УДК 004.056.5

А.А. Шелупанов, В.Г. Миронова, С.С. Ерохин, А.А. Мицель

Автоматизированная система предпроектного обследования информационной системы персональных данных «АИСТ-П»

Рассматривается автоматизация первого этапа создания системы защиты персональных данных, которая носит название «Предпроектное обследование».
Ключевые слова: персональные данные, информационная система, модель угроз безопасности персональных данных.

Сегодня день вряд ли можно представить деятельность организации без обработки информации о человеке. Каждая организация хранит и обрабатывает персональные данные о сотрудниках, клиентах, поставщиках, партнерах и других физических лицах. Утечка, потеря или несанкционированное изменение персональных данных (ПДн) приводят к невосполнимому ущербу и наносят урон как деятельности предприятия, так и самому физическому лицу. Необходимость принятия мер по защите ПДн также продиктована возросшими техническими возможностями по копированию, использованию и распространению информации [4, 5].

ПДн – это важная и ценная информация о человеке, поэтому, заботясь о соблюдении прав своих граждан, государство требует от организаций и физических лиц обеспечить надежную защиту ПДн. Первым шагом стало принятие Федерального закона №152-ФЗ от 27.07.2006 г. «О персональных данных» [6]. Закон вступил в силу в январе 2007 г. Понятия «персональные данные», «оператор персональных данных», «информационная система персональных данных» четко определены в данном Федеральном законе.

В соответствии со ст. 19 Федерального закона «О персональных данных» оператор при обработке ПДн обязан принимать необходимые организационные и технические меры для их защиты от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, распространения и копирования и иных неправомерных действий, а следовательно, оператор ПДн должен обеспечивать безопасность ПДн при их обработке в информационной системе персональных данных (ИСПДн). Обеспечение безопасности ПДн достигается путем исключения действий, результат выполнения которых может привести с негативным последствиям для субъекта ПДн.

Рис. 1. Этапы создания СЗПДн

Безопасность ПДн обеспечивается с помощью системы защиты персональных данных (СЗПДн).

СЗПДн включает в себя организационные меры и средства защиты информации, а также используемые в информационной системе технологии. Рекомендуемые этапы создания СЗПДн показаны на рис. 1.

В статье рассмотрена первая стадия создания СЗПДн, которая носит название «Предпроектное обследование ИСПДн».

В предпроектное обследование включается:

– классификация ИСПДн;

– разработка организационно-распорядительной документации;

– определения степени исходной защищенности ИСПДн;

– разработка частной модели угроз безопасности ПДн;

– разработка частного технического задания.

Структура, состав и основные функции СЗПДн определяются исходя из класса ИСПДн. В соответствии с этим первым шагом при предпроектном обследовании является классификация ИСПДн.

Классификация ИСПДн проводится оператором ПДн согласно [1] и включает в себя следующее:

– сбор и анализ исходных данных об ИСПДн;

– присвоение ИСПДн соответствующего класса ИСПДн согласно требованиям [1];

– документальное оформление – Акт классификации ИСПДн.

Под сбором и анализом исходных данных об ИСПДн будем понимать следующие сведения:

– категория обрабатываемых ПДн (категория 1; 2; 3; 4) [1];

– объем обрабатываемых ПДн (1, 2, 3 – количество субъектов, ПДн которых обрабатываются в ИСПДн);

– наличие подключений ИСПДн к сетям связи общего пользования и (или) сетям международного информационного обмена;

– режим разграничения прав доступа пользователей ИСПДн;

– заданные оператором характеристики безопасности ПДн;

– структура ИСПДн (ИСПДн – автономная локальная либо распределенная);

– режим обработки ПДн;

– местонахождение технических средств ИСПДн.

На основе сведений, представленных выше, осуществляется процесс классификации ИСПДн.

Следующий шаг в предпроектном обследовании – разработка организационно-распорядительной документации по защите ПДн, которая включает в себя:

– положение о персональных данных и их защите;

– инструкцию о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные;

– приказы о возложении персональной ответственности за защиту ПД;

– нормативный документ (перечень), аккумулирующий информацию о персональных данных, обрабатываемых оператором (в том числе их категорию, объем и сроки хранения);

– перечень информационных систем, обрабатывающих персональные данные;

– регламент допуска сотрудников к обработке персональных данных;

– перечень допущенных сотрудников к обработке персональных данных;

– должностные инструкции сотрудников, имеющих отношение к обработке ПД.

