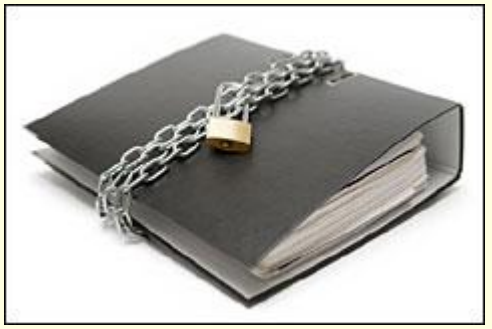


Основные этапы подготовки образовательного учреждения к реализации ФЗ №152 «О персональных данных»

Требования законодательства

- **С 1 января 2011 года** начинается действие закона № 152-ФЗ «О персональных данных», который должен соблюдаться в том числе в образовательных учреждениях

Персональные данные – это:

- любая информация, относящаяся к определенному физическому лицу, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация

Т.о., в школах обрабатываются персональные данные как учащихся, так и педагогов

Основной нормативный документ

- ФЗ № 152-ФЗ «О персональных данных», принятый в июле 2006 г.,

  обязывает операторов персональных данных «принять необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий».

До 1 января 2011 года

- **Во всех ОУ** должен быть выполнен комплекс работ, по итогам которого создан портфель документов (25 документов), который будут проверять контролирующие организации
- Положение осложняется тем, что в отличие от некоторых других ведомств, в образовании не приняты нормативные акты, утверждающие типовые ведомственные документы по защите ПД

Перечень документов в организации, проверяемой регуляторами*

1. Положение о защите персональных данных
2. Положение о подразделении по защите информации
3. Приказ о назначении лиц, ответственных за обработку ПДн
4. Концепция информационной безопасности
5. Политика информационной безопасности
6. Перечень персональных данных, подлежащих защите
7. Приказ о проведении внутренней проверки
8. Отчет о результатах проведения внутренней проверки
9. Акт классификации информационной системы персональных данных
10. Положение о разграничении прав доступа к обрабатываемым персональным данным

* **Регуляторы** - ФСБ, ФСТЭК и Роскомнадзор Министерства связи и массовых коммуникаций

Перечень документов в организации, проверяемой регуляторами*

11. Модель угроз безопасности персональным данным
12. План мероприятий по защите ПДн
13. Порядок резервирования ТС и ПО, баз данных и Сзи
14. План внутренних проверок
15. Журнал по учету мероприятий по контролю
16. Журнал учета обращений субъектов ПДн о выполнении их законных прав
17. Инструкция администратора ИСПДн
18. Инструкция пользователя ИСПДн
19. Инструкция администратора безопасности ИСПДн
20. Инструкция пользователя по обеспечению безопасности обработки ПД при возникновении внештатных ситуаций

* **Регуляторы** - ФСБ, ФСТЭК и Роскомнадзор Министерства связи и массовых коммуникаций

Перечень документов в организации, проверяемой регуляторами*

21. Перечень по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним
22. Типовое Техническое задание на разработку системы обеспечения безопасности информации объекта вычислительной техники
23. Эскизный проект на создание системы обеспечения безопасности информации объекта вычислительной техники
24. Положение об Электронном журнале обращений пользователей информационных систем персональных данных (проект приказа)
25. Методические рекомендации для организации защиты информации при обработке персональных данных

* **Регуляторы** - ФСБ, ФСТЭК и Роскомнадзор Министерства связи и массовых коммуникаций

Подготовка к выполнению ФЗ № 152-ФЗ

- Выделяют 9 основных этапов организации систем защиты персональных данных

Этапы организации системы защиты ПД

1. Инвентаризация ресурсов
2. Ограничение доступа работников к персональным данным
3. Документальное регламентирование работы с персональными данными (ПД)
4. Формирование модели угроз персональным данным
5. Классификация Информационных систем ПД ОУ
6. Составление и отправка в уполномоченный орган уведомления об обработке ПД
7. Приведение системы защиты ПД в соответствии с требованиями регуляторов
8. Создание системы ИБ ИСПД и ее аттестация (сертификация) – для ИСПД классов К1, К2
9. Организация эксплуатации ИСПДн и контроля за безопасностью

Шаг 1. Инвентаризация ресурсов

- Проанализировать все эксплуатируемые информационные системы и традиционные хранилища данных, выявить все, где присутствуют и обрабатываются персональные данные.

