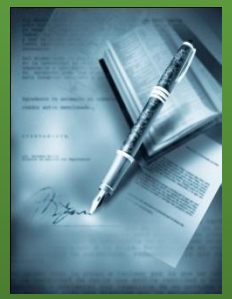
Разработка автоматизированной системы категорирования и выбора средств защиты информационных систем персональных данных

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 приведении 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.

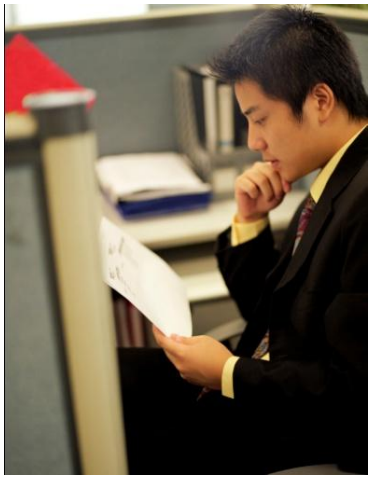


Схема работы автоматизированной системы

Обработка данных

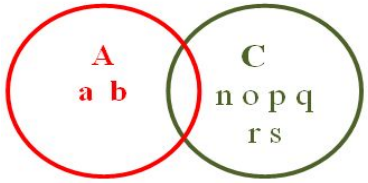
На входе

Информация, позволяющая дать оценку ИСПДн

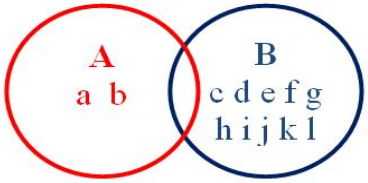
На выходе

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

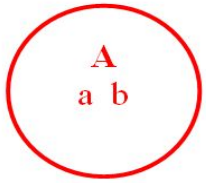
Формализация процесса категорирования



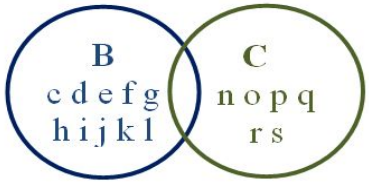
1-ая категория ПДн



2-ая категория ПДн



3-я категория ПДн



4-ая категория ПДн

Элемент множества	Наименование элемента
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

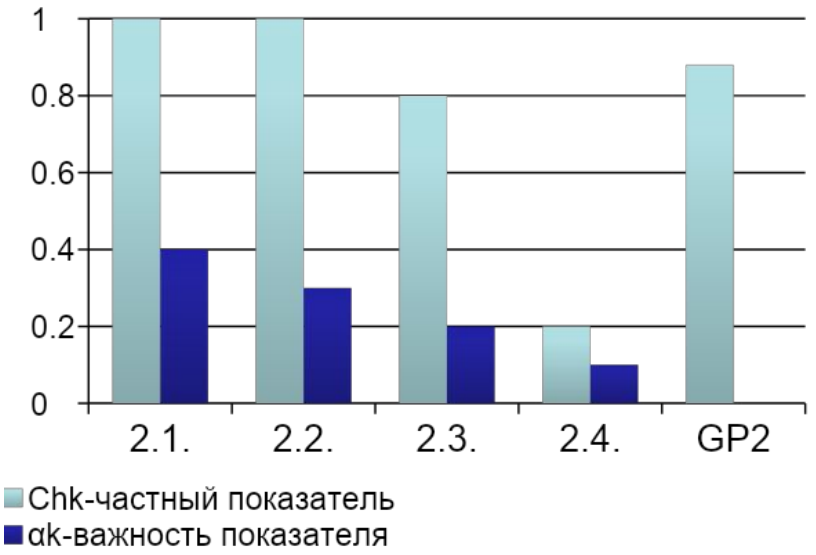
Расчет оценки защищенности ИСПДн

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?**		**0,4**
	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**	

