ЭЛВИС-ПЛЮС

Федеральный закон «О персональных данных»: ближайшие перспективы применения и развития

(комментарии и рекомендации)

ЭЛВИС-ПЛЮС

ПРОЛОГ

Конституция РФ (1993 г.), Статья 23

1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

Статья 24

1. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

19 декабря 2005 г. РФ ратифицировала (ФЗ № 160-ФЗ) «Европейскую конвенцию о защите физических лиц при автоматизированной обработке персональных данных»
(Страсбург, 28 января 1981 г., с изменениями от 15.06.1999 г.)

По оценкам Роскомнадзора на сегодняшний день требования Закона касаются более 7 млн. организаций-операторов.

ЭЛВИС-ПЛЮС

СОСТОЯНИЕ НОРМАТИВНОЙ БАЗЫ ПО ЗАЩИТЕ ПДн на 10.12.2009 г. (более 25 д-тов)

1. ФЗ 2006 г. № 152-ФЗ «О персональных данных».
2. ФЗ 2006 г. № 149-ФЗ «Об информации, информатизации и защите информации».
3. 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».
4. Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
5. 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».
6. Нормативно- методические документы уполномоченных федеральных органов.

ЭЛВИС-ПЛЮС

Требования ФЗ «О персональных данных»

Принципы обработки ПДн (ст. 5)

1. Обработка персональных данных должна осуществляться на основе ***принципов***:

1) законности целей и способов обработки ПДн и добросовестности;

2) соответствия целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям оператора;

3) соответствия объема и характера обрабатываемых ПДн, способов обработки персональных данных целям обработки персональных данных;

4) достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки ПДн, избыточных по отношению к целям, заявленным при сборе персональных данных;

5) недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

2. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и они ***подлежат уничтожению*** по достижении целей обработки или в случае утраты необходимости в их достижении.

ЭЛВИС-ПЛЮС

Требования ФЗ «О персональных данных»

Условия обработки ПДн (ст. 6)

1. Обработка ПДн может осуществляться оператором ***с согласия субъектов ПДн,*** за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Согласие субъекта ПДн, не требуется в следующих случаях:

1) обработка ПДн осуществляется ***на основании ФЗ***, устанавливающего её цель, условия получения ПДн и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;

2) обработка ПДн осуществляется ***в целях исполнения договора, одной из сторон которого является субъект персональных данных***;

3) Других случаях, предусмотренных ФЗ.

4. В случае, если оператор на основании договора поручает обработку персональных данных другому лицу, ***существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.***

ЭЛВИС-ПЛЮС

Случаи, когда в обязательном порядке требуется наличие согласия в письменной форме

1. При обработке специальных категорий ПДн (Ст. 10).

2. При обработке биометрических персональных данных (Ст. 11).

3. При включении ПДн субъекта в общедоступные источники персональных данных (в том числе справочники, адресные книги и т.п.) (Ст. 8).

4. При необходимости трансграничной передачи ПДн на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов ПДн (Ст. 22).

5. В случае принятия решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы на основании исключительно автоматизированной обработки его ПДн (Ст. 16).

ЭЛВИС-ПЛЮС

Требования ФЗ «О персональных данных»

Обеспечение конфиденциальности ПДн (ст. 7)

1. Операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением случаев, предусмотренных частью 2 статьи 7:

2. Обеспечение конфиденциальности персональных данных не требуется:

1) в случае обезличивания персональных данных;

2) в отношении общедоступных персональных данных.

ЭЛВИС-ПЛЮС

Требования ФЗ «О персональных данных»

Обеспечение безопасности ПДн (ст. 19)

1. Оператор при обработке ПДн ***обязан принимать необходимые организационные и технические меры***, в том числе использовать шифровальные (криптографические) средства, *для защиты ПДн* от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий.

2. Правительство РФ устанавливает требования к обеспечению безопасности ПДн при их обработке в ИСПДн, требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне ИСПДн.

4. Использование и хранение биометрических ПДн вне ИСПДн могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения.

ЭЛВИС-ПЛЮС

Требования ФЗ «О персональных данных»

Сроки реализации требований закона (ст. 25)

После дня вступления в силу Федерального закона ***(26.01.2007 г.)*** обработка персональных данных, включенных в информационные системы персональных данных до дня его вступления в силу, осуществляется в соответствии с Федеральным законом.

Информационные системы персональных данных, созданные до дня вступления в силу Федерального закона, должны быть приведены в соответствие с требованиями настоящего Федерального закона ***не позднее 1 января 2010 года***.

