

## Организация работы с персональными данными и их защита

---

Федеральный закон № 152-ФЗ от 27.07.2006

Как защитить персональные данные в соответствии с положениями законодательства?

Как минимизировать затраты на создание системы защиты?

Как завершить работы в установленный срок (не позднее 01.01.2011г.)?

Ответственность за нарушение закона.

Необходимость и степень защиты информации в коммерческих структурах до недавнего времени определялись каждой компанией самостоятельно. С принятием федерального закона № 152-ФЗ от 27.07.2006г. «О персональных данных» ситуация кардинально изменилась – теперь обработка персональных данных физических лиц и меры по их защите строго регламентированы и охраняются государством.

**Персональные данные** - 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.

Персональные данные (ПДн) есть в любой компании: это кадровый учет, базы данных клиентов, контрагентов, партнеров, контактные списки электронной почты и т.п.

# Обязанность операторов



В соответствии с положениями закона **ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ** является прямой обязанностью операторов персональных данных, а это практически все предприятия Российской Федерации. Срок завершения работ по созданию системы защиты персональных данных – не позднее 01.01.2011 года, т.е. в течении текущего 2010 года.

За неисполнение требований законом предусмотрена административная, уголовная, гражданская, дисциплинарная и иные виды ответственности. Санкции применяются как к руководителям индивидуально, так и к предприятию в целом, вплоть до прекращения обработки персональных данных или аннулирования лицензии на основной вид деятельности компании.

# Нарушение конфиденциальности ПДн или правил работы с ними



## Нарушение: пример 1

Ваша компания начала работу после вступления в силу закона 152-ФЗ или же вы создали новую информационную систему в которой содержатся персональные данные, но не представили уведомления в РОСКОНАДЗОР РФ.

В случае проверки или возникновения конфликтной ситуации, исходя из требований ст. 13.23 КоАП РФ:  
Должностные лица – штраф до 2.000 руб;  
Юридическое лицо – штраф до 20.000 руб.

# Нарушение конфиденциальности ПДн или правил работы с ними



## Нарушение: пример 2

В компании имеется бланк заявления на предоставление отпуска сотруднику, который не соответствует требованиям п.7 постановления правительства РФ №687 от 15.09.2008.

В случае проверки или возникновения конфликтной ситуации, исходя из требований ст. 13.11 КоАП РФ:  
Должностные лица – штраф до 1.000 руб;  
Юридическое лицо – штраф до 10.000 руб.  
(за каждый факт нарушения)

# Нарушение конфиденциальности ПДн или правил работы с ними



## Нарушение: пример 3

Ваша торговая система или интернет магазин не были приведены в соответствие требованиям методических рекомендаций ФСБ ФСТЭК по защите персональных данных или при классификации ИС были допущены ошибки. В системе был зафиксирован заказ клиента, но сотрудник компании смог преднамеренно или случайно изменить дату заказа, детали или операции с заказом. Это повлекло последствия для клиента.

В случае проверки или возникновения конфликтной ситуации, исходя из требований ст. 274 УК РФ:  
лишение права занимать определённые должности до 5 лет;  
обязательные работы до 240 часов;  
ограничение свободы до 2х лет;

Комплекс мероприятий по защите персональных данных регламентирован нормативно-методическими документами и состоит из организационных и технических мер защиты информации. Отдельные виды работ выполняются при наличии соответствующих лицензий, а их качество зависит от квалификации и подготовки специалистов по информационной безопасности.

# Факторы успеха проектов по защите ПДн



1. Наличие высококвалифицированных специалистов в области информационной безопасности.
2. Минимизация временных и финансовых затрат в ходе ведения проектов.
3. Разработка комплексных систем защиты информации с максимальным использованием существующих возможностей ИТ – инфраструктуры.
4. Строгое соответствие требованиям законодательства и стандартам по ИБ.

# Основные мероприятия по организации защиты ПДн



1. Определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз.	6. Учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных.
2. Разработка на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем.	7. Учет лиц, допущенных к работе с персональными данными в информационной системе.
3. Проверка готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации.	8. Контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.
4. Установка и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией.	9. Разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.
5. Обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними.	10. Описание системы защиты персональных данных.

# Подготовительный этап



1. Принятие решения о подаче уведомления как оператора персональных данных.
2. Определение ответственного подразделения.
3. Подготовка плана мероприятий.

# Основной этап



1. Проведение нормативно-методических мероприятий.
2. Проведение анализа эксплуатируемых и создаваемых систем с целью определения их принадлежности к ИСПДн.
3. Обследование и классификация ИСПДн.
4. Разработка Плана организационных и технических мероприятий по приведению ИСПДн в соответствие с документами.
5. Доработка эксплуатируемых и разработки новых систем в соответствии с документами.

