ФЗ №152
«О персональных данных»

КАЛИНИНГРАД 2012

Мишина,3
992299
bit39.ru

БЮРО iT

Цель настоящего Федерального закона

- Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Основные понятия, используемые в настоящем Федеральном законе

- **Персональные данные** - любая информация, относящаяся к определенному 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;
- **Оператор персональных данных** - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных.
- **Информационная система персональных данных** - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также технических средств, позволяющих осуществлять обработку таких персональных данных.

ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

- 1) Соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;
- 2) Соответствия объема и характера обрабатываемых персональных данных, целям обработки персональных данных;
- 3) Достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

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.

Безопасность персональных данных

Целостность

Конфиденциальность

Доступность

Мишина,3
99 22 99
bit39.ru
БЮРО IT

Конфиденциальность персональных данных

Операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, путем регламентированного допуска к их обработке.

Обеспечения конфиденциальности персональных данных не требуется:

1) в случае обезличивания персональных данных;

2) в отношении общедоступных персональных данных.

Мишина,3
99 22 99
bit39.ru
БЮРО IT

Общедоступные источники персональных данных

1. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.
2. Сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

Согласие субъекта персональных данных на обработку своих персональных данных

фамилию, имя, отчество, адрес субъекта, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;

перечень персональных данных, на обработку которых дается согласие субъекта;

цель обработки персональных данных;

перечень действий с персональными данными, на совершение которых дается согласие;

срок, в течение которого действует согласие, а также порядок его отзыва.

Специальные категории персональных данных

персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни

- субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;
- персональные данные являются общедоступными;

Категории персональных данных

категория 1

персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

категория 2

персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию;

категория 3

персональные данные, позволяющие идентифицировать субъекта персональных данных;

категория 4

обезличенные и (или) общедоступные персональные данные.

Классы Информационных систем персональных данных

- **класс 1 (К1)** - информационные системы, для которых нарушение безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных;
- **класс 2 (К2)** - информационные системы, для которых нарушение безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных;
- **класс 3 (К3)** - информационные системы, для которых нарушение безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных;
- **класс 4 (К4)** - информационные системы, для которых нарушение безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.

Число субъектов Персональных Данных		меньше 1000	от 1000 до 100 000	свыше 100 000
ИСПдн	Категория 4	к4	к4	к4
	Категория 3	к3	к3	к2
	Категория 2	к3	к2	к1
	Категория 1	к1	к1	к1

Типовые ИСПДн

информационные системы, в которых требуется обеспечить только конфиденциальность ПДн.

Тип ИСП Дн

Специальные ИСПДн

информационные системы, в которых кроме конфиденциальности необходимо обеспечить еще хотя бы одну характеристику безопасности персональных данных (целостность, доступность)

К специальным системам относятся все ИСПДн, обрабатывающие данные о здоровье субъектов и ИСПДн, в которых предусмотрено принятие решений порождающих для субъекта юридические последствия на основании автоматизированной обработки.

Большинство существующих ИСПДн - специальные. Это связано с тем, что кроме конфиденциальности также важно, чтобы ПДн были всегда доступны для обработки, целостны и достоверны. Для всех специальных систем необходимо разработать **«Частную модель угроз».**

ЧАСТЬ 2

ПРИВЕДЕНИЕ ИСПДН В СОСТОЯНИЕ СООТВЕТСТВИЯ С ФЗ -152

Мишина,3
992299
bit39.ru

БЮРО IT

Этапы построения защищенной ИСПДн:

Правовой

Международное и федеральное законодательство В сфере защиты информации

Организационный

Исследование и документирование процессов обработки информации в ИСПДн

Инженерно-технический

Принятие соответствующих мер технического, режимного характера. Внедрение средств Физической и программной защиты персональных данных.

Правовой этап

Основные международные законодательные акты

1. Конвенция совета Европы от 28 января 1981 года «О защите личности в связи с автоматической обработкой персональных данных» (ратифицирована ФЗ №160 от 19 декабря 2005 года)
2. Директива 95/46/ЕС Европейского парламента «О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных»
3. Директива 97/66/ЕС Европейского парламента и Совета Европейского союза от 15 декабря 1997 года, касающаяся использования персональных данных и защиты неприкосновенности частной жизни в сфере телекоммуникации

Правовой этап

Персональные данные:

1. Должны быть получены и обработаны добросовестным и законным образом
2. Должны накапливаться для точно определенных и законных целей, не использоваться в противоречии этим целям
3. Должны быть адекватными, относящимися к делу и не должны быть избыточными.
4. Должны быть точными, в случае необходимости обновляться
5. Должны храниться в той форме которая позволит идентифицировать субъекта персональных данных не дольше чем этого требует цель, для которой эти данные накапливаются.