ЭЛВИС-ПЛЮС

НОРМАТИВНО-МЕТОДИЧЕСКАЯ БАЗА РЕГУЛЯТОРОВ (1)

1. Порядок проведения классификации информационных систем персональных данных. Совместный приказ ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20. Зарегистрирован в Минюсте России 3 апреля 2008 года, регистрационный № 11462.

ФСТЭК России

2. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.

3. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 14 февраля 2008 г.

4. Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены заместителем директора ФСТЭК России 15 февраля 2008 г.

5. Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных. Утверждены заместителем директора ФСТЭК России 15 февраля 2008 г.

НОРМАТИВНО-МЕТОДИЧЕСКАЯ БАЗА РЕГУЛЯТОРОВ (2)

ФСБ России

6. 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. № 149/6/6-622, 2008 г., ФСБ России.

7. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. № 149/54-144, 2008 г. ФСБ России.

ЭЛВИС-ПЛЮС

Защищать или нет персональные данные?

- Обязанность операторов обеспечить защиту обрабатываемых ПДн установлена ФЗ «О персональных данных», принятие которого обусловлено вхождением России в цивилизованный мир.
- В цивилизованных странах мира (35 европейских стран), США, Канаде и др. с начала – середины 80-х годов действуют аналогичные требования по обеспечению приватности частной жизни.
- Непринятие адекватных мер защиты ПДн создаёт существенные проблемы при взаимодействии с западными партнёрами.
- Выбор стратегии административной ответственности - опасный путь для оператора – т.к. планируется существенное усиление административной ответственности.

ЭЛВИС-ПЛЮС

Базовые принципы (парадигма) защиты персональных данных

Требуемый уровень безопасности персональных данных при их обработке в ИС достигается обеспечением:

- Локализации персональных данных.
- Счётности субъектов и объектов ИС.
- Доверенности конфигурации и настроек ИС.
- Целостности всех элементов ИС.
- Подконтрольности всех действий субъектов.
- Документированности всех событий в ИС.

ЭЛВИС-ПЛЮС

Методы защиты ПДн

- **Правовые**
  - ✓ правовая регламентация порядка сбора, использования, предоставления и уничтожения ПДн;
  - ✓ распределение полномочий между субъектами;
  - ✓ нормативно-правовой контроль использования ПДн;
  - ✓ установление ответственности за нарушения.
- **Организационно-административные**
  - ✓ формирование системы управления ПДн;
  - ✓ регламентация деятельности персонала по использованию ПДн;
  - ✓ регламентация порядка взаимодействия пользователей и администраторов ИС;
  - ✓ контроль за деятельностью персонала.
- **Технические (аппаратно-программные и др.)**
  - ✓ идентификация и аутентификация пользователей;
  - ✓ разграничение и контроль доступа к ПДн;
  - ✓ обеспечение целостности ПДн;
  - ✓ регистрация событий безопасности;
  - ✓ защита каналов передачи ПДн.

ЭЛВИС-ПЛЮС

ОБЯЗАННОСТИ ОПЕРАТОРОВ
Что надо сделать?

- Провести инвентаризацию ИР, определить перечень ПДн.
- Урегулировать правовые вопросы обработки ПДн.
- Провести обследование ИС с целью оценки текущего состояния ИБ и определения необходимых ИД для создания СЗПДн;
- Разработать модель угроз безопасности ПДн.
- Провести классификацию ИСПДн.
- Направить (при необходимости) в Роскомнадзор уведомление о намерении осуществлять обработку ПДн.
- *Получить лицензию на деятельность по ТЗКИ (не для всех).*
- Определить требования по защите ПДн.
- Спроектировать Систему защиты ПДн и реализовать проект.
- Провести оценку соответствия ИСПДн требованиям.
- Организовать контроль соблюдения использования СЗИ.

ЭЛВИС-ПЛЮС

С чего начать ?

Разработка внутренних нормативных актов организации

Положение об обработке персональных данных

- Правовые основания обработки ПДн.
- Цели обработки персональных данных.
- Категории и перечень обрабатываемых персональных данных.
- Категории субъектов персональных данных.
- Перечень действий с персональными данными.
- Порядок предоставления персональных данных.
- Дата начала обработки, срок или условие её прекращения.
- Основания и порядок уничтожения персональных данных.
- Форма согласия субъекта персональных данных на их обработку.
- Обязанности персонала при обработке персональных данных.

ЭЛВИС-ПЛЮС

Как строить систему защиты ?

- Мероприятия по защите ПДн должны сочетать реализацию ***правовых***, ***организационных*** и ***технических*** мер защиты.
- Состав мероприятий зависит от класса ИСПДн и результатов моделирования угроз.
- Для защиты должны использоваться рекомендованные СЗИ (***www.fstec.ru***).
- Мероприятия по защите ПДн реализуются в рамках подсистем:
  - ✓ **управления доступом**
  - ✓ **регистрации и учёта**
  - ✓ **обеспечения целостности**
  - ✓ **антивирусной защиты**
  - ✓ криптографической защиты (*при необходимости*)
  - ✓ обнаружения вторжений (*при необходимости*)
  - ✓ защиты от утечки за счёт ПЭМИН (*для ИС 1 и 2 классов*)

Все мероприятия одинаково значимы, а невыполнение одних сводит на нет результаты реализации других

ЭЛВИС-ПЛЮС

Как оценить достаточность защиты ?

- ***Обязательно:*** **для ИСПДн 1 и 2 класса и специальных ИСПДн – сертификация (аттестация).**
- ***По решению оператора:*** **для ИСПДн 3 класса – декларирование соответствия или сертификация (аттестация).**
- ***По решению оператора:*** **для ИСПДн 4 класса – оценка соответствия.**

Аттестация – официальное подтверждение наличия на объекте защиты необходимых и достаточных условий, обеспечивающих выполнение установленных требований

Правом проведения аттестации и выдачи аттестатов соответствия обладают лицензиаты, имеющие лицензию на деятельность по технической защите конфиденциальной информации

(по постановлению Правительства РФ 2006 г. № 504)

ЭЛВИС-ПЛЮС

Государственный контроль и надзор выполнения требований по обеспечению безопасности персональных данных

Обеспечение контроля и надзора ***за соответствием обработки персональных данных требованиям Федерального закона*** возлагается на федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи ***(Роскомнадзор).***

(Ст. 23, ч. 1 ФЗ № 152)

Контроль и надзор ***за выполнением технических требований*** по защите ПДн осуществляются ***ФСБ России*** и ***ФСТЭК России*** в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в ИСПДн.

(Ст. 19, ч. 3 ФЗ № 152)

ЭЛВИС-ПЛЮС

Проверяемые вопросы

(В соответствии с проектом Административного регламента Роскомнадзора)

- Рассмотрение документов Оператора, включающих сведения:
  - ✓ содержащиеся в уведомлении об обработке ПДн;
  - ✓ изложенные в обращениях граждан;
  - ✓ о выполнении предписаний об устранении ранее выявленных нарушений;
  - ✓ о наличии письменного согласия субъекта персональных данных на обработку его персональных данных;
  - ✓ о соблюдении требований законодательства РФ при обработке специальных категорий и биометрических ПДн;
  - ✓ о порядке и условиях трансграничной передачи ПДн;
  - ✓ о порядке обработки ПДн, осуществляемой без использования средств автоматизации;
  - ✓ о соблюдении требований конфиденциальности при обработке ПДн;
  - ✓ о фактах уничтожения ПДн по достижении цели обработки;
- Анализ локальных актов оператора, регламентирующих порядок и условия обработки ПДн.
- Обследование ИСПДн, в части касающейся обрабатываемых в ней ПДн.

ЭЛВИС-ПЛЮС

Примерный перечень документации Оператора

- Уведомление об обработке ПДн.
- Положение о порядке обработки ПДн.
- Положение о подразделении, осуществляющем функции по организации защиты ПДн.
- Приказ о назначении ответственных лиц по работе с ПДн.
- Должностные регламенты лиц, осуществляющих обработку ПДн.
- Типовые формы документов, содержащих ПДн.
- Договоры с субъектами ПДн, лицензии на виды деятельности, в рамках которых осуществляется обработка персональных данных.
- Приказы об утверждении мест хранения материальных носителей ПДн.
- Письменное согласие субъектов персональных данных на обработку их персональных данных (типовая форма).
- Справки о постановке на балансовый учёт ПЭВМ, на которых осуществляется обработка ПДн.
- Журналы (реестры, книги) содержащие ПДн, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится Оператор, или в иных аналогичных целях.
- Заключения экспертизы (сертификаты) ФСБ России, ФСТЭК России на СЗИ.
- Приказ о создании комиссии и акты проведения классификации ИСПДн.
- Акты об уничтожении ПДн субъекта(ов) (в случае достижения цели обработки).
- Планы мероприятий по защите ПДн и внутренних проверок состояния защиты ПДн.
- Журналы (книги) учёта обращений граждан (субъектов ПДн).
- Журнал учёта проверок (Приказ Минэкономразвития России №141 от 30.4.2009).

ЭЛВИС-ПЛЮС

Документация системы защиты (СЗПДн)

- Положение по организации и проведению работ по обеспечению безопасности ПДн при их обработке в ИСПДн.
- Модель угроз безопасности персональных данных.
- Акт классификации ИСПДн.
- Требования по обеспечению безопасности ПДн при их обработке в ИСПДн.
- Описание системы защиты персональных данных.
- Перечень применяемых средств защиты информации.
- Заключение о возможности эксплуатации средств защиты информации (разрабатывается по результатам проверки готовности к использованию СЗИ) (Аналог приёмо-сдаточной документация на СЗИ).
- Правила пользования средствами защиты информации, предназначенными для обеспечения безопасности персональных данных.
- Рекомендации (инструкции) по использованию программных и аппаратных средств защиты информации.
- Список лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей (утверждается оператором или уполномоченным лицом).
- Должностные инструкции персоналу ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн.

ЭЛВИС-ПЛЮС

ПЕРСПЕКТИВЫ СОВЕРШЕНСТВОВАНИЯ ЗАКОНОДАТЕЛЬСТВА О ПДн

Направления совершенствования законодательства

- Внесение ряда изменений в ФЗ «О персональных данных».
- Принятие ФЗ «О внесении изменений в некоторые законодательные акты РФ в связи с принятием ФЗ «О ратификации Конвенции Совета Европы» и ФЗ «О персональных данных» *(более чем в 23 ФЗ).*
- Внесение изменений в ФЗ 2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности» в части ограничения лицензируемого вида деятельности по технической защите КИ ***деятельностью по предоставлению услуг по технической защите информации конфиденциальной информации.***
- Усиление ответственности оператора в случае нарушения прав субъектов персональных данных;
- Приведение в соответствие с ФЗ нормативных правовых актов Правительства РФ и нормативных актов федеральных органов исполнительной власти.

ЭЛВИС-ПЛЮС

Планируемые изменения в ФЗ «О персональных данных»

- Закрепление права оператора определять сроки хранения и уничтожения ПДн в соответствии с условиями договора с субъектом персональных данных (ст. 5, 21).
- Уточнение перечня случаев, когда согласие субъекта на обработку его персональных данных не требуется (ч. 2 ст. 6).
- Расширение перечня случаев, когда обеспечение конфиденциальности ПДн не требуется (ст. 7).
- Уточнение порядка и сроков уничтожения ПДн с учетом возможности прекращения доступа к персональным данным и последующим их уничтожением (ст. 21).
- Уточнение перечня случаев, когда оператор вправе осуществлять обработку ПДн без уведомления уполномоченного органа по защите прав субъектов ПДн.

ЭЛВИС-ПЛЮС

Стратегия реализации технических требований (ст. 19 ФЗ)

- Расширение полномочий оператора по выбору методов и средств обеспечения безопасности обработки персональных данных.
- Сужение сферы исполнения обязательных требований и большей публичности при их подготовке.
- Исключение требования об обязательном использовании шифровальных (криптографических) средств защиты.
- Централизованная разработка отраслевых методических рекомендации по обеспечению безопасности ПДн.
- Уточнение полномочий государственных регуляторов.
- Перенос сроков приведения ИСПДн в соответствие с требованиями ФЗ на 1 год (не позднее 1.01.2011).

ЭЛВИС-ПЛЮС

Усиление административной ответственности

Предложения Роскомнадзора в КоАП

Статья 13.11. «Несоблюдение требований к обеспечению безопасности персональных данных»

Влечет наложение административного штрафа:

на должностных лиц – от пятидесяти до ста тысяч рублей;

на юридических лиц – от ***пятисот тысяч*** до ***1 млн. руб.*** или адм. приостановление деятельности на срок ***до 90 суток.***

Статья 13.30. «Обработка ПДн в ИСПДн, не соответствующих требованиям законодательства РФ в области ПДн» ***повлекшее за собой нарушение прав и законных интересов субъектов персональных данных***

Влечет наложение административного штрафа:

на должностных лиц – от двадцати до пятидесяти тысяч руб.;

на юридических лиц – от ***пятисот тысяч*** до ***1 млн. руб***. или адм. приостановление деятельности на срок ***до 90 суток.***

ЭЛВИС-ПЛЮС

Вопросы?

124460, МОСКВА, Зеленоград,
Центральный проспект, 11
тел. 777-42-92,
факс 531-8863
http://www.elvis.ru

ЭЛВИС-ПЛЮС

Спасибо за внимание !

**124498, Москва, Зеленоград,
проезд 4806, д.5, стр.23
тел. (495) 276-02-11,
факс (499) 731-24-03
http://www.elvis.ru**