# Нормативно-методические мероприятия



1. Цели обработки ПДн;
2. Перечень персональных данных, обрабатываемых в ИС;
3. Требования по объему, содержанию, срокам обработки ПДн;
4. Условия получения согласия на обработку ПДн и форму такого согласия;
5. Порядок доступа работников к обработке ПДн;
6. Требования к порядку хранения носителей ПДн;
7. Условия прекращения обработки ПДн и порядок их уничтожения;
8. Порядок обработки обращений субъектов (или их законных представителей) по вопросам обработки их ПДн, также порядок действий в случае запросов Уполномоченного органа по защите прав субъектов ПДн.

# Обследование и классификация ИС



1. Определить тип ИСПДн.
2. Определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз.
3. Определение категории персональных данных, обрабатываемых в информационной системе.
4. Определение объёма обрабатываемых персональных данных.
5. Определение структуры информационной системы.
6. Определение режима обработки персональных данных в информационной системе.

# Примерный перечень документов по защите ПДн



Частные модели угроз безопасности	Уведомление о начале обработки ПДн	Инструкция ответственного за информационную безопасность	Описание технологического процесса
Положение о порядке организации и проведения работ по защите конфиденциальной информации	Перечень сведений, содержащих ПДн	Инструкция по организации антивирусной защиты	Инструкция по физической охране информационной системы ПДн, контролю доступа в помещение
Положение о порядке обработки ПДн без использования средств автоматизации	Перечень лиц, допущенных к работе с ПДн	Инструкция по организации парольной защиты	Инструкция по учету материальных носителей, регистрации их выдачи
Положение об обработке ПДн работников	Согласие субъекта на обработку ПДн	Инструкция по разграничению доступа пользователя к средствам защиты и информационным ресурсам	Регламент резервного копирования данных
Приказ о проведении классификации информационной системы ПДн	Обязательство о неразглашении конфиденциальной информации (приложение к трудовому договору)	Журнал учета выдачи материальных носителей информации	Журнал учета паролей пользователя информационной системы
Акты проведения классификации информационной системы ПДн	Инструкция о порядке работы с ПДн	Журнал учета ключей от помещений	Журнал учета средств защиты информации
Приказ о назначении ответственного за информационную безопасность	Инструкция пользователя информационной системы ПДн	Журнал учета ключей от сейфов	Журнал учета уничтожения материальных носителей

# Как заработать деньги с помощью ФЗ-152 ?



1. Иметь в штате высокопрофессиональных ИТ специалистов.
2. Иметь необходимые лицензии для осуществления деятельности по защите персональных данных.
3. Наладить контакты с поставщиками аппаратно/программных средств.
4. Провести анализ рынка.
5. Провести маркетинг.

1. Руководитель проекта.
2. Аналитик по информационной безопасности.
3. Архитектор по информационной безопасности.
4. Инженер по информационной безопасности.

## 1. Руководитель проекта:

- Общий контроль за ходом работ.
- Ведение проектной документации.
- Решение организационных вопросов.
- Взаимодействие с представителями Заказчика.
- Планирование графиков работ.
- Решение вопросов выделения ресурсов.
- Планирование регулярных работ и процедур.
- Предоставление отчетности.

## **2. Аналитик по информационной безопасности:**

- Выявление и анализ системных требований.
- Разработка архитектуры решения.
- Написание и согласование проектной документации.
- Предоставление отчетности Руководителю проекта.

## **3. Архитектор по информационной безопасности:**

- Выполнение проектного плана.
- Постановка локальных задач для Инженера.
- Разработка архитектуры решения.
- Написание и согласование проектной документации.
- Предоставление отчетности Руководителю проекта.

## **4. Инженер по информационной безопасности:**

- Выполнение проектного плана.
- Решение организационных и технических проблем, связанных с выполнением проекта.
- Разработка архитектуры решения.
- Написание и согласование проектной документации.
- Предоставление отчетности Руководителю проекта.

# Получение лицензии ФСТЭК



Согласно «Положения о лицензировании деятельности по технической защите конфиденциальной информации» утвержденное ПП РФ от 15 августа 2006г. за номером № 504, для получения лицензии необходимо:

1. Провести аттестацию помещения и АС **(200 тыс.руб).**
2. Для осуществления лицензируемой деятельности купить программы для электронно-вычислительных машин (программа поиска и гарантированного уничтожения информации на дисках «TERRIER» версия 3.0; программа фиксации и контроля исходного состояния программного комплекса «ФИКС» версия 2.0.1; программа контроля полномочий доступа к информационным ресурсам «Ревизор 2 XP»; средство создания модели системы разграничения доступа «Ревизор 1 XP») **(20 тыс. руб.).**

# Получение лицензии ФСТЭК



3. Обучить сотрудников по защите информации (**30 тыс. руб.**)
4. Приобрести производственное, испытательное и контрольно-измерительное оборудование, средств защиты информации и средств контроля защищенности информации, необходимых для осуществления лицензируемой деятельности (**около 1 мл. руб.**)
5. Разработать внутреннюю нормативно-методическую документацию по защите конфиденциальной информации (**можно сделать своими силами**).