



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

М.Ю.Емельяников

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.*



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

Персона: Пушкин Александр Сергеевич

Информация События Семья Документы Источники

Фамилия: Пушкин
Имя: Александр
Отчество: Сергеевич

Дата рождения: 26.05.1799 ст.
Дата смерти: 29.01.1837 ст.

Пол: Мужской

Основное занятие: Великий поэт

Комментарий: Родоначальник новой русской литературы, основоположник русского литературного языка.

Место жительства: Нет данных. Щёлкните, чтобы выбрать...

Создано: 09.01.2006, изменено: 23.08.2006

OK Отмена

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

Персона №1, мужчина

Фамилия: Пушкин
Имя: Александр
Отчество: Сергеевич

Дата рождения: 26.5.1799
Место рождения: Москва

Основное занятие: Великий поэт

Комментарий: Родоначальник новой русской литературы, основоположник русского литературного языка.

Дата	Событие	Место	Комментарий
26.5.1799	Родился	Москва	
18.2.1831	Женился	Щерков Большой Вознесен	
19.5.1832	Родилась Мария	Петербург	
6.7.1833	Родился Александр	Петербург	
14.5.1835	Родился Григорий		

Роль	Участник
Мать	Пушкина (Ганнибал) Надежда Осиповна
Отец	Пушкин Сергей Львович

OK Отмена



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

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



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»

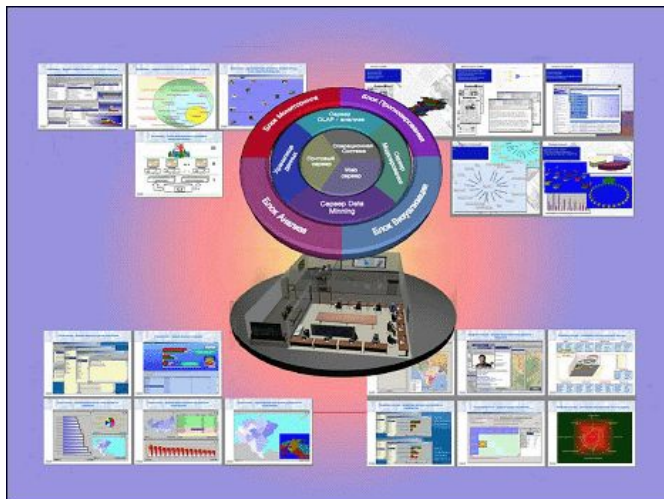
ФОРМИРОВАНИЕ ПЕРЕЧНЯ ПДн

№№ 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



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

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

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

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

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

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



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.

Типичная ошибка:

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



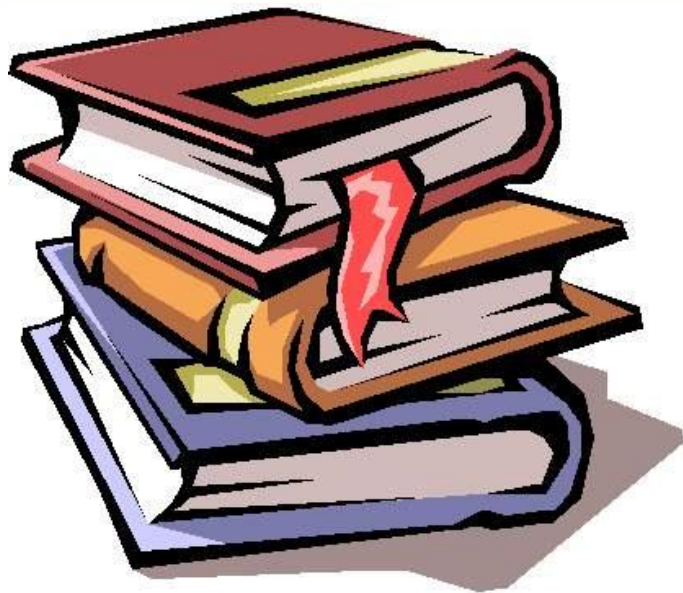
ПРОЕКТИРОВАНИЕ СИСТЕМЫ БЕЗОПАСНОСТИ ИСПДн



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
- ✓ Заключение о возможности эксплуатации средств защиты персональных данных
 - + документы, предусмотренные для соответствующих процедур оценки соответствия (аттестация, сертификация)

ЛИЦЕНЗИРОВАНИЕ ДЕЯТЕЛЬНОСТИ ОПЕРАТОРОВ

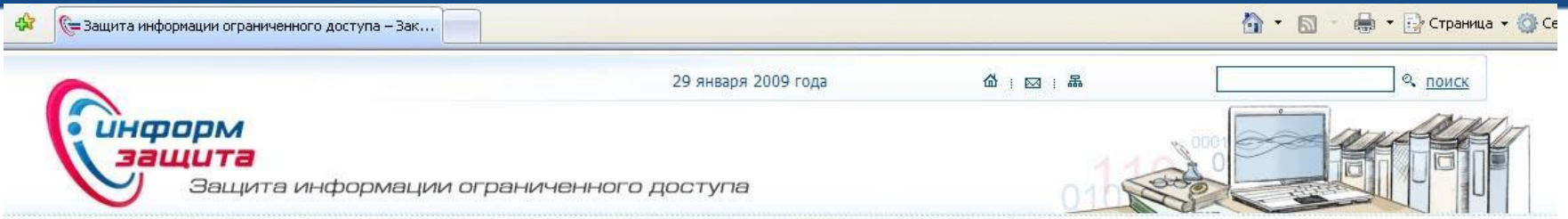


Операторы ИСПДн при проведении мероприятий по обеспечению безопасности ПДн (конфиденциальная информация) при их обработке в ИСПДн *1 и 2 классов и распределенных ИС 3 класса должны получить лицензию* на осуществление деятельности по технической защите конфиденциальной информации

Альтернатива: договор об аутсорсинге системы безопасности ИСПДн с лицензиатом

АЛЬТЕРНАТИВНЫЕ СЦЕНАРИИ





Законодательство

- > [Общее](#)
- > [Персональные данные](#)
- > [Материальные носители](#)
- > [Служебная тайна](#)

- [Законодательство](#)
- [Услуги](#)
- [Пресс-центр](#)
- [Вопрос-Ответ](#)
- [Контакты](#)

Главная > Законодательство > Персональные данные
Персональные данные

КОНТАКТЫ

127018, Россия, Москва, а/я 55,
 ул. Образцова, 38
 +7 (495) 980-23-45
 (многоканальный)

За два с небольшим года, прошедших с момента принятия Федерального закона №152 «О персональных данных», было выпущено и опубликовано множество подзаконных актов – Постановлений Правительства РФ, приказов государственных регуляторов, нормативно-методических документов ФСТЭК, ФСБ и Россвязькомнадзора. Уточнялись требования, функции и наименования регулирующих и контролирующих органов, образцы документов. Изменения и дополнения продолжают и до сих пор. На сайте собраны практически все документы, которые, по нашему мнению, в той или иной степени касаются обработки персональных данных и обеспечения их безопасности.

Вопросы-ответы

РОССИЙСКОЕ ЗАКОНОДАТЕЛЬСТВО

Федеральный закон Российской Федерации 30 декабря 2001 г. № 197-ФЗ
[Трудовой кодекс Российской Федерации \(14 глава\)](#)

Федеральный закон от 19 декабря 2005 г. N 160-ФЗ

[О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных](#)

Федеральный закон Российской Федерации от 27 июля 2006 г. N 152-ФЗ
[О персональных данных](#)

Федеральный закон Российской Федерации от 3 декабря 2008 г. N 242-ФЗ
[О государственной геномной регистрации в Российской Федерации](#)

Постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781
[Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных](#)

Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687
[Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации](#)

Постановление 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](#)

Публикации

Форум – скоро!





ВОПРОСЫ?

М.Ю.Емельяников

☐ (495) 980-2345

☐ m.eme@infosec.ru