ИС ОУ, относящиеся к ИСПДН

- Автоматизированная информационная библиотечная система
- «1С-Бюджет», «1С-Зарплата-Кадры»
- Электронный журнал
- …
- АРМ СЭД УФК – ОУ
- ИС «Налогоплательщик»
- ПД СПУ Пенсионного фонда

Участки обработки ПД

- Библиотека
- Бухгалтерия
- Учительская
- Медпункт
- …

Шаг 2. Ограничение доступа работников к персональным данным

- **Принятие в организации *Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных (ИСПДн)***
- **Положение об обеспечении безопасности персональных данных при их обработке в ИСПДн должно включать:**
- 12. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя … ***учет лиц, допущенных к работе с персональными данными*** в информационной системе
- 14. Лица, доступ которых к ПД, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, ***допускаются к*** соответствующим персональным сданным ***на основании списка, утвержденного оператором*** или уполномоченным лицом.

ШАГ 3: Документальное регламентирование работы с персональными данными

- **Статья 86 (Трудовой кодекс РФ).** Общие требования при обработке персональных данных работника и гарантии их защиты
- 8) ***работники*** и их представители ***должны быть ознакомлены под роспись с документами*** работодателя, ***устанавливающими порядок обработки персональных данных*** работников, а также об их правах и обязанностях в этой области

ШАГ 3: Документальное регламентирование работы с персональными данными

Субъект ПД самостоятельно решает вопрос передачи кому-либо своих ПД, документально оформляя свое намерение. В соответствии со статьей 9 ФЗ-№152 обработка персональных данных осуществляется только при условии согласия в письменной форме с указанием следующих данных:

- фамилия, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование (фамилия, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие, а также порядок его отзыва.

ШАГ 4: Формирование модели угроз персональным данным

- **15.02.2008 г. Заместителем директора ФСТЭК России утверждены:**
- Базовая модель угроз безопасности ПД при их обработке в ИСПД
- Методика определения актуальных угроз безопасности ПД при их обработке в ИСПД

ШАГ 5: Классификация ИСПДн ОУ

(см. также комментарий к слайду – в режиме редактирования)

Категория ПДн, обрабатываемых в ИС	Объем ПДн, обрабатываемых в ИС		
	В ИС одновременно обрабатываются ПДн менее чем 1000 субъектов ПДн или ПДн субъектов ПДн в пределах конкретной организации	В ИС одновременно обрабатываются ПДн от 1000 до 100 000 субъектов ПДн или ПДн субъектов ПДн, работающих в отрасли экономики РФ, в органе госвласти, проживающих в пределах муниципального образования	В ИС одновременно обрабатываются ПДн более чем 100 000 субъектов ПДн или ПДн субъектов ПДн в пределах субъекта РФ или РФ в целом
Обезличенные и (или) общедоступные ПДн	К4	К4	К4
ПДн, позволяющие идентифицировать субъекта ПДн	К3	К3	К2
ПДн, позволяющие идентифицировать субъекта ПДн и получить о нем дополнительную информацию	К3	К2	К1
ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни	К1	К1	К1

Таблица

ОУ регион МО РФ

Категория ПДн, обрабатываемых в ИС	Объем ПДн, обрабатываемых в ИС		
	В ИС одновременно обрабатываются ПДн менее чем 1000 субъектов ПДн или ПДн субъектов ПДн в пределах конкретной организации	В ИС одновременно обрабатываются ПДн от 1000 до 100 000 субъектов ПДн или ПДн субъектов ПДн, работающих в отрасли экономики РФ, в органе госвласти, проживающих в пределах муниципального образования	В ИС одновременно обрабатываются ПДн более чем 100 000 субъектов ПДн или ПДн субъектов ПДн в пределах субъекта РФ или РФ в целом
Обезличенные и (или) общедоступные ПДн	К4	К4	К4
ПДн, позволяющие идентифицировать субъекта ПДн	К3	К3	К2
ПДн, позволяющие идентифицировать субъекта ПДн и получить о нем дополнительную информацию	К3	К2	К1
ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни	К1	К1	К1

