

Требования нормативных правовых актов и нормативных документов в области обеспечения безопасности персональных данных

Основные нормативные правовые акты Российской Федерации, определяющие область деятельности и ответственность руководителей за организацию безопасности персональных данных

- Конституция Российской Федерации
- Кодекс РФ от 30 декабря 2001 г. № 195-ФЗ “Об административных правонарушениях”
- Трудовой кодекс РФ, принятый 30 декабря 2002г. ФЗ № 197-ФЗ, Гл.14
- Гражданский кодекс Российской Федерации 30 ноября 1994 г. № 51-ФЗ
- Федеральный закон от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»
- Федеральный закон от 27 июля 2006 г. № 149 – ФЗ «Об информации, информационных технологиях и защите информации»
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»
- Федеральный закон от 03 декабря 2008 г. № 242-ФЗ «О государственной геномной регистрации в Российской Федерации»
- Указ Президента РФ от 30 мая 2005 г. № 609 "Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»
- Указ Президента РФ от 17 марта 2008 № 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»
- Постановление Правительства РФ от 17 ноября 2007 г. № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных
- Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

- **Постановление Правительства РФ** от 6 июля 2008 г. № 512 «**Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных**»
- **Постановление Правительства РФ** от 21 марта 2012 г. № 211 «**Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами**»
- **Приказ ФСТЭК, ФСБ, Мининформсвязи** от 13 февраля 2008 года № 55/86/20 «**Об утверждении порядка проведения классификации информационных систем персональных данных**»
- **Приказ Россвязькомнадзора** от 28 марта 2008 г. № 154 «**Об утверждении положения о ведении реестра операторов, осуществляющих обработку персональных данных**»
- **Приказ Россвязькомнадзора** от 17 июля 2008 г. № 08 «**Об утверждении образца формы уведомления об обработке персональных данных**»
- **Приказ ФСТЭК России** от 5 февраля 2010 г. № 58 «**Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных**»
- **Методические материалы ФСТЭК** «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15.02.2008
- **Методические материалы ФСТЭК** «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15.02.2008
- **Методические материалы ФСБ** «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
- **Методические материалы ФСБ** «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

Основные понятия используемые в Федеральном законе «О персональных данных»

Федеральным законом «О персональных данных» регулируются отношения, связанные с обработкой ПДн, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами

(далее - государственные органы), органами местного самоуправления, иными муниципальными органами (далее - муниципальные органы), юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка ПДн без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

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

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

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

Угрозы безопасности персональным данным

В соответствии со статьей 19 Федерального закона №152-ФЗ угрозы безопасности ПДн при их обработке в ИСПДн могут быть связаны как с **непреднамеренными** действиями персонала ИСПДн и(или) потребителей, пользующихся услугами, предоставляемыми ИСПДн в соответствии с ее назначением, так и **со специально** осуществляемыми неправомерными действиями иностранных государств, криминальных сообществ, отдельных организаций и граждан.

Угрозы безопасности ПДн могут быть реализованы за счет утечки ПДн по техническим каналам (технические каналы утечки информации, обрабатываемой в технических средствах ИСПДн, технические каналы перехвата информации при ее передаче по каналам связи, технические каналы утечки акустической (речевой) информации) либо за счет несанкционированного доступа (НСД) с использованием соответствующего программного обеспечения.

Источниками угроз, реализуемых за счет НСД к базам данных с использованием штатного или специально разработанного программного обеспечения, являются субъекты, действия которых

нарушают регламентируемые в ИСПДн правила разграничения доступа к информации. Этими субъектами могут быть:

нарушитель; носитель вредоносной программы; аппаратная закладка.

Под нарушителем понимается физическое лицо (лица), случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности ПДн при их обработке техническими средствами в информационных системах.

С точки зрения наличия права легального доступа в помещения, в которых размещены аппаратные средства, обеспечивающие доступ к ресурсам ИСПДн, нарушители подразделяются на два типа:

внешние нарушители - нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена;

внутренние нарушители - нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн.