Правовой этап

Основные федеральные законодательные акты

1. Федеральный закон от 27 июля 2006 года №152-ФЗ «О персональных данных»
2. Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
3. Трудовой кодекс Российской Федерации (14 глава, Федеральный закон 30 декабря 2001 года № 197-ФЗ)
4. Указ президента РФ от 30 мая 2005 года № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего РФ и ведении его личного дела»

Федеральные органы, регулирующие деятельность в сфере обработки персональных данных

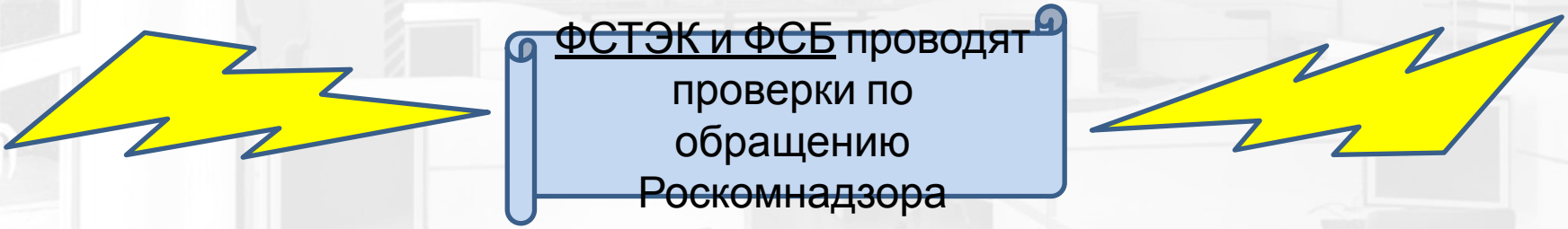
- **Роскомнадзор** (Федеральная служба по надзору в сфере связи и массовых коммуникаций) – осуществляет контроль и надзор за соответствием обработки ПДн требованиям законодательства.
- **ФСТЭК России** (Федеральная служба по техническому и экспортному контролю) – устанавливает методы и способы защиты информации с использованием технических средств.
- **ФСБ России** (Федеральная служба безопасности РФ) – устанавливает методы и способы защиты информации в пределах своих полномочий (сфера пользования криптографических средств защиты информации)

!!! Проведение проверок !!!

Правовой этап

Виды проверок Роскомнадзора:

1. В отношении операторов, подавших уведомление об обработке персональных данных и (или) включенных в Реестр операторов;
2. Внеплановые проверки по контролю нарушений обязательных требований.
3. В отношении операторов на основании полученных жалоб и обращений граждан или юридических лиц по вопросам, связанным с обработкой персональных данных или обеспечением их безопасности.



Если вашей ИСПДн присвоена категория К3 или К4

Правовой этап

Основания

Плановые проверки

Начало осуществления оператором деятельности по обработке персональных данных

Истечение 3х лет со дня:

1. Гос. Регистрации оператора как юридического лица;
2. Окончания проведения последней плановой проверки

ВНЕПЛАНОВЫЕ ПРОВЕРКИ

1.Истечение срока исполнения оператором ранее выданного предписания об устранении выявленных нарушений в области ПДн.

2. Поступление заявлений граждан, юр. Лиц, органов власти, местного самоуправления о фактах:

-Возникновения угрозы причинения вреда жизни, здоровья граждан;

- Причинение вреда жизни, здоровья граждан.

Формы проверок

ДОКУМЕНТАРНАЯ

- По месту нахождения службы.
- Предметом являются сведеня, содержащиеся в документах оператора, используемые при осуществлении деятельности по обработке персональных данных.

Если выявлены ошибки, противоречия, несоответствия, то направляется требование предоставлении в течении 10 рабочих дней необходимых пояснений в письменной форме.
Если, по предоставлению дополнителых документов и пояснений будут выявлены признаки нарушений обязательных требований

ВЫЕЗДНАЯ

- На территории оператора.
- Проверка полноты и достоверности сведений, содержащихся в уведомлении об обработке персональных данных, а так же в иных документах, имеющихся в распоряжении территориального органа.