Таблица 1

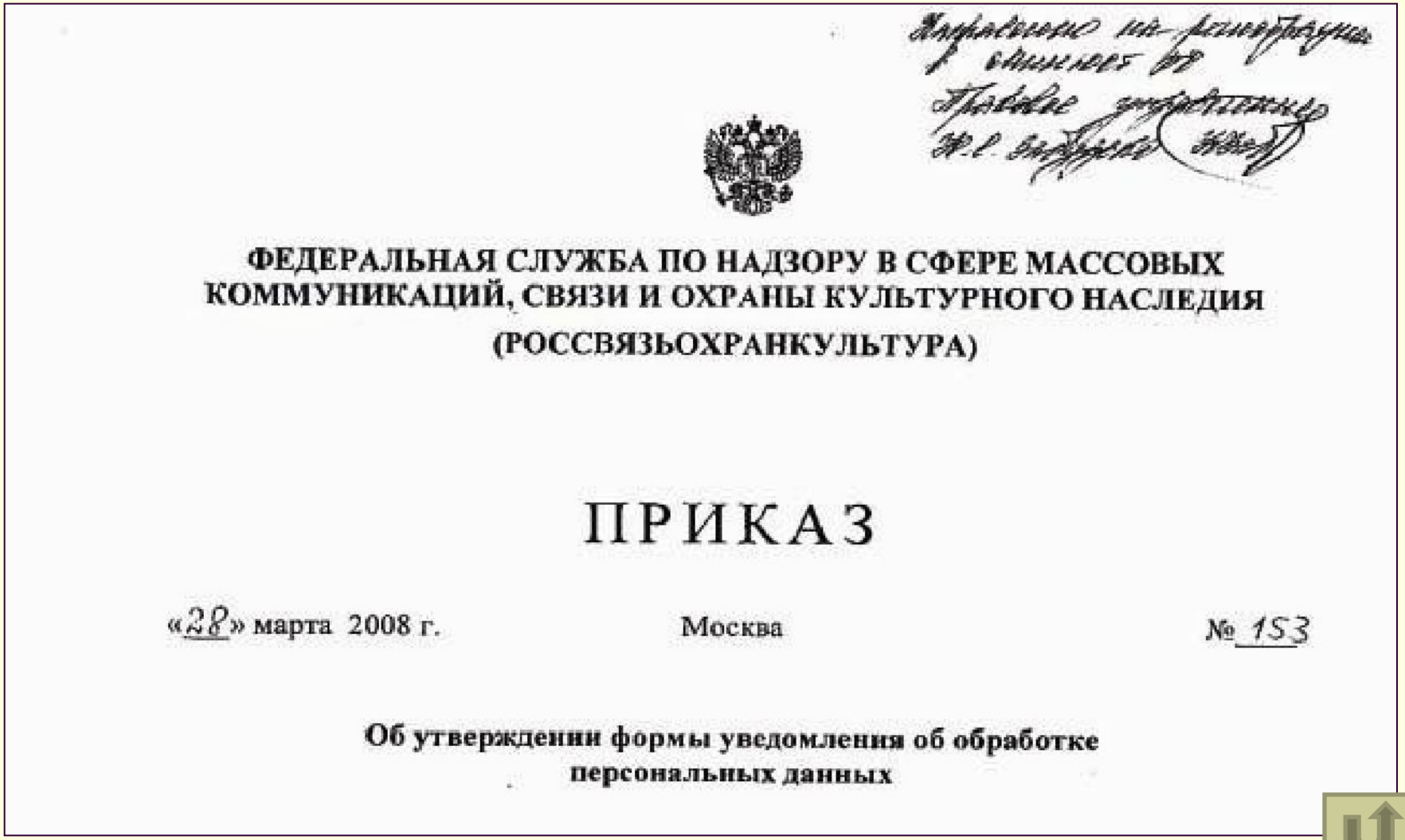
(см. также комментарий к слайду – в режиме редактирования)

Организации, ИС которых отнесены к классам К1, К2 должны:

- получить **лицензию ФСТЭК** России на деятельность по технической защите конфиденциальной информации (**для классов ИСПДн К1 и К2**);

т.е.направить туда по определенной форме запрос и получить лицензию, подтверждающую их соответствие

ШАГ 6: Составление и отправка в уполномоченный орган уведомления



ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ МАССОВЫХ КОММУНИКАЦИЙ, СВЯЗИ И ОХРАНЫ КУЛЬТУРНОГО НАСЛЕДИЯ

(РОССВЯЗЬОХРАНКУЛЬТУРА)

ПРИКАЗ

«28» марта 2008 г. Москва № 153

Об утверждении формы уведомления об обработке персональных данных

ШАГ 7: Приведение системы защиты персональных данных в соответствии с требованиями регуляторов*

ФЗ «О персональных данных»: ***Статья 19. Меры по обеспечению безопасности персональных данных при их обработке***

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

---

* **Регуляторы** - ФСБ, ФСТЭК и Роскомнадзор Министерства связи и массовых коммуникаций

ШАГ 8. Создание подсистемы информационной безопасности ИСПДн и ее аттестация (сертификация)

Включает в себя:

- Основные мероприятия по организации и техническому обеспечению безопасности ПД, обрабатываемых в ИСПД
- Оценка соответствия ИСПДн по требованиям безопасности ПДн производится: Для ИСПДн 1 и 2 классов – *обязательная сертификация (аттестация)* по требованиям безопасности информации

Перечень объектов информатизации, подлежащих аттестации в Системе сертификации средств защиты информации по требованиям безопасности информации

1. Автоматизированные системы различного уровня и назначения.
2. Системы связи, приема, обработки и передачи данных.
3. Системы отображения и размножения.
4. Помещения, предназначенные для ведения конфиденциальных переговоров.