Основные требования по обеспечению безопасности персональных данных

Меры по обеспечению оператором безопасности ПДн:

назначение оператором ответственного за организацию обработки персональных данных;

издание оператором документов, определяющих политику оператора в отношении обработки ПДн, локальных актов по вопросам обработки ПДн, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений;

применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со [статьей 19](#) ФЗ № 152;

осуществление внутреннего контроля и (или) аудита соответствия обработки ПДн ФЗ № 152 и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, политике оператора в отношении обработки ПДн, локальным актам оператора;

оценка вреда, который может быть причинен субъектам ПДн в случае нарушения настоящего ФЗ;

ознакомление работников оператора, непосредственно осуществляющих обработку ПДн, с положениями законодательства РФ о ПДн, в том числе требованиями к защите ПДн, документами, определяющими политику оператора в отношении обработки ПДн, локальными актами по вопросам обработки ПДн, и (или) обучение указанных работников.

Федеральный закон «О персональных данных» (статья 19)

Обеспечение безопасности персональных данных достигается:

определением угроз безопасности ПДн при их обработке в ИСПДн;

применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн установленные Правительством РФ;

применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;

учетом машинных носителей ПДн;

обнаружением фактов несанкционированного доступа к ПДн принятием мер;

восстановлением ПДн, модифицированных или уничтоженных вследствие НСД к ним;

установлением правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;

контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

Постановление Правительства РФ от 17 ноября 2007 г. № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты ПДн, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных)

Информационные системы **классифицируются** государственными органами, муниципальными органами, юридическими или физическими лицами, организующими и (или) осуществляющими обработку персональных данных

Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с ПДн, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей ПДн и средств защиты информации, а

также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе оператором или уполномоченным лицом может назначаться структурное подразделение или должностное лицо (работник), ответственные за обеспечение безопасности персональных данных.

Мероприятия по обеспечению безопасности ПДн их обработке в информационных системах включают в себя:

- а) определение угроз безопасности ПДн при их обработке, формирование на их основе модели угроз;
- б) разработку на основе модели угроз системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса информационных систем;
- в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
- г) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;
- д) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
- е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- ж) учет лиц, допущенных к работе с персональными данными в информационной системе;
- з) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей ПДн, использования средств защиты информации, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
- к) описание системы защиты персональных данных.

**Постановление Правительства РФ от 15 сентября 2008 г. №
687 «Об утверждении положения об особенностях
обработки персональных данных, осуществляемой без
использования средств автоматизации»**

Обработка ПДн, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором.

**Постановление Правительства РФ от 21 марта 2012 г. №
211 «Об утверждении перечня мер, направленных на
обеспечение выполнения обязанностей,
предусмотренных Федеральным законом «О
персональных данных» и принятыми в соответствии с ним
нормативными правовыми актами, операторами,
являющимися государственными или муниципальными
органами**

Операторы, являющиеся государственными или муниципальными органами, принимают следующие меры, направленные на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами:

назначают ответственного за организацию обработки персональных данных в государственном или муниципальном органе **из числа служащих данного органа;**

при эксплуатации ИСПДн , принимают правовые, организационные и технические меры по обеспечению безопасности ПДн при их обработке, предусмотренные соответствующими нормативными правовыми актами, для выполнения установленных Правительством РФ требований к защите ПДн при их обработке;

при обработке ПДн, осуществляемой без использования средств автоматизации, **выполняют требования**, установленные постановлением Правительства РФ от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";

в целях осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям организуют проведение периодических проверок условий обработки ПДн. Проверки осуществляются ответственным за организацию обработки ПДн либо комиссией, образуемой

руководителем государственного или муниципального органа. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, руководителю государственного или муниципального органа докладывает ответственный за организацию обработки ПДн в государственном или муниципальном органе либо председатель комиссии;