Номер частного показателя	Chk	αk
2.1.	1	0,4
2.2.	1	0,3
2.3.	0,8	0,2
2.4.	0,2	0,1
GP2	0,58	

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



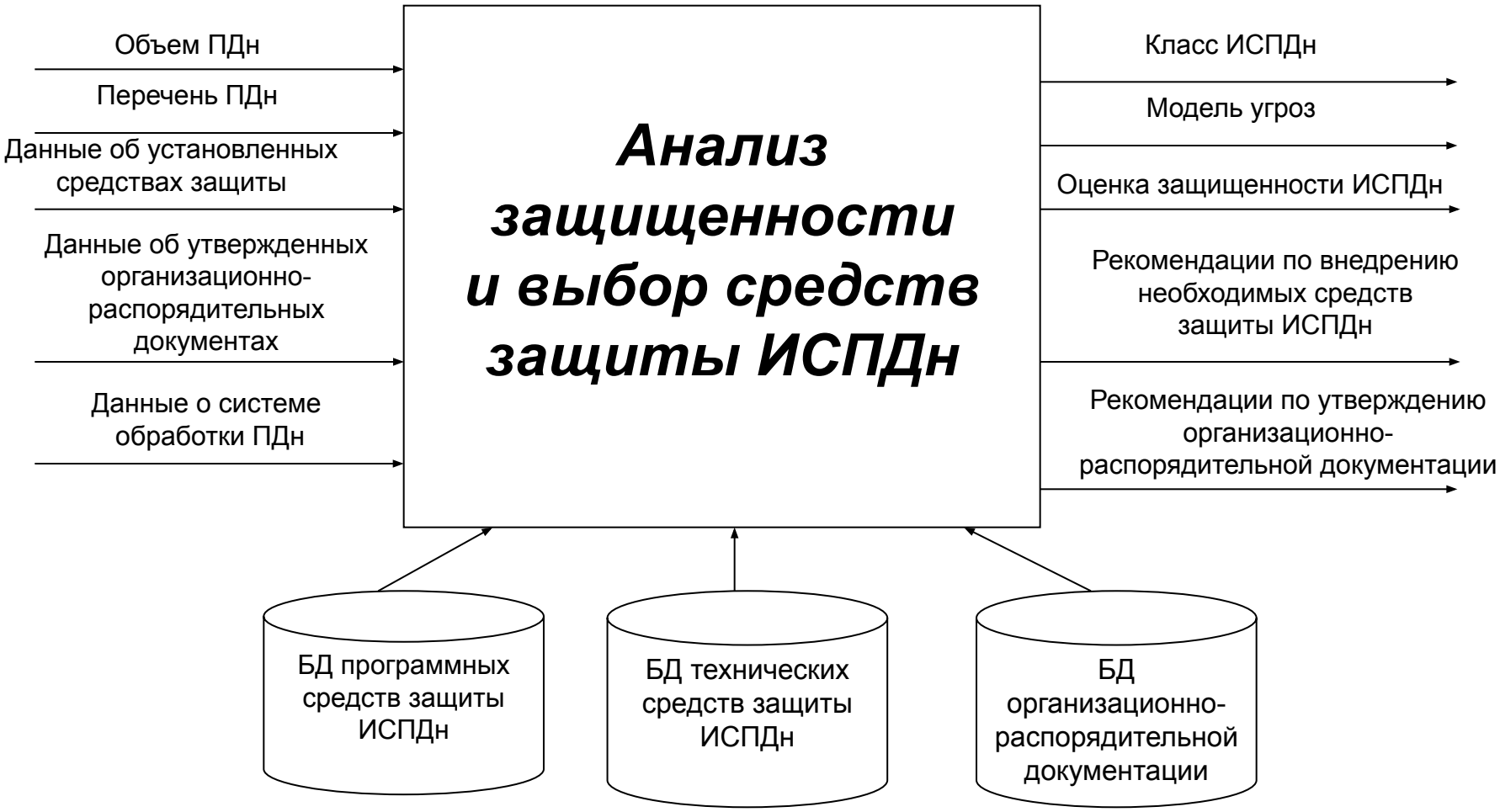
Шкала защищенности ИСПДн:

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



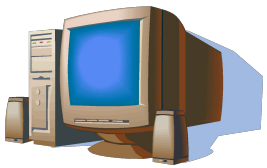
Заполнение опросной электронной анкеты

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»
1. Общий блок 2. Блок организационной-распорядительной документации 3. Блок программно-аппаратного оснащения 4. Блок технической оснащенности	1. Общий блок 2. Блок организационной-распорядительной документации 3. Блок программно-аппаратного оснащения 4. Блок технической оснащенности

Основа - законодательная база:

Определение диапазона цен, приемлемых для клиента

Система защиты 1

Система защиты 2

Система защиты 3

Система защиты 4

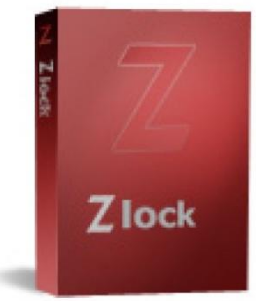
Система защиты будет соответствовать выявленной категории ИСПДн

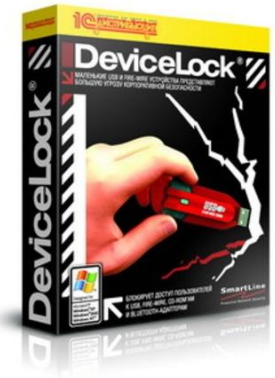
Перечень средств и методов, необходимых для защиты информационной системы персональных данных

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:….



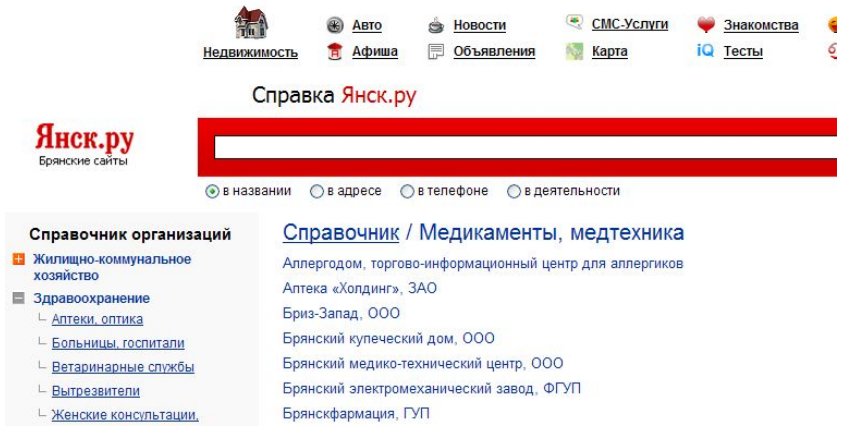


Применение автоматизированной системы выбора средств и методов защиты персональных данных

Частные и государственные организации различных форм собственности

ОБЗОР УЧРЕЖДЕНИЙ ГОРОДА БРЯНСКА, ОБРАБАТЫВЮЩИХ 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

АНАЛОГИ

Сторонние аудиторские компании:

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


РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2010611664

WingDoc II.1

Правообладатель(ли): *Общество с ограниченной ответственностью «Компания информационных технологий» (RU)*

