика обеспечения безопасности персональных данных
- Перечень персональных данных, обрабатываемых в ИСПДн
- Акт классификации ИСПДн
- Инструкция по учёту носителей персональных данных
- Инструкция администратору ИСПДн
- Инструкция о порядке допуска лиц к информационным ресурсам ИСПДн
- Инструкция по внесению изменений в ИСПДн
- Инструкция по организации антивирусной защиты в ИСПДн
- Инструкция по организации парольной защиты
- Инструкция по резервному копированию и восстановлению персональных данных
- Инструкция пользователю ИСПДн
- Инструкция по использованию ресурсов сети Интернет
- План внутренних проверок состояния защиты персональных данных
- Журнал регистрации входящих запросов и обращений субъектов
- Журнал инструктажа пользователей и обслуживающего персонала
- Журнал учета мероприятий по защите информации

Ответственность за несоблюдение требований ФЗ №152

Административная

Нарушение	Санкция
Обработка персональных данных в случаях, не предусмотренных законом, либо обработка, несовместимая с целями сбора персональных данных. Часть 1 ст. 13.11 КоАП РФ	Штраф до 50 тыс. руб. (за каждый выявленный факт)
Обработка персональных данных без письменного согласия субъекта, когда это необходимо, либо обработка данных с нарушением требований к составу сведений, включаемых в такое согласие. Часть 2 ст. 13.11 КоАП РФ	Штраф до 75 тыс. руб. (за каждый выявленный факт)
Невыполнение оператором обязанности по опубликованию или обеспечению иным образом неограниченного доступа к политике обработки персональных данных. Часть 3 ст. 13.11 КоАП РФ	Штраф до 30 тыс. руб.
Невыполнение оператором обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных. Часть 4 ст. 13.11 КоАП РФ	Штраф до 40 тыс. руб.
Невыполнение оператором в установленные сроки требования субъекта персональных данных или его представителя либо Роскомнадзора об уточнении персональных данных, их блокировании или уничтожении. Часть 5 ст. 13.11 КоАП РФ	Штраф до 45 тыс. руб.

Ответственность за несоблюдение требований ФЗ №152

Уголовная

Нарушение	Санкция
<p>Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или СМИ.</p> <p>Статья 137 Уголовного кодекса</p>	<p>Штраф до 200 тыс. руб., лишение свободы на срок до 2-х лет</p>
<p>Незаконное публичное распространение информации, указывающей на личность лица, не достигшего 16 лет, по уголовному делу, либо информации, содержащей описание полученных им в связи с преступлением физических или нравственных страданий.</p> <p>Статья 137 Уголовного кодекса</p>	<p>Штраф до 300 тыс. руб., либо лишение свободы на срок до 5-ти лет</p>
<p>Неправомерный доступ к охраняемой законом компьютерной информации, если это повлекло ее уничтожение, блокирование, модификацию либо копирование.</p> <p>Статья 272 УК РФ</p>	<p>Штраф до 200 тыс. руб., либо лишение свободы на срок до 2-х лет</p>
<p>Неправомерный отказ должностного лица в предоставлении документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление ему неполной или заведомо ложной информации, если это причинило вред правам и законным интересам граждан.</p> <p>Статья 140 УК РФ</p>	<p>Штраф до 200 тыс. руб.</p>

Ответственность за несоблюдение требований ФЗ №152

Гражданско-правовая

Нарушение	Санкция
Причинение лицу убытков в результате нарушения правил обработки его персональных данных. Статья 15 Гражданского кодекса	Возмещение убытков
Причинение гражданину морального вреда (нравственных страданий) вследствие нарушения правил обработки персональных данных. Статья 24 закона о персональных данных, ст. 151 ГК РФ	Компенсация морального вреда

Дисциплинарная

Разглашение одним работником персональных данных другого, если они стали известны ему в связи с исполнением трудовых обязанностей. Подпункт "в" п. 6 ч. 1 ст. 81 Трудового кодекса	Увольнение
Иные нарушения в области персональных данных при их обработке. Статья 90, ст. 192 ТК РФ	Замечание или выговор



info@swrit.ru



Москва, Складочная ул., 3, стр. 2
Телефон: +7 499 755-74-33

www.swrit.ru 