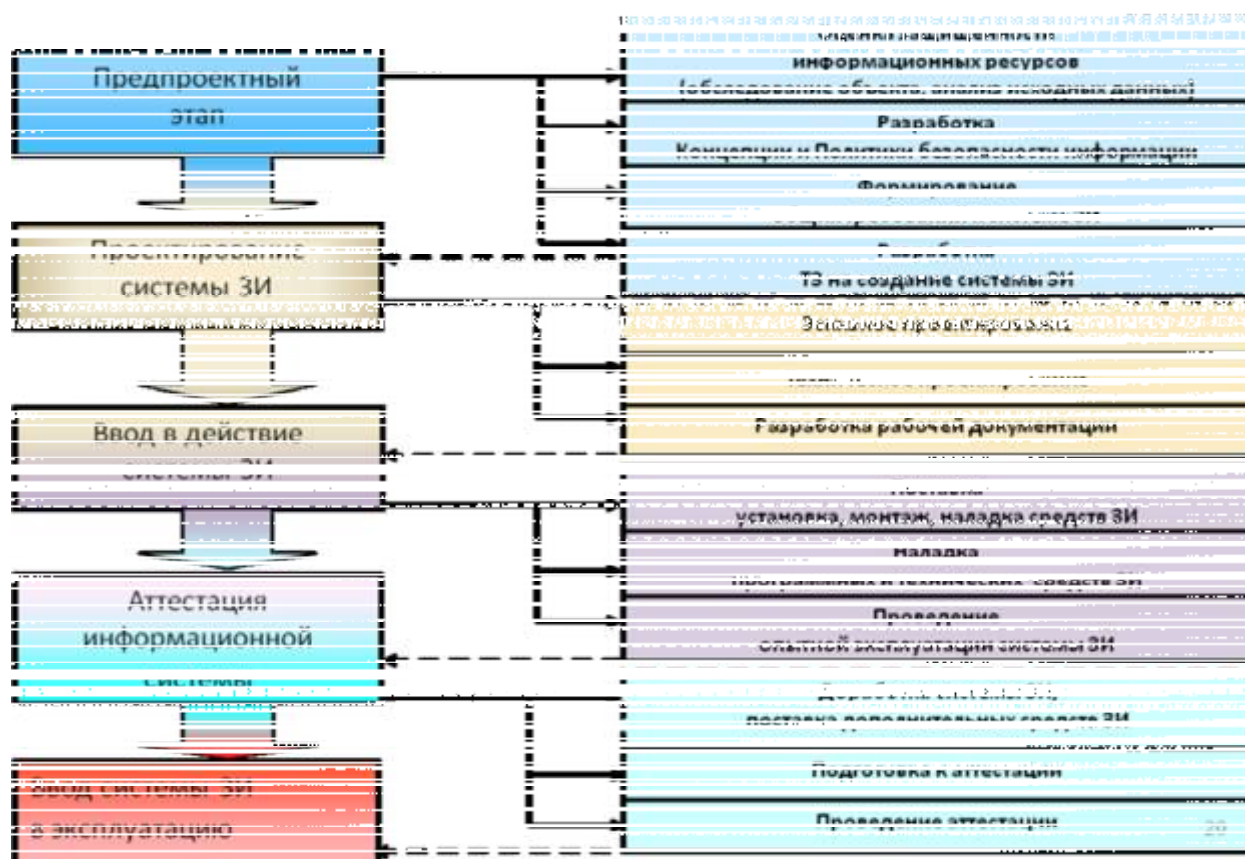
осуществляют ознакомление служащих, непосредственно осуществляющих обработку ПДн, с положениями законодательства РФ о ПДн (в том числе с требованиями к защите ПДн), локальными актами по вопросам обработки ПДн и (или) организуют обучение указанных служащих;

уведомляют уполномоченный орган по защите прав субъектов ПДн об обработке (намерении осуществлять обработку) ПДн, за исключением случаев, установленных Федеральным законом "О персональных данных";

согласно требованиям и методам, установленным уполномоченным органом по защите прав субъектов ПДн, осуществляют обезличивание ПДн, обрабатываемых в ИСПДн, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ.

Документы, определяющие политику в отношении обработки персональных данных, подлежат опубликованию на официальном сайте государственного или муниципального органа в течение 10 дней после их утверждения.

Основные этапы и содержание работ по созданию системы защиты персональных данных при их обработке в информационных системах



Организационные мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах

Назначить ответственного за организацию обработки и защиту персональных данных (ПДн)
Ввести режим защиты ПДн (Приказ)
Организовать учет обращений субъектов персональных данных (журнал)
Разработать Концепцию информационной безопасности
Разработать Политику информационной безопасности
Разработать перечень персональных данных, подлежащих защите (перечень)
Определить ответственность лиц участвующих в обработке ПДн (приказ)
Определить перечень лиц участвующих в обработке персональных данных (перечень)
Организовать доступ пользователей ИСПДн, необходимых для выполнения должностных обязанностей (ма
Провести классификацию, выявленных ИСПДн (Акт классификации ИСПДн)

Определить актуальные угрозы безопасности персональным данным (Модель угроз безопасности ПДн)
Определить контролируемую зону вокруг ИСПДн (План контролируемой зоны)
Организовать режим охраны и контроля доступа в помещения, в которых установлены аппаратные средства защиты
Организовать работу и разработать инструкции: по организации резервного копирования защищаемой информации; по организации восстановления работоспособности технических средств, ПО, баз данных ; по порядку формирования и хранения паролей; о порядке обработки ПДн и обеспечении введенного режима защиты ПДн; о порядке работы с ПДн; о порядке пользования и (или) международного обмена; о действии в случае возникновения внештатных ситуаций;
Организовать информирование и обучение сотрудников о порядке обработки и защиты ПДн (журнал ознакомления)
Организовать учет технических средств и средств защиты, а так же документации к ним (журнал учёта)
Определить порядок проведения внутренних проверок состояния защиты ПДн (Положение, журнал учёта проверок)
Направить Уведомление о начале обработки ПДн в Роскомнадзор
Организация планирования работ по защите персональных данных (План работы)

Постановление Правительства РФ от 21 марта 2012 г. № 211

Актом руководителя государственного или муниципального органа **утверждаются** следующие документы:

правила обработки ПДн, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства РФ в сфере ПДн, а также определяющие для каждой цели обработки ПДн содержание обрабатываемых ПДн, категории субъектов, ПДн которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований;

правила рассмотрения запросов субъектов ПДн или их представителей;

правила осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн;

правила работы с обезличенными данными;

перечень информационных систем персональных данных;

перечни ПДн, обрабатываемых в связи с реализацией трудовых отношений, а также в связи с оказанием государственных или муниципальных услуг и осуществлением государственных или муниципальных функций;

перечень должностей служащих, ответственных за проведение мероприятий по обезличиванию обрабатываемых ПДн;

перечень должностей служащих, замещение которых предусматривает осуществление обработки ПДн либо осуществление доступа к ПДн;

должностная инструкция ответственного за организацию обработки ПДн;

типовое обязательство служащего, непосредственно осуществляющего обработку ПДн, в случае расторжения с ним контракта прекратить обработку ПДн, ставших известными ему в связи с исполнением должностных обязанностей;

типовая форма согласия на обработку ПДн служащих, иных субъектов ПДн, а также типовая форма разъяснения субъекту ПДн юридических последствий отказа предоставить свои персональные данные;

порядок доступа служащих государственного или муниципального органа в помещения, в которых ведется обработка персональных данных.

Мероприятия по обеспечению физической защиты персональных данных при их обработке в информационных системах

- Установка **жалюзи (штор)** на окна в помещениях, где осуществляется работа с ПДн
- Установка **замков на дверях** в помещениях с аппаратными средствами ИСПДн
- Установка пожарно-охранной **сигнализации**
- Выставление **поста охраны** для пропуска в контролируемую зону
- Установка **технической системы контроля** доступа в контролируемую зону и помещения (по э. биометрическим данным и т.п.)
- Установка системы **видеонаблюдения**
- Осуществлять **сдачу под охрану помещений**, в которых находятся средства, обрабатывающие ПДн
- Установка **решеток на окнах** первого и последнего этажей здания
- Установка **систем кондиционирования** в помещениях, где расположены аппаратные средства ИСПДн
- Установка систем **бесперебойного питания** на ключевые элементы ИСПДн
- Установка **резервных (дублирующих) технических средств** ключевых элементов ИСПДн