Автор(ы): *Попов Виктор Анатольевич, Кодинцев Константин Николаевич (RU)*

Заявка № 2010610151

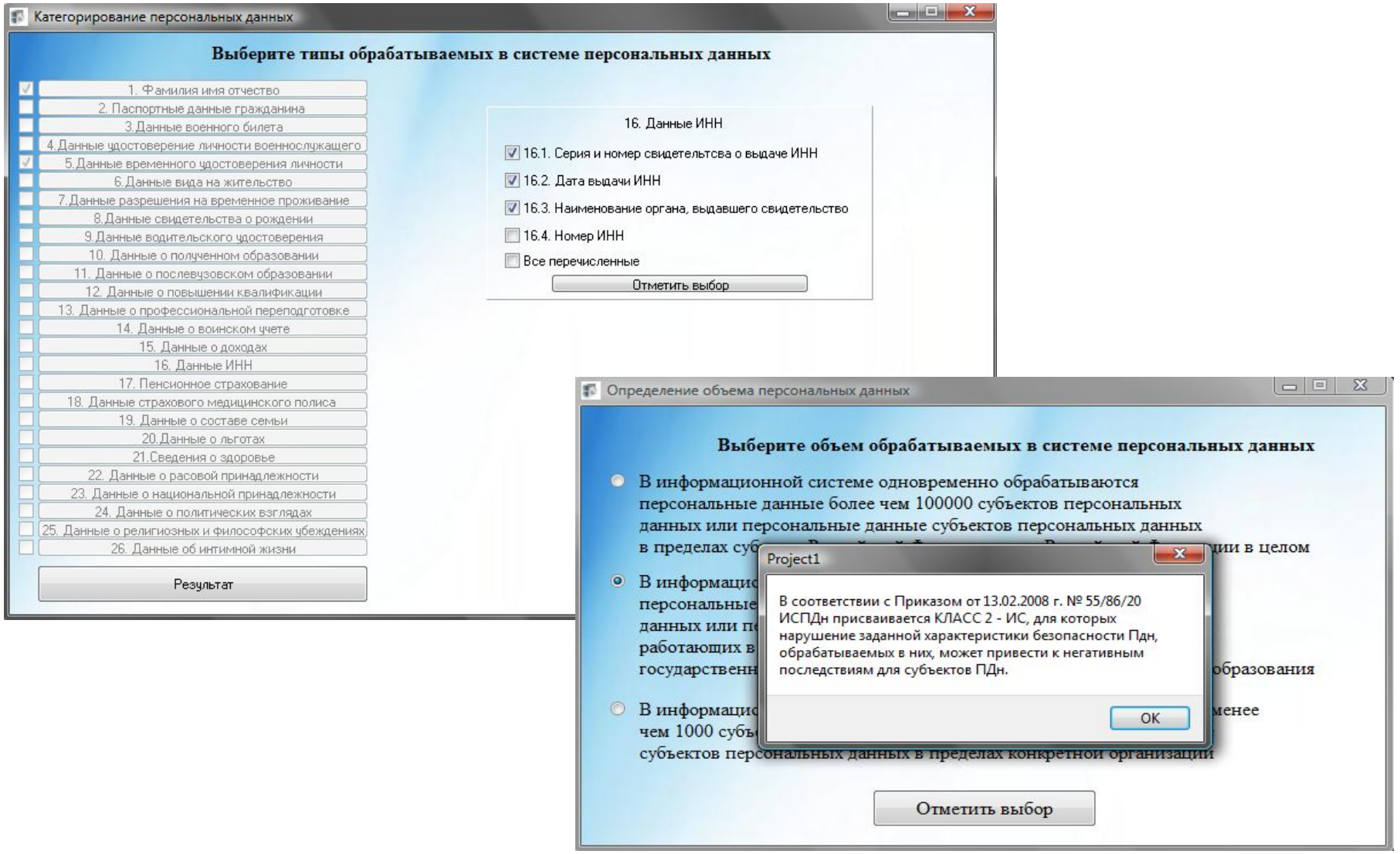
Дата поступления 2 февраля 2010 г.

Зарегистрировано в Реестре программ для ЭВМ 1 марта 2010 г.

