11-й НАЦИОНАЛЬНЫЙ ФОРУМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ «ИНФОФОРУМ»
"Информационная безопасность России в условиях глобального информационного общества“
30.01.2009

Реализация положений Федерального закона «О персональных данных»: время действовать

М.Ю.Емельянников
Директор по развитию бизнеса
НИП «ИНФОРМЗАЩИТА»

ФЗ «О ПЕРСОНАЛЬНЫХ ДАННЫХ»

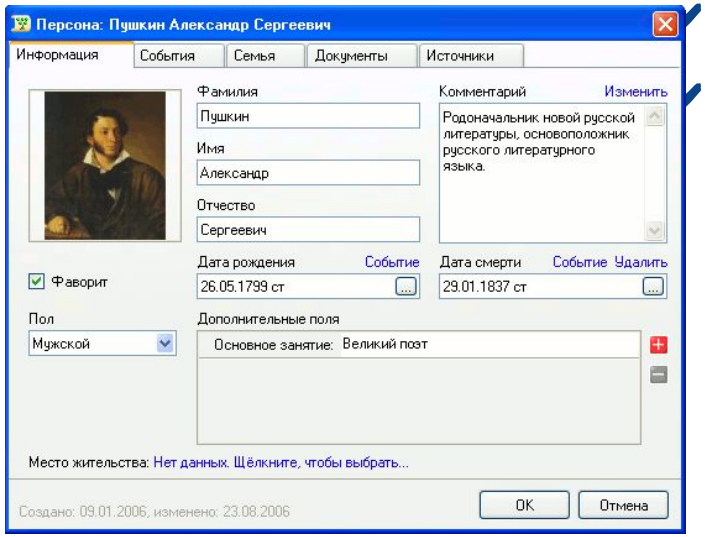
Информационные системы персональных данных, созданные до дня вступления в силу настоящего Федерального закона, должны быть приведены в соответствие с требованиями настоящего Федерального закона *не позднее 1 января 2010 года*.

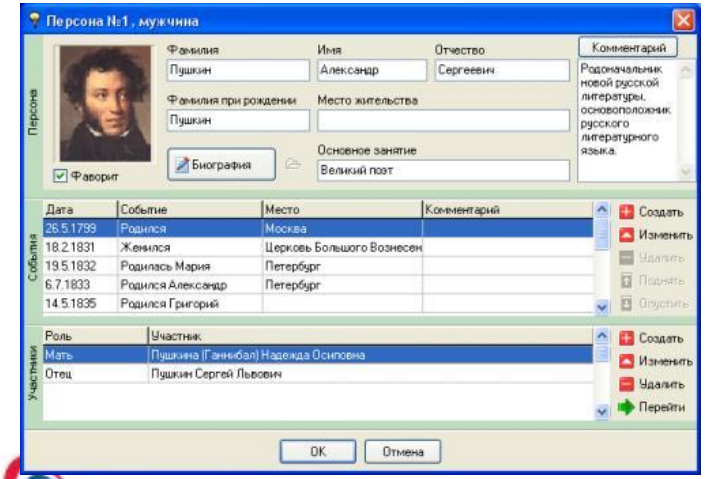
ФЗ «О ПЕРСОНАЛЬНЫХ ДАННЫХ»

Статья 19. Меры по обеспечению безопасности персональных данных при их обработке

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

РЕШЕНИЯ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ





- технически сложные
- требуют:
  - высокой квалификации исполнителей
  - специальных знаний
  - глубокого понимания функциональности:
    - приложений, обрабатывающих персональные данные
    - средств защиты информации, необходимых для нейтрализации актуальных угроз персональным данным

ЧТО МОЖНО И НУЖНО БЫЛО СДЕЛАТЬ ЕЩЕ ВЧЕРА

Первые необходимые шаги

1. Выявить все информационные системы, обрабатывающие персональные данные
2. Классифицировать все ИСПДн
3. Сформировать и актуализировать модели угроз персональным данным применительно к каждой системе или однотипным системам

КЛАССИФИКАЦИЯ ИСПДн

Приказ ФСТЭК/ФСБ/Мининформсвязи от 13.02 2008 № 55/86/20

«Об утверждении порядка проведения классификации ИС персональных данных»

1. Классификация - задача неформальная
2. На этапе сбора и анализ исходных данных по ИСПДн:
   - ✔ Определение целей обработки ПДн
   - ✔ Формирование перечня ПДн (состав сведений, отнесенных к такой категории)
3. Оценка необходимости и целесообразности отнесения ИСПДн к специальным

КЛАССИФИКАЦИЯ ИСПДн

Проблемы классификации

- ✔ Следование духу, а не формальной букве закона
- ✔ Разумный выбор параметров определяющих класс ИСПДн:
  - количество субъектов Vs локальность обработки
  - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию
- ✔ Отсутствие формальных (законодательно определенных) определений таких понятий, как:
  - «состояние здоровья»,
  - «принятие решений, порождающих юридические последствия в отношении субъекта персональных данных»