ШАГ 9: Организация эксплуатации ИСПДн и контроля за безопасностью

Положение об обеспечении безопасности персональных данных при их обработке в ИСПДн:

- 12. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:
- з) контроль за соблюдением условий использования СЗИ, предусмотренных эксплуатационной и технической документацией;
- и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей ПДн, использования СЗИ, которые могут привести к нарушению конфиденциальности ПДн…

Перечень документов в организации, проверяемой регуляторами

1. Положение о защите персональных данных
2. Положение о подразделении по защите информации
3. Приказ о назначении лиц, ответственных за обработку ПДн
4. Концепция информационной безопасности
5. Политика информационной безопасности
6. Перечень персональных данных, подлежащих защите
7. Приказ о проведении внутренней проверки
8. Отчет о результатах проведения внутренней проверки
9. Акт классификации информационной системы персональных данных
10. Положение о разграничении прав доступа к обрабатываемым персональным данным

Перечень документов в организации, проверяемой регуляторами

11. Модель угроз безопасности персональным данным
12. План мероприятий по защите ПДн
13. Порядок резервирования ТС и ПО, баз данных и Сзи
14. План внутренних проверок
15. Журнал по учету мероприятий по контролю
16. Журнал учета обращений субъектов ПДн о выполнении их законных прав
17. Инструкция администратора ИСПДн
18. Инструкция пользователя ИСПДн
19. Инструкция администратора безопасности ИСПДн
20. Инструкция пользователя по обеспечению безопасности обработки ПД при возникновении внештатных ситуаций

Перечень документов в организации, проверяемой регуляторами

21. Перечень по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним
22. Типовое Техническое задание на разработку системы обеспечения безопасности информации объекта вычислительной техники
23. Эскизный проект на создание системы обеспечения безопасности информации объекта вычислительной техники
24. Положение об Электронном журнале обращений пользователей информационных систем персональных данных (проект приказа)
25. Методические рекомендации для организации защиты информации при обработке персональных данных

Этапы построения системы защиты ПДн

- После того, как в организации сформирована рабочая или проектная группа и выбрана сторонняя ИТ-компания, предстоит последовательно реализовать следующие этапы работы.
- Прежде всего, нужно определить все ситуации, когда требуется проводить сбор, хранение, передачу или обработку ПДн.
- Затем - выделить процессы, связанные с такими ситуациями.
- Разумно выбрать ограниченное число процессов и проанализировать их. В рамках такого исследования формируется перечень подразделений и сотрудников компании, участвующих в обработке ПДн в рамках своей служебной деятельности.
- Потом нужно определить круг информационных систем и совокупность обрабатываемых ПДн.
- Следующий шаг - категорирование ПДн и предварительная классификация ИС.
- Затем проводится выработка предложений по снижению класса обрабатываемых ПДн.
- После этого формируется актуальная модель угроз для каждой ИСПДн, подготавливается задание по созданию требуемой системы защиты.
- Потом проводится уточнение классов ИС и подготовка рекомендаций по использованию технических средств защиты ПДн.
- Затем в Роскомнадзор подается уведомление о деятельности в качестве оператора ПДн, а в ФСТЭК - заявка на получение экземпляров руководящих документов по организации системы защиты.

Этапы построения системы защиты ПДн

- Эти работы предстоит выполнить на первом, начальном этапе.
- Именно в это время закладывается фундамент успеха всего проекта и **делаются основные расходы на консалтинг**.
- Но основанная работа происходит на последующих стадиях, которые включают
  - развертывание полноценной системы обработки ПДн,
  - полномасштабное внедрение средств защиты,
  - аттестацию ИС,
  - приведение всех процессов обработки ПДн в соответствие с требованиями закона,
  - реагирование на регулярные проверки и т.д.

781-е Постановление Правительства определяет 11 основных типов мероприятий:

1. Назначение ответственного лица/подразделения
2. Определение угроз безопасности ПДн и формирование модели угроз
3. Разработка на основе модели угроз системы защиты с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем
4. Проверка готовности систем защиты информации (СЗИ) к использованию
5. Установка и ввод в эксплуатацию СЗИ
6. Обучение персонала правилам работы с СЗИ
7. Учет применяемых СЗИ и носителей ПДн
8. Учет лиц, допущенных к работе с ПДн
9. Контроль за соблюдением условий использования СЗИ
10. Реагирование на нарушение режима защиты ПД
11. Описание системы защиты

Нормативные документы

- Рекомендации по обеспечению 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
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных