



# **152-ФЗ:** **Соблюдать нельзя игнорировать**

22 сентября 2009 г.

**Леонид Хоревский**  
Директор Департамента сопровождения  
Компания «Диасофт»

# Историческая справка

- **1981 год** - Совет Европы принял Конвенцию «О защите личности в связи автоматической обработкой персональных данных»
- **2001 год** – Россия присоединилась к Конвенции Совета Европы
- **2005 год** - подписан Федеральный закон от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматической обработке персональных данных»)
- **2006 год** - подписан Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных».

**К 2006 году почти вся Европа, многие страны Азии, Америки и даже Африки имели аналогичные законы. В чем Россия пошла дальше других стран, так это в разработке технических регламентов и требований, которые транслируют положения верхнего уровня в конкретные советы и рекомендации.**

# Законодательство и нормативные документы в области защиты персональных данных

**Федеральный закон  
«О персональных данных» №152-ФЗ  
от 27.06.2006**

**Постановление  
Правительства РФ №781**

«Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» от 17.11.2007

**Постановление  
Правительства РФ №687**

«Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008

**Приказ ФСТЭК РФ №55,  
ФСБ РФ №86,  
Мининформсвязи РФ  
№20**

«Об утверждении порядка проведения классификации информационных систем персональных данных» от 13.02.2008

**Документ ФСТЭК**

«Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» от 14.02.2008

**Документ ФСТЭК**

«Рекомендации по обеспечению безопасности персональных данных при их обработке, в информационных системах персональных данных» от 14.02.2008

**Документ ФСТЭК**

«Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных» от 14.02.2008

**Документ ФСТЭК**

«Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 14.02.2008

# Требования 152-ФЗ

1. **Определить информационные системы, обрабатывающие персональные данные (ИСПДн), перечень обрабатываемых данных и причины их обработки**
2. **Выполнить организационные мероприятия и разработать эксплуатационно-технологическую документацию на используемые системы**
3. **Выполнить технические мероприятия по защите персональных данных – ввести в эксплуатацию сертифицированные средства защиты информации (СЗИ)**
4. **Получить аттестат на используемые системы (ИСПДн) и защищаемые помещения**
5. **Получить лицензию ФСТЭК на техническую защиту информации и, если используются СКЗИ, лицензию ФСБ.**

**Необходимо обеспечить выполнение требований законодательства к 01.01.2010 г.**

## Взгляд «Диасофт» на 152-ФЗ

- Основная часть предъявляемых законом требований относится **не к АБС, а к системному окружению** (операционной системе, антивирусному ПО, сетевому взаимодействию) или организационным мерам (ограничение физического доступа к системе, регистрация носителей, регулярная проверка и резервное копирование и т. д.).
- Лишь незначительная часть требований ФСТЭК относятся к АБС. В целом, Diasoft FA# соответствует требованиям №152-ФЗ, требуются только доработки системы аудита и отчетности (для сохранения информации о полученных отчетах).
- Соблюдение требований законодательства по защите персональных данных в срок – **насущная необходимость и огромная комплексная задача** на стыке ответственности операторов ПДн и разработчиков ПП. Поэтому в компании открыт проект по 152-ФЗ, в рамках которого проводятся как общие информационные мероприятия, так и индивидуальные консультирования клиентов по решению вопросов 152-ФЗ.

# Ответственность операторов ПДн

## Юридические процедуры:

- Приведение внутренней нормативной базы и перестройка технологических процессов в соответствии с требованиями законодательства и нормативных документов
- Уведомление уполномоченного органа (Россвязькомнадзор) о намерении осуществлять обработку персональных данных.
- Получение согласия субъектов персональных данных на обработку их персональных данных.
- Аттестация по требованиям безопасности (получение аттестатов на системы и помещения)
- Получение лицензий ФСТЭК и ФСБ

## Технические процедуры:

- Идентификация информационных систем персональных данных. Формирование перечня ПДн, включая причины их обработки
- Классификация информационных систем персональных данных
- Построение модели угроз и определение необходимых мер по защите
- Документирование информационных систем
- Реализация системы защиты персональных данных

# Ответственность за нарушение законодательства в области защиты ПДн

## **Закон 152-ФЗ гласит:**

*«Глава 5. Контроль и надзор за обработкой персональных данных.*

*Статья 24. Ответственность за нарушение требований настоящего Федерального закона*

*Лица, виновные в нарушении требований настоящего Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность»*

## **Кто проверяет:**

*«Федеральная служба по надзору в сфере связи и массовых коммуникаций (Россвязькомнадзор) является федеральным органом исполнительной власти, осуществляющим ... функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных...»*

*На практике пока непонятно, какие меры воздействия будут применены к нарушителям по результатам проверок Россвязькомнадзором. Ожидается, что последствия будут аналогичны другим административным инспекциям – например, пожарным надзором (сначала - предписание на устранение нарушений, потом - приостановление деятельности оператора).*

# Но не все так плохо

**Ассоциация российских банков готовит письмо в Государственную Думу Федерального Собрания Российской Федерации и Правительство Российской Федерации с просьбой перенести сроки реализации требований Закона № 152-ФЗ на один год, а также:**

- уточнить некоторые положения Федеральных законов и привести в соответствие с законодательными требованиями положения подзаконных актов, устранив противоречия
- срочно создать рабочую группу по вопросам реализации Закона № 152-ФЗ с целью оперативного решения возникающих вопросов, в том числе выработать совместные рекомендации по реализации требований Закона № 152-ФЗ, исключая различные толкования его положений при практическом применении на местах
- обратить внимание на то, что при разработке требований по защите ПДн необходимо принять во внимание, что защита таких данных в значительной мере уже достигается существующими мерами обеспечения информационной безопасности, применяемыми в банках; разработанная нормативная база не учитывает специфику организаций банковской системы Российской Федерации.
- предложить поэтапную реализацию требований Закона № 152-ФЗ в срок до 01.01.2011 г.



## Рекомендуем

- Не рассчитывать на отмену или перенос сроков 152-ФЗ и с полной ответственностью приступать к приведению всей деятельности организации к требованиям законодательства
- Привлечь к работам по обследованию, классификации, аттестации и сертифицированию надежных партнеров, обладающих необходимыми кадровыми ресурсами и минимальным опытом в проведении данных работ
- Не игнорировать рекомендации поставщиков ПП
- «Держать руку на пульсе» текущих изменений законодательства в части защиты персональных данных



# **Спасибо за внимание!** **Ваши вопросы?**

Россия, 127018, Москва, ул. Полковная 3, стр. 14

Тел.: +7(495) 780 7575, 789 9339

Факс: +7(495) 780 7576, 789 9338

[info@diasoft.ru](mailto:info@diasoft.ru), [www.diasoft.ru](http://www.diasoft.ru)