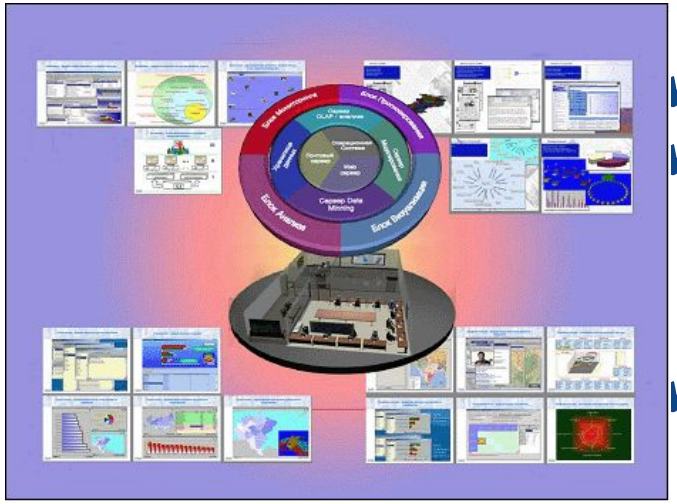
ФОРМИРОВАНИЕ ПЕРЕЧНЯ ПДн

№№ пп	Основания для обработки	Содержание сведений	Срок хранения, условия прекращения обработки
1	Глава 14 Трудового кодекса	Фамилия, имя, отчество Дата и место рождения Гражданство ИНН Номер свидетельства государственного пенсионного страхования … Др. сведения унифицированной формы № Т-2	75 лет ЭПК

ФОРМИРОВАНИЕ ПЕРЕЧНЯ ПДн

№№ пп	Основания для обработки	Содержание сведений	Срок хранения, условия прекращения обработки
2	ФЗ «О связи», Постановление Правительства от 27.08.2005 г. № 538	Фамилия, имя, отчество абонента Адрес абонента или адрес установки оконечного оборудования, Абонентские номера и другие данные, позволяющие идентифицировать абонента или его оконечное оборудование …	3 года с момента оказания последней услуги

СОЗДАНИЕ МОДЕЛИ УГРОЗ ПДн



Актуализация угроз:

- ✔ Полномочия, но не произвол оператора
- ✔ Необходимость следования методологии регуляторов и установленным критериям актуализации
- ✔ Необходимость принятия мер по нейтрализации актуальных угроз

ПРОЕКТИРОВАНИЕ СИСТЕМЫ БЕЗОПАСНОСТИ ИСПДн

На основе исходных данных, указанных в акте классификации и актуализированной модели угроз определяются:

- ✔ механизмы безопасности, которые должны быть реализованы в системе защиты
- ✔ конкретные требования к функциональности этих механизмов

ПРОЕКТИРОВАНИЕ СИСТЕМЫ БЕЗОПАСНОСТИ ИСПДн

Мероприятия по защите ПДн при их обработке в ИСПДн от НСД и неправомерных действий, включают:

- *Управление доступом*
- Регистрацию и учет
- Обеспечение целостности
- Контроль отсутствия недекларированных возможностей
- Антивирусную защиту
- Обеспечение безопасного межсетевого взаимодействия ИСПДн
- Анализ защищенности
- Обнаружение вторжений

ПРОЕКТИРОВАНИЕ СИСТЕМЫ БЕЗОПАСНОСТИ ИСПДн

Подсистема *управления доступом* рекомендуется реализовывать на базе программных средств блокирования НСД, сигнализации и регистрации – *специальных, не входящих в ядро какой-либо ОС программных и программно-аппаратных средства защиты* самих ОС, электронных баз ПДн и прикладных программ, реализующих функции:

- Диагностики
- Регистрации
- Уничтожения
- *Сигнализации*
- Имитации

ПРОЕКТИРОВАНИЕ СИСТЕМЫ БЕЗОПАСНОСТИ ИСПДн

Средства сигнализации предназначены для:

- ✔ предупреждения операторов при их обращении к защищаемым ПДн
- ✔ для предупреждения администратора об обнаружении факта
  - НСД к ПДн
  - Искажения программных средств защиты
  - Выходе или выводе из строя аппаратных средств защиты
  - Других фактах нарушения штатного режима функционирования ИСПДн

ПРОЕКТИРОВАНИЕ СИСТЕМЫ БЕЗОПАСНОСТИ ИСПДн

Межсетевое экранирование:

Класс ИСПДн	Уровень защищенности МЭ
3 и 4	5
2	4
1	3

Системы обнаружения вторжений:

Класс ИСПДн	Системы обнаружения вторжений
3 и 4	Системы обнаружения сетевых атак, использующие сигнатурные методы анализа
1 и 2	Системы обнаружения сетевых атак, использующие сигнатурные методы анализа и методы выявления аномалий

ПРОЕКТИРОВАНИЕ СИСТЕМЫ БЕЗОПАСНОСТИ ИСПДн

Минимизация затрат на создание систем безопасности ИСПДн:

- ✔ максимальное использование возможностей уже имеющихся в КИС средств безопасности, а также ОС и прикладного ПО, сертифицированных или *имеющих перспективы сертификации* в системах ФСТЭК и ФСБ
- ✔ принятие дополнительных мер, позволяющих снизить требования к части ИСПДн или сегментам сети, где такие ИСПДн расположены

МИНИМИЗАЦИЯ ЗАТРАТ НА БЕЗОПАСНОСТЬ ИСПДн

- сокращение числа работников (АРМ), обрабатывающих ПДн, разделение функций, минимизирующее возможность одновременной обработки ПДн из разных систем;
- обезличивание части ИСПДн (переход на абонентские и табельные номера, номера лицевых счетов и т.п.);
- разделение КИС сертифицированными межсетевыми экранами на сегменты, классификация каждой (групп) ИСПДн и снижения требований к части из них;
- организация терминального доступа к ИСПДн;
- исключения части сведений, хранение их на бумажных или иных носителях вне ИСПДн.

ПРОЕКТИРОВАНИЕ СИСТЕМЫ БЕЗОПАСНОСТИ ИСПДн

Типичная ошибка:

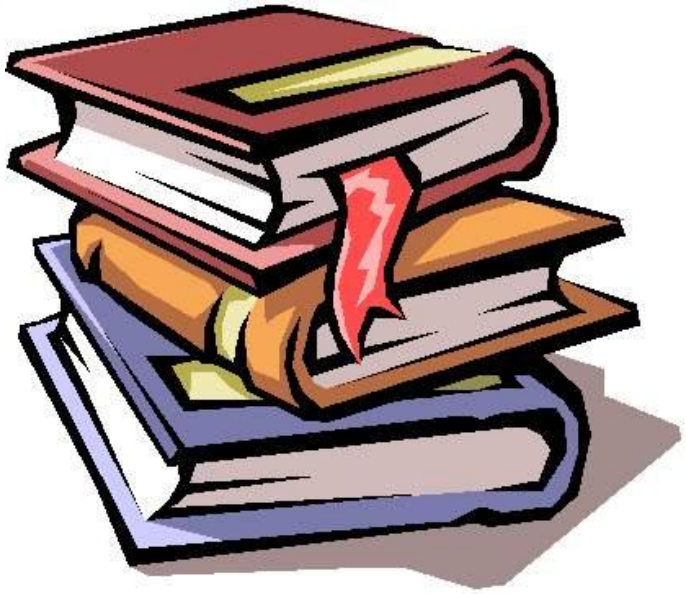
наличие у СЗИ сертификата, позволяющего применять его в системе определенного класса защищенности, является *необходимым и достаточным* для выполнения всего объема требований

ПРОЕКТИРОВАНИЕ СИСТЕМЫ БЕЗОПАСНОСТИ ИСПДн

Имеющихся сертифицированных средств защиты информации достаточно для реализации практически всех требований, изложенных в нормативно-методических документах ФСТЭК и ФСБ.

Вопрос лишь в знании их функциональности и правильном сочетании

МИНИМАЛЬНЫЙ ПАКЕТ НОРМОДОКОВ



- ✔ Перечень персональных данных
- ✔ Модель угроз безопасности персональных данных
- ✔ Акт о классификации ИСПДн
- ✔ Положение (инструкция, руководство) об обеспечении безопасности персональных данных при их обработке
- ✔ Описание системы защиты, обеспечивающей нейтрализацию угроз для соответствующего класса ИСПДн
- ✔ Заключения о возможности эксплуатации средств защиты персональных данных

+ документы, предусмотренные для соответствующих процедур оценки соответствия (аттестация, сертификация)

ЛИЦЕНЗИРОВАНИЕ ДЕЯТЕЛЬНОСТИ ОПЕРАТОРОВ

СЕРИЯ КИ 0022 НОМЕР 001058

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ЛИЦЕНЗИЯ

НА ДЕЯТЕЛЬНОСТЬ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Регистрационный номер 0283 от 26 ноября 2004 г.

Федеральная служба по техническому и экспортному контролю разрешает осуществление мероприятий и оказание услуг по технической защите конфиденциальной информации

Лицензия выдана Закрытому акционерному обществу НАУЧНО-ИНЖЕНЕРНОЕ ПРЕДПРИЯТИЕ «ИНФОРМЗАЩИТА»

129010, г. Москва, Протопоповский пер., д.19, стр.10 (корп.14)

ИНН 7702148410

Лицензия действительна до 26 ноября 2009 г.

