



# Разработка автоматизированной системы категорирования и выбора средств защиты информационных систем персональных данных

В.И.Аверченков, М.Ю.Рытов, О.М.Голембиовская, Е.В.Лексиков



# Постановка проблемы



В 2007 году в силу вступил федеральный закон «О персональных данных». Не готовность операторов персональных данных привела к отсрочке выполнения требований закона до 1 января 2011 года.

## Причины неподготовленности:

1. Объемная законодательная база в области защиты персональных данных, требующая изучения.
2. Дорогостоящая процедура защиты информационных систем персональных данных.

# Законодательство в области ПДн

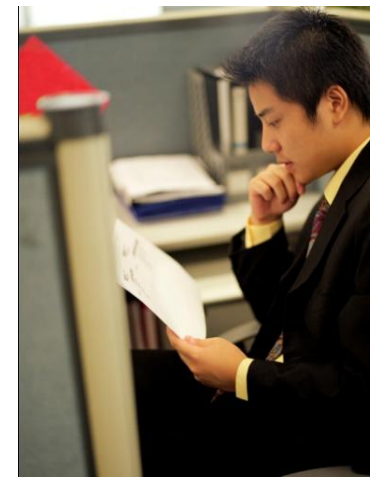
- Конституция Российской Федерации (принята на всенародном голосовании 12 декабря 1993 г.);
  - Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63–ФЗ (
  - Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195–ФЗ
  - Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197–ФЗ
  - Основы законодательства Российской Федерации об охране здоровья граждан от 22 июля 1993 г. №
  - Федеральный закон от 8 августа 2001 г. № 129–ФЗ «О государственной регистрации юридических лиц и индивидуальных предпринимателей»
  - Федеральный закон от 27 мая 2003 г. № 58–ФЗ «О системе государственной службы Российской Федерации»
  - Федеральный закон от 27 июля 2004 г. № 79–ФЗ «О государственной гражданской службе Российской Федерации»
  - Федеральный закон от 22 октября 2004 г. № 125–ФЗ «Об архивном деле в Российской Федерации»
  - Федеральный закон № 160–ФЗ от 19 декабря 2005 г. «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
  - Федеральный закон от 27 июля 2006 г. № 149–ФЗ «Об информации, информационных технологиях и о защите информации»;
  - Федеральный закон от 27 июля 2006 г. № 152–ФЗ «О персональных данных»
  - Федеральный закон от 29 декабря 2006 г. № 256–ФЗ «О дополнительных мерах государственной поддержки семей, имеющих детей» (с изменениями от 23 июля, 25 декабря 2008 г.);
  - Федеральный закон от 2 марта 2007 г. № 25–ФЗ «О муниципальной службе в Российской Федерации».
- Статья 29. Персональные данные муниципального служащего (с изменениями от 23 июля, 27 октября, 25 ноября, 22, 25 декабря 2008 г., 17 июля 2009 г.);
- Федеральный закон Российской Федерации от 3 декабря 2008 г. № 242–ФЗ «О Государственной геномной регистрации в Российской Федерации» (с изменениями от 17 декабря 2009 г.);
  - Указ Президента Российской Федерации от 06 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера» (с изменениями от 23 сентября 2005 № 1111);
  - Указ Президента Российской Федерации от 12 мая 2008 № 724 «Вопросы системы и структуры федеральных органов исполнительной власти» (с изменениями от 30 мая, 24 июля, 6 сентября, 7, 14 октября, 3, 25, 31 декабря 2008 г., 11 сентября, 5 октября 2009 г.);

# Актуальность и необходимость разработки

На территории Российской Федерации более 7 миллионов юридических лиц и предпринимателей.

Дорогостоящую и длительную процедуру по приведению ИСПДн в соответствие ФЗ №152 «О персональных данных» может позволить себе небольшой процент из этих 7 миллионов.

Разработанная автоматизированная система позволит снизить трудоемкость работ и уменьшить материальные затраты.