Мероприятия по технической защите персональных данных при их обработке в информационных системах

- Проведение **проектирования системы** защиты информации в ИСПДн
- Установка **средств защиты информации** от утечки по техническим каналам и от несанкционированного доступа
- Создание **единого хранилища** зарегистрированных действий пользователей с ПДн
- Разработка **подсистемы управления** доступом, регистрации и учета
- Установка **программных средств** антивирусной защиты
- Создание **электронного журнала** регистрации обращений пользователей информационной системы
- Установка **межсетевого экранирования** (по необходимости)
- Реализация **разрешительной системы допуска** пользователей (обслуживающего персонала) к информации
- Установка **подсистемы анализа защищенности**
- Реализация **резервирования** технических средств, **дублирования** массивов и носителей информации
- Установка **подсистемы обнаружения вторжений**
- Установка средств **криптографической защиты** информации (по необходимости)
- **Описание системы** защиты персональных данных
- Проведение **оценки соответствия** СЗИ ИСПДн требованиям законодательства РФ

Мероприятия по контролю состояния защиты персональных данных при их обработке в информационных системах

- Проведение **внутреннего контроля** (аудита) состояния защиты ПДн
- **Контроль** за соблюдением **режима обработки** ПДн
- **Контроль** за соблюдением **режима защиты** ПДн
- **Контроль** за выполнением мероприятий **антивирусной защиты**

- **Контроль** за соблюдением режима **защиты при подключении к сетям общего пользования и (или)**
- **Контроль** за **обновлениями** программного обеспечения и **единообразия** применяемого ПО на всех
- **Контроль** за обеспечением **резервного копирования**
- Организация **анализа и пересмотра** имеющихся **угроз** безопасности ПДн, а так же **прогнозирование** неизвестных, угроз
- Поддержание в **актуальном состоянии** нормативно-организационных **документов**
- **Контроль** за разработкой и внесением **изменений в программное обеспечение** собственной специально дорабатываемое собственными разработчиками или сторонними организациями.

Ответственность за не выполнение требований нормативных актов и нормативных документов в области обеспечения безопасности персональных данных

Кодекс РФ об административных правонарушениях от 30.12.2001 № 195-ФЗ

Статья 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)
Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) - влечет предупреждение или наложение административного штрафа на должностных лиц - от пятисот до одной тысячи рублей; **на юридических лиц - от пяти тысяч до десяти тысяч рублей.**

Статья 13.12.
Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации - на должностных лиц - от одной тысячи до двух тысяч рублей; **на юридических лиц - от десяти тысяч до двадцати тысяч рублей с конфискацией несертифицированных средств защиты информации или без таковой.**

Статья 19.5.

Невыполнение в установленный срок законного предписания (постановления, представления, решения) органа (должностного лица), осуществляющего государственный надзор (контроль), об устранении нарушений законодательства – влечет наложение административного штрафа на

должностных лиц - от одной тысячи до двух тысяч рублей или дисквалификацию на срок до трех лет; **на юридических лиц - от десяти тысяч до двадцати тысяч рублей.**

Статистическая справка

По данным Роскомнадзора, всего с момента возложения на эту организацию полномочий по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации нами (т.е. с ноября 2007 года) проведено 3307 проверок.

Результатами этих проверок стали более чем 4500 предписаний об устранении выявленных нарушений, и 7591 протокол об административных правонарушениях.

В 2011 году проведено 1743 проверки.

По результатам проверок в 2011 году в прокуратуру было передано около 900 материалов.

Сумма взысканных штрафов составила более 12,5 миллионов рублей. При этом средний размер штрафа не так уж и велик и составляет 3-5 тысяч рублей.

Источник: [сайт Роскомнадзора](#).