Заместитель директора

А. Гапонов

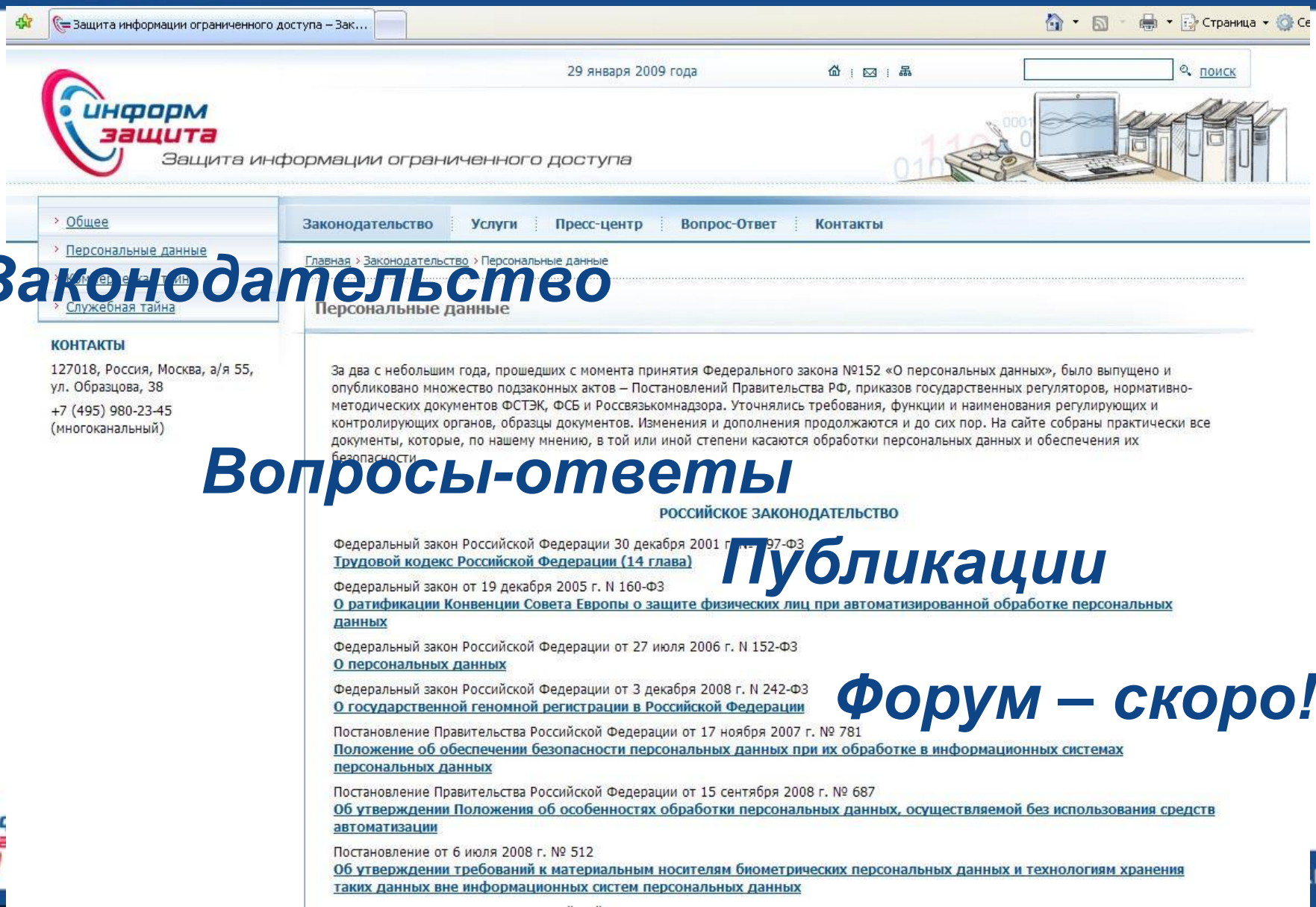
Операторы ИСПДн при проведении мероприятий по обеспечению безопасности ПДн (конфиденциальная информация) при их обработке в ИСПДн *1 и 2 классов и распределенных ИС 3 класса должны получить лицензию* на осуществление деятельности по технической защите конфиденциальной информации

Альтернатива: договор об аутсорсинге системы безопасности ИСПДн с лицензиатом

АЛЬТЕРНАТИВНЫЕ СЦЕНАРИИ

защита

ZKI.INFOSEC.RU



Законодательство

Вопросы-ответы

Публикации

Форум – скоро!

ВОПРОСЫ?

М.Ю.Емельянников

 (495) 980-2345
 m.eme@infosec.ru