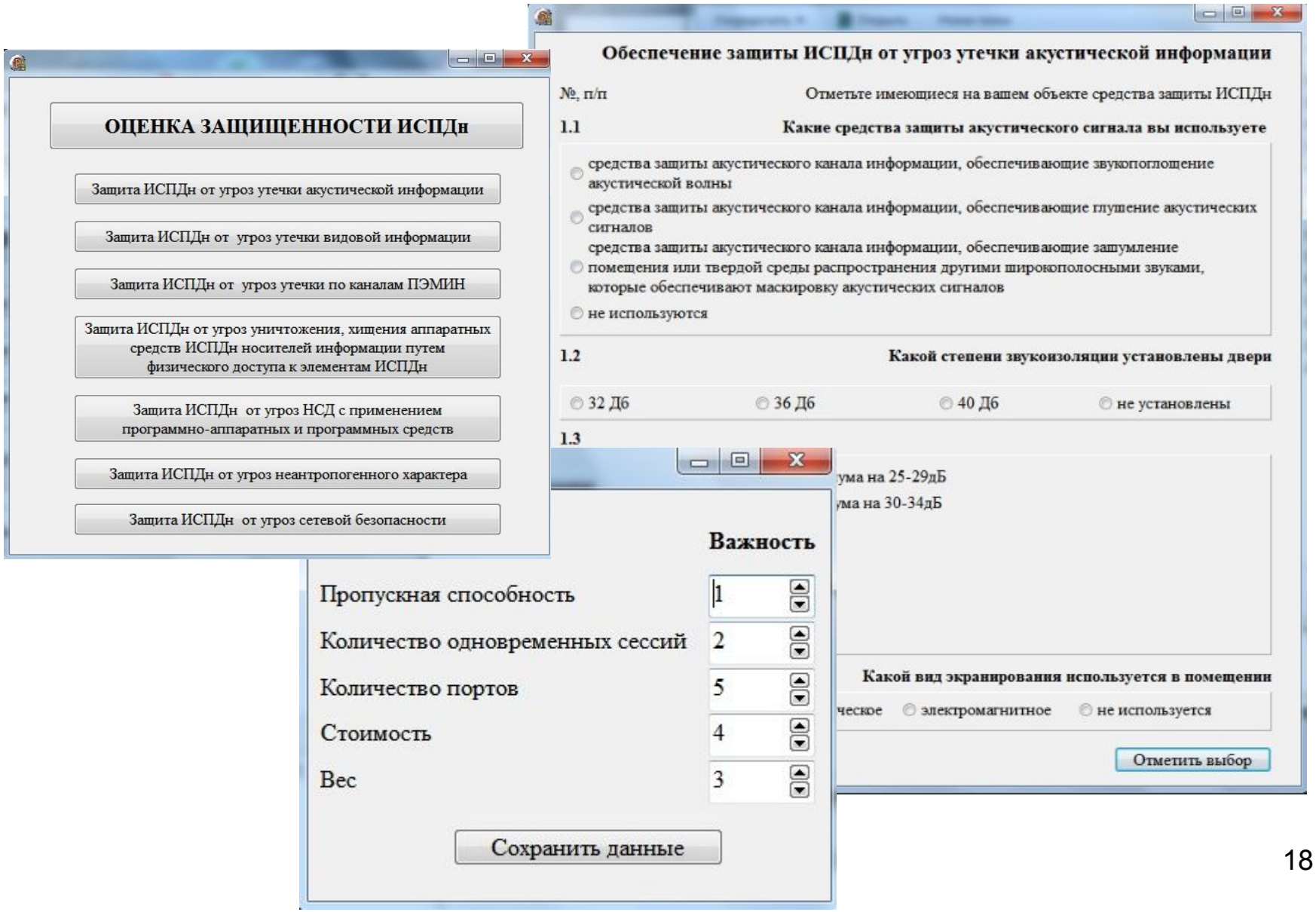
Руководитель Федеральной службы по интеллектуальной собственности, патентам и товарным знакам — Б.П. Симонов

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

Категорирование ПДн



Оценка защищенности ИСПДн



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