



ФЗ 152: Что грозит и как этого избежать.

Практические решения по выполнению требований Федерального закона № 152-ФЗ "О персональных данных"

ЗАО «Научно-производственное предприятие
«Безопасные информационные технологии»

Сергей Юрьевич ЛЁВИН

ИТОГИ ДЕЯТЕЛЬНОСТИ РОСКОМНАДЗОРА (на октябрь 2010 г.)

С момента возложения на Роскомнадзор полномочий по защите прав субъектов персональных данных проведено 1327 проверок в области персональных данных, из них:

плановые проверки	– 886
внеплановые проверки	– 441

Результат:



**устранено свыше 3000 нарушений в области персональных данных
выдано 1 917 предписаний
составлено 1 633 протокола об АП
взыскано штрафов на сумму свыше 2 170 тыс. руб.**



I Общие положения Федерального закона № 152-ФЗ в части защиты персональных данных

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

ОСНОВНЫЕ ПОНЯТИЯ ЗАКОНА:

- **персональные данные** - любая информация, относящаяся к определенному физическому лицу;
- **оператор** - государственный или муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку ПДн, а также определяющие цели и содержание обработки персональных данных;
- **использование ПДн** - действия (операции) с ПДн, совершаемые оператором в целях принятия решений или совершения иных действий;
- **конфиденциальность ПДн** - обязательное для соблюдения оператором требование не допускать их распространения без согласия субъекта ПДн;
- **информационная система ПДн** - совокупность ПДн, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн



Существенные условия закона №152-ФЗ

- оператор до начала обработки ПДн **обязан уведомить уполномоченный орган** по защите прав субъектов ПДн о своем намерении осуществлять обработку ПДн;
- **операторами** и третьими лицами, получающими доступ к ПДн, **должна обеспечиваться конфиденциальность** таких данных, за исключением случаев обезличивания ПДн, а также в отношении общедоступных ПДн;
- оператор при обработке ПДн **обязан принимать** необходимые **организационные и технические меры для защиты ПДн** от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий



II Примерная структура подзаконных актов Федерального закона № 152-ФЗ

Примерная структурная схема нормативно-правового обеспечения требований по защите прав субъектов персональных данных в Российской Федерации

**Федеральный закон от 27 июля 2006 г.
№ 152-ФЗ «О персональных данных»**

Постановление Правительства РФ № 781 – 2007 г.
(Автоматизированная обработка)

Совместный приказ от 13 февраля 2008 г. N 55/86/20
ФСБ России, ФСТЭК России, Минкомсвязи России

Нормативно-методические
документы
ФСТЭК России

Нормативно-методические
документы
ФСБ России

Административ-
ный регламент
Роскомнадзора

Организационно-распорядительные документы
различных министерств и ведомств

Постановление
Правительства
РФ
№ 687 – 2008 г.
(Обработка БЕЗ
средств
автоматизации)

ФСБ России – орган уполномоченный осуществлять контроль и надзор за выполнением требований, установленных Правительством Российской Федерации

**Д
О
К
У
М
Е
Н
Т
Ы**

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

Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации

ФСТЭК России – орган уполномоченный осуществлять контроль и надзор за выполнением требований, установленных Правительством Российской Федерации

Документы

Положение о методах и способах защиты информации в информационных системах персональных данных

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных

Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных

Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

Уполномоченный орган по защите прав субъектов персональных данных Роскомнадзор

Д
О
К
У
М
Е
Н
Т

Административный регламент проведения проверок при осуществлении федерального государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных

По состоянию на 15 октября 2010 г. в Реестр включено более **138 тыс. операторов**, осуществляющих обработку персональных данных

В 2010 году в Роскомнадзор поступило **1 296 обращений** от физических и юридических лиц, из них:

- 360 (28 %) даны разъяснения положений ФЗ;
- 338 (26%) материалы направлены в прокуратуру;
- 456 (35%) факт нарушений не установлен;
- 142 (11 %) находятся на рассмотрении

Основные функции уполномоченного органа по защите прав субъектов ПДн, контролю и надзору за соответствием обработки ПДн

Роскомнадзор обязан:

- **организовывать защиту** прав субъектов персональных данных;
- **рассматривать жалобы** и обращения граждан или юридических лиц по вопросам, связанным с обработкой ПДн, а также принимать решения по результатам рассмотрения указанных жалоб и обращений;
- **вести реестр** операторов;
- **принимать** в установленном порядке **меры** по приостановлению или прекращению обработки персональных данных

Роскомнадзор имеет право:

- **запрашивать** и безвозмездно получать у физических или юридических лиц **информацию**, необходимую для реализации своих полномочий;
- **осуществлять проверку** сведений, содержащихся в уведомлении об обработке ПДн

Согласно № 359-ФЗ от 23 декабря 2010 г.

"О внесении изменения в статью 25 Федерального закона "О персональных данных""

"Информационные системы персональных данных, созданные до 1 января 2011 г., должны быть приведены в соответствие с требованиями настоящего Федерального закона не позднее 1 июля 2011 г."





III СОСТАВ РАБОТ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Оператор персональных данных, обязан:

Провести инвентаризацию информационных ресурсов, обрабатываемых в ИС и определить перечень обрабатываемых ПДн

Урегулировать правовые вопросы обработки (использования) ПДн

Оформить и направить в территориальный орган Роскомнадзора уведомление об обработке
(о намерении осуществлять обработку) ПДн

Провести классификацию ИС с оформлением соответствующего акта

Принять организационные и технические меры для обеспечения конфиденциальности ПДн в виде создаваемой системы (подсистемы) защиты ПДн

Получить (для операторов ИСПДн 1 и 2 класса) лицензию ФСТЭК России на деятельность по технической защите информации

Состав работ по созданию системы защиты персональных данных

Определение угроз безопасности ПДн их обработке, формирование на их основе модели угроз (на основании результатов комплексного обследования защищённости ИС)

Разработка (проектирование) СЗПДн соответствующего класса и оформление документации СЗПДн

Установка и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией, проверка их готовности к использованию и составление заключения о возможности их эксплуатации

Оценка соответствия (аттестация) ИСПДн требованиям безопасности согласно присвоенному классу

Обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними

Учёт лиц, допущенных к работе с ПДн в информационной системе, а также реализация иных организационных мер защиты



IV ВОЗМОЖНЫЕ САНКЦИИ

Уголовная ответственность за нарушение требований ФЗ «О персональных данных»

ст. 137 УК РФ – незаконное собирание и распространение сведений о частной жизни лица, составляющих его личную и семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении;

ст. 140 УК РФ – неправомерный отказ должностного лица в предоставлении документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации;

ст. 272 УК РФ – неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло за собой уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети

Административная ответственность за нарушение требований ФЗ «О персональных данных»

ст. 5.39 КОАП РФ – отказ в предоставлении гражданину документов и материалов, непосредственно затрагивающих права и свободы гражданина либо несвоевременное представление таких материалов, либо предоставление гражданину неполной или заведомо недостоверной информации;

ст. 13.11 КОАП РФ – нарушение установленного законом порядка сбора, хранения, использования и распространения персональных данных;

ст. 13.14 КОАП РФ – разглашение информации доступ к которой ограничен федеральным законом;

ст. 19.7 КОАП РФ – непредставление или несвоевременное представление уведомления об обработке персональных данных или иной информации по запросу уполномоченного органа.