Необходимые документы предоставляются в виде копий, заверенных печатью и подписью руководителя или другого уполномоченного представителя оператора.

Не допускается требовать нотариального удостоверения копий документов.
(П 67.6 и 67.7 Регламента)

Возможные результаты проведения проверок

1. Выдача предписания об устранении выявленного нарушения и осуществления контроля за его исполнением.
2. Выявление административного правонарушения и составление протокола об административном правонарушении, направление протокола в суд либо прокуратуру.
3. Выявление уголовно наказуемого деяния ,направление материала в органы прокуратуры, для рассмотрения вопроса о возбуждении уголовного дела.

Количество, состав участников проверки	Не менее двух должностных лиц, в том числе лицо отвечающее за вопросы правового обеспечения
Срок уведомления оператора о начале проведения плановой проверки	Не познее чем в течении трех рабочих дней до начала проведения проверки
Срок уведомления оператора о начале проведения внеплановой проверки	Не позднее чем за 24 часа до начала ее проведения
Порядок предварительного уведомления о начале проведения плановой проверки	Направление оператору копии приказа руководителя службы\его заместителя
Порядок предварительного уведомления о начале проведения плановой проверки	Любым доступным способом
Срок проведения проверки	20 рабочих дней (продление возможно на срок не более 20 рабочих дней)
Срок предоставления	10 рабочих дней

Этапы построения защищенной ИСПДн:

Правовой

Международное и федеральное законодательство В сфере защиты информации

Организационный

Исследование и документирование процессов обработки информации в ИСПДн

Инженерно-технический

Принятие соответствующих мер технического, режимного характера. Внедрение средств Физической и программной защиты персональных данных.

Действия оператора по выполнению требований Федерального закона

Начинать надо с определения:

– перечня персональных данных
– категорий обрабатываемых персональных данных
– целей их обработки

Затем:

– необходимо направить уведомление в Уполномоченный орган

После этого:

– разработать документы, регламентирующие обработку персональных данных в организации
– реализовать требования по инженерно-технической защите помещений
– провести аттестацию или осуществить декларирование соответствия по требованиям безопасности информации

Определение перечня ПДн, целей сроков их обработки

1. Персональные данные работников

   - *Трудовой договор, личная карточка Т-2*

   (Паспортные данные, семейное положение, сведения об образовании, номер страхового свидетельства, сведения о трудовой деятельности)

2. Сведения о контактных лицах контрагентов

   (ФИО, должность, телефон адрес и т.п.) Могут быть общедоступными!

3. От сферы деятельности:

   - *Для образовательных учреждений*

   (о воспитанниках, учащихся, студентах, преподавателях и.т.п)

4. Дополнительные персональные данные

   - Наличие заболеваний у работников

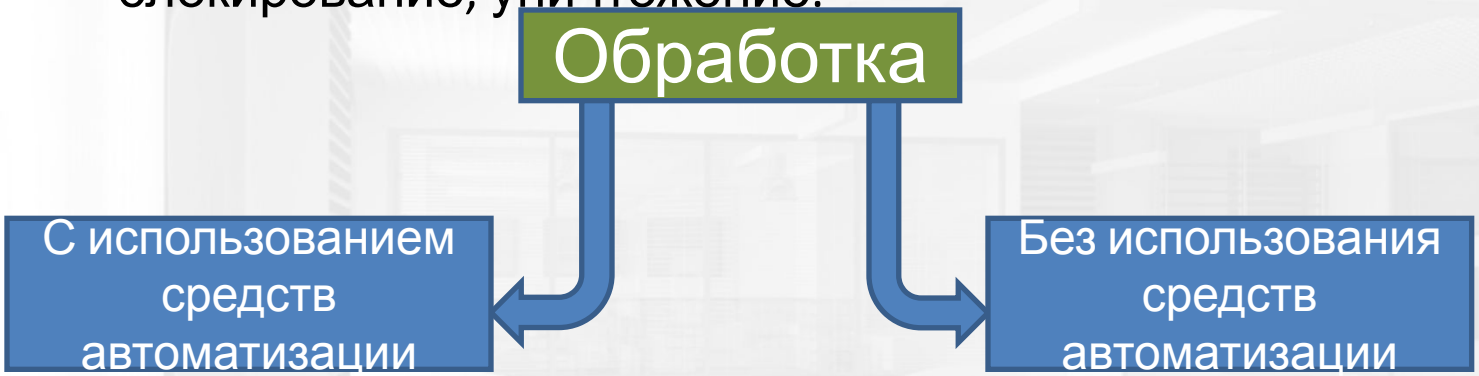
   -сведения полученные подразделениями безопасности

   (данные службы охраны о посетителях)

Мишина,3
99 22 99
bit39.ru
БЮРО IT

Наиболее вероятная цель обработки Пдн – трудовые отношения с работниками.