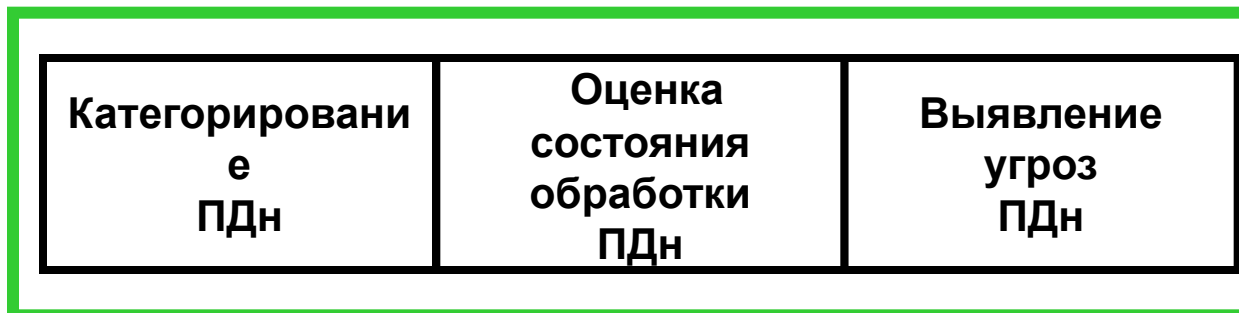
# Схема работы автоматизированной системы

## Обработка данных

На входе



Информация,  
позволяющая  
дать оценку  
ИСПДн

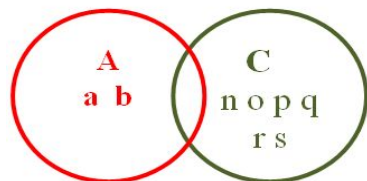


На выходе

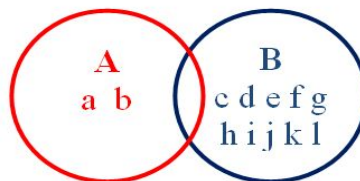


Конкретный  
перечень мер и  
средств,  
необходимых для  
должной защиты  
выявленной  
категории ИСПДн

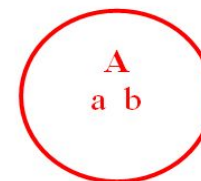
# Формализация процесса категорирования



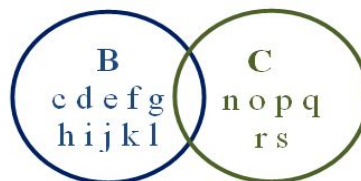
1-ая категория ПДн



2-ая категория ПДн



3-я категория ПДн



4-ая категория ПДн

Элемент множеств	Наименование элемента
<b>a</b>	
a	Фамилия Имя Отчество
b	Паспортные данные
c	Данные свидетельства о рождении
d	Данные водительского удостоверения
e	Данные об образовании
f	Данные о повышении квалификации
g	Данные о прохождении профессиональной переподготовке
h	Данные о воинском учете
i	Данные о доходах

j	Данные об ИНН гражданина
k	Данные страхового свидетельства
l	Данные о составе семьи
m	Данные о льготах
n	Данные о здоровье
o	Данные о расовой принадлежности
p	Данные о национальной принадлежности
q	Данные о политических взглядах
r	Данные о религиозных убеждениях
s	Данные об интимной жизни

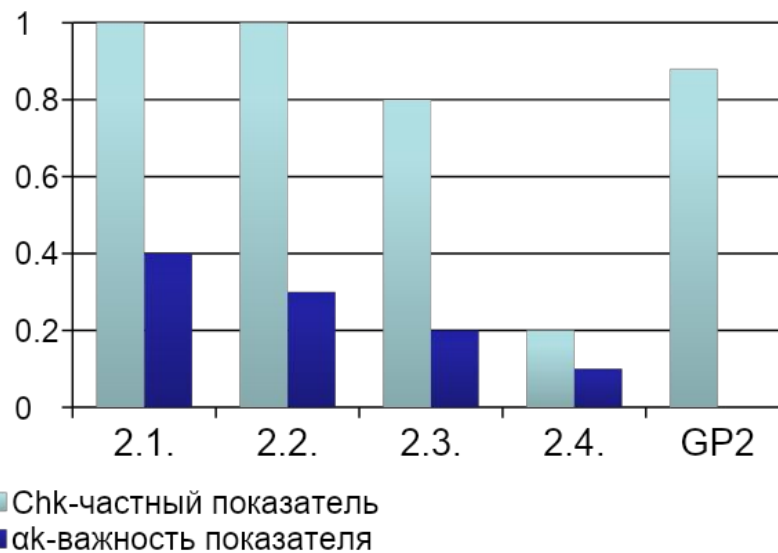


# Расчет оценки защищенности ИСПДн

Групповой показатель GP1 - Обеспечение защиты ИСПДн от угроз утечки видовой информации

№, п/п	Частный показатель	Вес	Важность
Ch 2.1	С помощью каких средств в учреждении введен контроль доступа в контролируемую зону?		<b>0,4</b>
	Система контроля доступа	1	
	Пропускной пункт с охраной	0,5	
	Не используется	0	
Ch 2.2	АРМ пользователей на которых производится обработка ПДн расположены так, что практически исключен визуальный доступ к мониторам?		0,3
	Да	1	
	Нет	0	
<b>Номер частного показателя</b>	<b>Chk</b>	<b>αk</b>	
2.1.	1	0,4	
2.2.	1	0,3	
2.3.	0,8	0,2	
2.4.	0,2	0,1	
<b>GP2</b>	<b>0,58</b>		

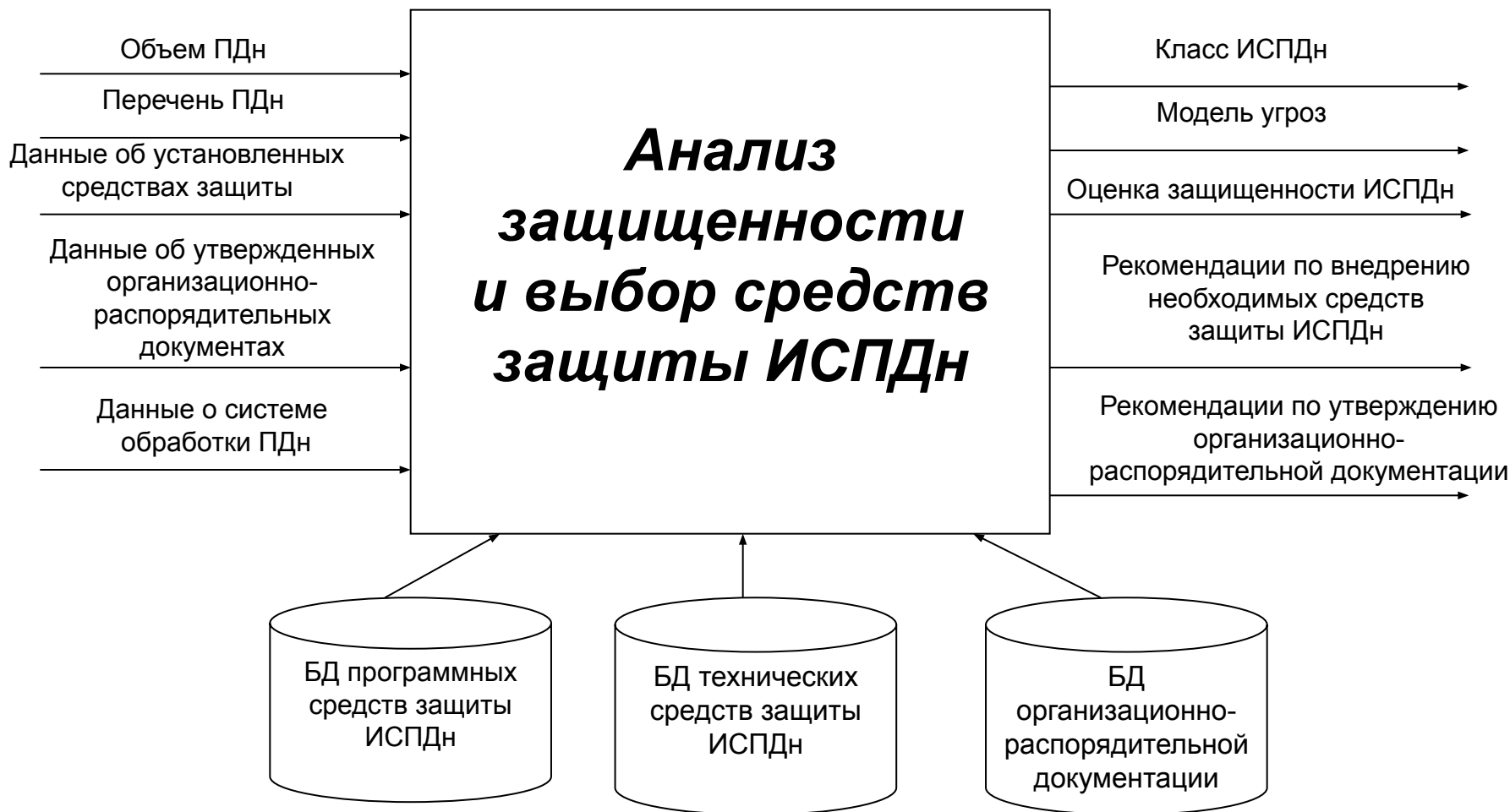
$$GP_i = \alpha_1 Ch_1 + \alpha_2 Ch_2 + \dots + \alpha_k Ch_k$$



## Шкала защищенности ИСПДн:

- 1 – высокий достаточный уровень защиты
- [0,8;1) – высокий недостаточный уровень защиты
- [0,5;0,8) – средний недостаточный уровень защиты
- [0;0,2) – низкий недостаточный уровень защиты
- 0 – система не защищена

# Представление процедуры анализа защищенности и выбора средств защиты ИСПДн





# Заполнение опросной электронной анкеты

## ОПРОСНЫЕ БЛОКИ

### **Общий блок**

(вопросы о численности штата, квалификации работников)



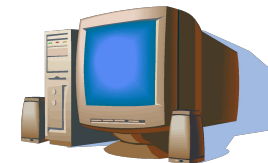
### **Блок организационной документации**

(вопросы о наличии тех или иных организационно-распорядительных документов в области защиты ПДн)



### **Программно-аппаратное оснащение**

(вопросы об оснащенности теми или иными программными средствами защиты ПДн)



### **Техническое оснащение**

(вопросы об оснащенности техническими средствами защиты ПДн)



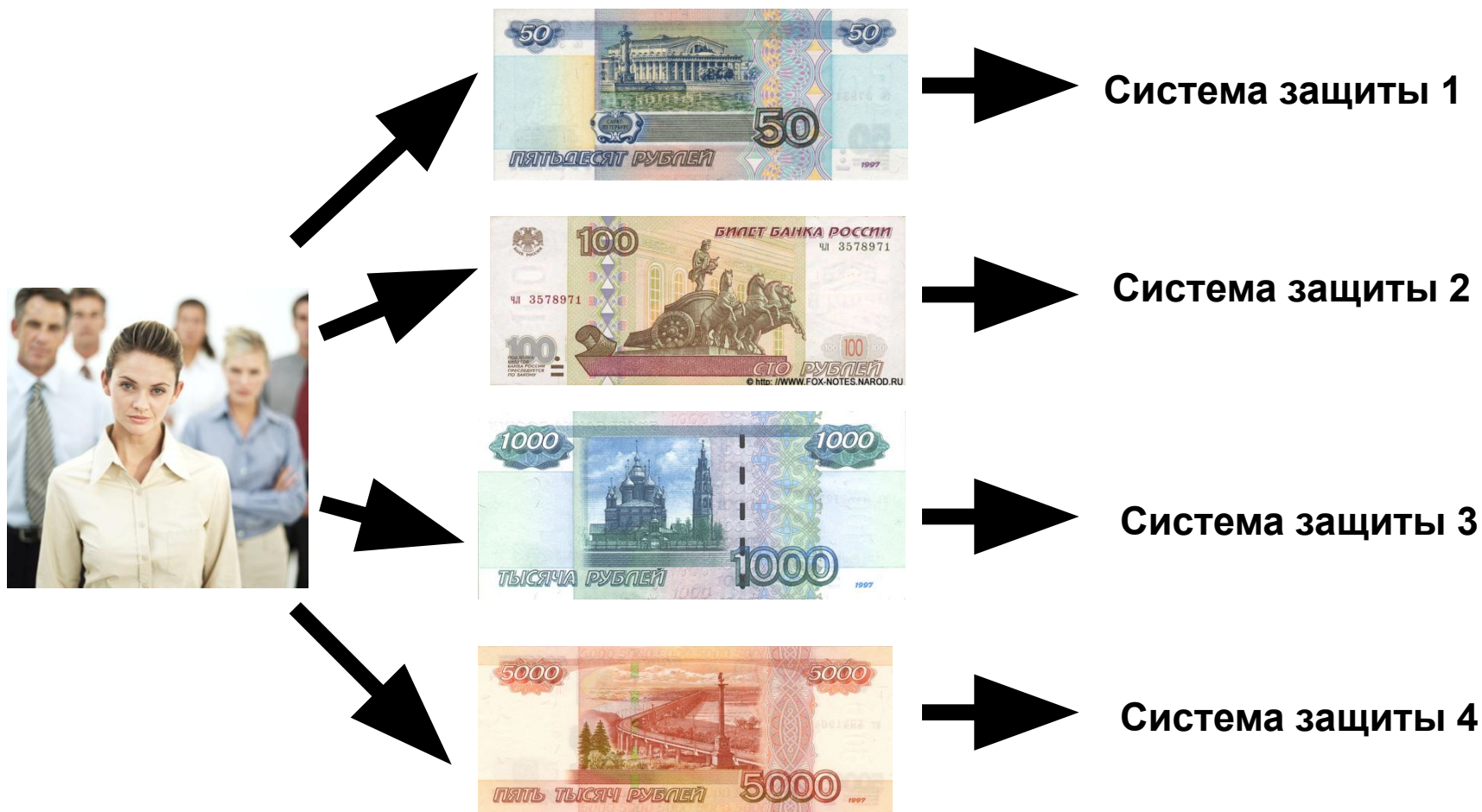
# Формирование отчета по принципу «как есть» и «как должно быть»

Общее состояние защиты информационной системы персональных данных «КАК ЕСТЬ»	Общее состояние защиты информационной системы персональных данных «КАК ДОЛЖНО БЫТЬ»
<ol style="list-style-type: none"><li>1. Общий блок</li><li>2. Блок организационно-распорядительной документации</li><li>3. Блок программно-аппаратного оснащения</li><li>4. Блок технической оснащенности</li></ol> <p style="text-align: right;">—</p>	<ol style="list-style-type: none"><li>1. Общий блок</li><li>2. Блок организационно-распорядительной документации</li><li>3. Блок программно-аппаратного оснащения</li><li>4. Блок технической оснащенности</li></ol> <p style="text-align: right;">+</p>

## Основа - законодательная база:



# Определение диапазона цен, приемлемых для клиента



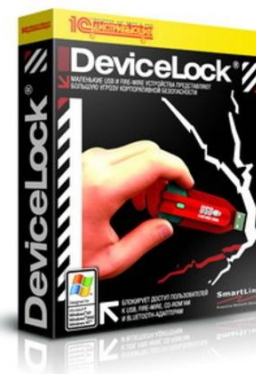
Система защиты будет соответствовать выявленной категории ИСПДн

# Перечень средств и методов, необходимых для защиты информационной системы персональных данных

## Организационные меры:

Для соответствующей системы защиты персональных данных, вам необходимо дополнить вашу базу организационно-распорядительных документов следующими:.....

В соответствии с выбранным диапазоном стоимости оборудования Вам необходимо установить следующие **программно-аппаратные и технические средства защиты** персональных данных:.....





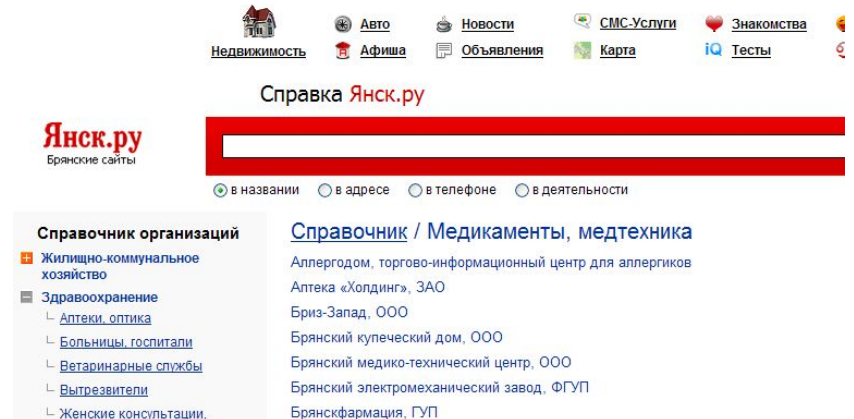
# Применение автоматизированной системы выбора средств и методов защиты персональных данных



**Частные и государственные  
организации различных  
форм собственности**

# ОБЗОР УЧРЕЖДЕНИЙ ГОРОДА БРЯНСКА, ОБРАБАТЫВАЮЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ СОТРУДНИКОВ

- ✓ Жилищно-коммунальное хозяйство - 392
- ✓ Учреждения культуры и искусства - 42
- ✓ Учреждения здравоохранения - 260
- ✓ Заводы, фабрики - 250 в том числе ИП
- ✓ Муниципальные учреждения - 293
- ✓ Учреждения образования и науки - 404
- ✓ Общественные организации - 502
- ✓ Оптовая торговля, склады, магазины - 361
- ✓ Розничная торговля, магазины - 360
- ✓ Развлекательные учреждения - 269
- ✓ Спортивные учреждения - 74
- ✓ Средства массовой информации - 64
- ✓ Строительные организации - 500
- ✓ Транспортные организации - 320
- ✓ Организации, оказывающие различные виды услуг - 580
- ✓ Банковские и финансовые организации, казначейства - 129



**Примерно: 4  
800**

*Данные представлены, в соответствии со сведениями сайта Брянских организаций [www.yansk.ru](http://www.yansk.ru)*

# АНАЛОГИ

## Сторонние аудиторские компании:

- Информзащита;
- ООО «Анкад»;
- ЗАО «Калуга Астрал»;
- НТЦ «Сфера»;
- ЗАО «Орбита»;
- ОАО «ЭЛВИС-ПЛЮС»





# Структура решаемых задач в автоматизированной системе анализа и выбора средств защиты ИСПДн



# Категорирование Пдн

Категорирование персональных данных

Выберите типы обрабатываемых в системе персональных данных

<input checked="" type="checkbox"/>	1. Фамилия имя отчество
<input type="checkbox"/>	2. Паспортные данные гражданина
<input type="checkbox"/>	3. Данные военного билета
<input type="checkbox"/>	4. Данные удостоверения личности военнослужащего
<input checked="" type="checkbox"/>	5. Данные временного удостоверения личности
<input type="checkbox"/>	6. Данные вида на жительство
<input type="checkbox"/>	7. Данные разрешения на временное проживание
<input type="checkbox"/>	8. Данные свидетельства о рождении
<input type="checkbox"/>	9. Данные водительского удостоверения
<input type="checkbox"/>	10. Данные о полученном образовании
<input type="checkbox"/>	11. Данные о послевузовском образовании
<input type="checkbox"/>	12. Данные о повышении квалификации
<input type="checkbox"/>	13. Данные о профессиональной переподготовке
<input type="checkbox"/>	14. Данные о воинском учете
<input type="checkbox"/>	15. Данные о доходах
<input type="checkbox"/>	16. Данные ИНН
<input type="checkbox"/>	17. Пенсионное страхование
<input type="checkbox"/>	18. Данные страхового медицинского полиса
<input type="checkbox"/>	19. Данные о составе семьи
<input type="checkbox"/>	20. Данные о льготах
<input type="checkbox"/>	21. Сведения о здоровье
<input type="checkbox"/>	22. Данные о расовой принадлежности
<input type="checkbox"/>	23. Данные о национальной принадлежности
<input type="checkbox"/>	24. Данные о политических взглядах
<input type="checkbox"/>	25. Данные о религиозных и философских убеждениях
<input type="checkbox"/>	26. Данные об интимной жизни

16. Данные ИНН

- 16.1. Серия и номер свидетельства о выдаче ИНН
- 16.2. Дата выдачи ИНН
- 16.3. Наименование органа, выдавшего свидетельство
- 16.4. Номер ИНН
- Все перечисленные

Отметить выбор

Результат

Определение объема персональных данных

Выберите объем обрабатываемых в системе персональных данных

- В информационной системе одновременно обрабатываются персональные данные более чем 100000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта Российской Федерации, но более чем 100000 субъектов персональных данных в целом
- В информационной системе одновременно обрабатываются персональные данные более чем 10000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта Российской Федерации, но более чем 10000 субъектов персональных данных в целом
- В информационной системе одновременно обрабатываются персональные данные более чем 1000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации

Project1

В соответствии с Приказом от 13.02.2008 г. № 55/86/20 ИСПДн присваивается КЛАСС 2 - ИС, для которых нарушение заданной характеристики безопасности Пдн, обрабатываемых в них, может привести к негативным последствиям для субъектов Пдн.

OK

Отметить выбор

# Оценка защищенности ИСПДн

## ОЦЕНКА ЗАЩИЩЕННОСТИ ИСПДн

- Защита ИСПДн от угроз утечки акустической информации
- Защита ИСПДн от угроз утечки видовой информации
- Защита ИСПДн от угроз утечки по каналам ПЭМИН
- Защита ИСПДн от угроз уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн
- Защита ИСПДн от угроз НСД с применением программно-аппаратных и программных средств
- Защита ИСПДн от угроз неантропогенного характера
- Защита ИСПДн от угроз сетевой безопасности

### Обеспечение защиты ИСПДн от угроз утечки акустической информации

№, п/п Отметьте имеющиеся на вашем объекте средства защиты ИСПДн

#### 1.1 Какие средства защиты акустического сигнала вы используете

- средства защиты акустического канала информации, обеспечивающие звукопоглощение акустической волны
- средства защиты акустического канала информации, обеспечивающие глушение акустических сигналов
- средства защиты акустического канала информации, обеспечивающие зашумление помещения или твердой среды распространения другими широкополосными звуками, которые обеспечивают маскировку акустических сигналов
- не используются

#### 1.2 Какой степени звукоизоляции установлены двери

- 32 Дб
- 36 Дб
- 40 Дб
- не установлены

#### 1.3

ума на 25-29дБ  
ума на 30-34дБ

#### Важность

Пропускная способность	1
Количество одновременных сессий	2
Количество портов	5
Стоимость	4
Вес	3

Какой вид экранирования используется в помещении  
ческое  электромагнитное  не используется

Отметить выбор

Сохранить данные

# Разработка автоматизированной системы категорирования и выбора средств защиты информационных систем персональных данных