- Обработка персональных данных – действия с персональными данными включающие сбор, систематизацию, накопление, хранение, уточнение, использование, распространение, обезличивание, блокирование, уничтожение.



Данные о бывших сотрудниках

Особенности обработки Пдн без использования средств автоматизации

1. Персональные данные, при их обработке должны обособиться от иной информации, в частности путем фиксации их на отдельных материальных носителях, в специальных разделах.
2. Не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы.
3. Обязательное раздельное хранение персональных данных, обработка которых касается различных целей.
4. В отношении каждой категории персональных данных нужно определить место хранения и установить перечень лиц, осуществляющих обработку Пдн или имеющих к ним доступ.
5. Лица осуществляющие обработку Пдн должны быто проинформированы о факте обработки, категориях обрабатываемых Пдн, а так же об особенностях и правилах такой обработки, установленных нормативно-правовыми актами.

Сроки хранения могут быть определены:

1. Нормативно-правовым актом;
2. Достижением цели обработки персональных данных;
3. Указан в согласии субъекта.

Сроки хранения документов в части расчетов с работниками организации, утвержденные Федеральной архивной службой России:

1. Лицевые счета рабочих (форма Т-2) -75 лет;
2. Расчетные ведомости – 5 лет;
3. Исполнительные листы – до минования надобности;
4. Справки на предоставление учебных отпусков, получения льгот по налогам и .т.д. – до минования надобности;
5. Договоры, соглашения – 5 лет.

Проведение классификации присвоение класса информационной системе

Цель проведения классификации:

Установление методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных.

Классификация проводится именно по отношению ИСПДн, а не программного обеспечения.

Когда проводим?

- На этапе создания информационных систем
- В ходе их эксплуатации

Кто проводит?

ФСТЭК
№55/86/20

-Государственные органы;
-Муниципальные органы;
-Юридические\физические лица;

Осуществляющие обработку персональных данных

Если организация «сомневается в своих силах», то для проведения классификации следует привлечь стороннюю организацию.

Мишина,3
99 22 99
bit39.ru
БЮРО iT

Какие данные участвуют при проведении классификации ИСПДн?

1. Категория обрабатываемых в информационной системе ПДн;
2. Объём обрабатываемы персональных данных;
3. Характеристики безопасности персональных данных, обрабатываемых в ИСПДн;
4. Структура информационной системы;
5. Наличие подключения ИСПДн к сетям интернет;
6. Режим обработки персональных данных;
7. Системы с разграничением прав доступа пользователей или без;
8. Место нахождение технических средств информационной системы;

Число субъектов Персональных Данных		меньше 1000	от 1000 до 100 000	свыше 100 000
ИСПдн	Категория 4	к4	к4	к4
	Категория 3	к3	к3	к2
	Категория 2	к3	к2	к1
	Категория 1	к1	к1	к1

Разработка нормативной правовой базы, регламентирующей обработку персональных данных

1. Административно-распорядительные документы предприятия.
2. Положение об обработке персональных данных
3. Инструкция о порядке обработки персональных данных без использования средств автоматизации
4. Инструкция о порядке обработки персональных данных с использованием средств автоматизации
5. Должностные инструкции специалистов, непосредственно осуществляющих обработку персональных данных
6. Соглашение о неразглашении сведений, составляющих персональные данные
7. Частная модель угроз

Мишина,3
99 22 99
bit39.ru

БЮРО IT

Организационно-распорядительные мероприятия

Правового характера	Организационного характера	Режимного характера
- Получение согласий у субъектов ПДн; - Направление уведомления в Роскомнадзор с целью включения в реестр операторов; - Разработка организационно-распорядительной документации.	- Проведение категорирования ПДн и классификация ИСПДн; - Разработка порядка работ с ПДн; - Доведение до сотрудников порядка работ; - Осуществление мер контроля	- Организация системы охраны территории, здания, помещения; - Организация порядка допуска в помещение; - Обеспечение сохранности сменных носителей