После того как была разработана организационно-распорядительная документация по защите ПДн, определяется степень исходной защищенности ИСПДн. При определении степени исходной защищенности ИСПДн рассматриваются технические и эксплуатационные характеристики ИСПДн, такие как:

– территориальное размещение;

– наличие соединений с сетями общего пользования;

– встроенные (легальные) операции с записями баз ПДн;

– наличие разграничения доступа;

– наличие соединений с другими базами ПДн иных ИСПДн;

– уровень обобщения (обезличивания) ПДн;

– объем ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки.

При составлении перечня актуальных угроз безопасности ПДн каждой степени исходной защищенности ставится в соответствие числовой коэффициент Y_1, а именно: 0 – для высокой степени исходной защищенности; 5 – для средней степени исходной защищенности; 10 – для низкой степени исходной защищенности.

Важным шагом в предпроектном обследовании является построение частной модели угроз безопасности ПДн, так как результатом, полученным в результате построения модели угроз, будем руководствоваться при проектировании СЗПДн. СЗПДн должна базироваться на модели угроз безопасности ПДн.

Целью модели угроз является выявление актуальных угроз безопасности ПДн при их обработке в ИСПДн. Но прежде всего перед началом построения модели угроз необходимо определить тип исследуемой ИСПДн, а для этого обратимся к Акту классификации ИСПДн. Согласно [1], по заданным оператором характеристикам безопасности ПДн, обрабатываемых в информационной системе (ИС), ИСПДн подразделяются на типовые и специальные. Если для ИС, относящихся к типовым, необходимо рассматривать угрозы информационной безопасности, которые нарушают только конфиденциальность ПДн и их перечень приведен в [2], то для специальных ИС этого недостаточно. Важно отметить, что «специальные ИС – ИС, в которых вне зависимости от необходимости обеспечения конфиденциальности ПДн требуется обеспечить хотя бы одну из характеристик их безопасности, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, несанкционированного доступа)» [1], в дополнение к перечисленным ха-

рактеристикам также могут рассматриваться неотказуемость, учетность (подконтрольность), аутентичность (достоверность), поэтому перечень угроз, приведенный в [2], должен быть дополнен.

За основу были взяты типовые модели угроз безопасности ПДн, предложенные Федеральной службой по техническому и экспертному контролю (ФСТЭК России) согласно [2] и дополненные согласно требованиям для специальных ИС, в результате чего перечень угроз безопасности ПДн существенно расширяется.

Кроме того, согласно [1], были выделены следующие ИСПДн: автоматизированные рабочие места без подключения к сетям общего пользования и (или) сетям международного информационного обмена; автоматизированные рабочие места с подключением к сетям общего пользования и (или) сетям международного информационного обмена; локальные информационные системы без подключения к сетям общего пользования и (или) сетям международного информационного обмена; локальные информационные системы с подключениями к сетям общего пользования и (или) сетям международного информационного обмена; распределенные информационные системы без подключения к сетям общего пользования и (или) сетям международного информационного обмена; распределенные информационные системы с подключениями к сетям общего пользования и (или) сетям международного информационного обмена.

Модель угроз является комплексом, в котором содержатся максимально полное описание угроз безопасности ПДн и модель нарушителя безопасности ПДн. Для каждой ИСПДн авторами было выделено более 40 угроз безопасности ПДн.

В зависимости от уровня компетенции, технической оснащенности, возможности доступа нарушители делятся на категории, которые в совокупности образуют модель нарушителя.

Согласно [2] различают следующие категории нарушителей:

– N0 – внешний, не имеет санкционированного доступа к ИСПДн и ПДн;

– N1 – внутренний, имеющий санкционированный доступ к ИСПДн, но не имеющий доступ к ПДн;

– N2 – внутренний, зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места;

– N3 – внутренний, зарегистрированные пользователи ИСПДн, осуществляющие удаленный доступ к ПДн по локальным и (или) распределенным информационным системам;

– N4 – внутренний, зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента (фрагмента) ИСПДн;

– N5 – внутренний, зарегистрированные пользователи с полномочиями системного администратора ИСПДн;

– N6 – внутренний, зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн;

– N7 – внутренний, программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте;

– N8 – внутренний, разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на ИСПДн.

Таким образом, модель нарушителя содержит описание предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак.

Вероятность возникновения угрозы Y_2 относительно каждого нарушителя определяется экспертным путем и содержит четыре возможных значения Y_2: 0 – для маловероятной угрозы; 2 – для низкой вероятности угрозы; 5 – для средней вероятности угрозы; 10 – для высокой вероятности угрозы.

Согласно [3], с учетом вероятности возникновения угрозы и степени исходной защищенности коэффициент реализуемости угрозы Y будет определяться соотношением

$$Y = (Y_1 + Y_2)/20 .$$

По значению коэффициента реализуемости угрозы Y формируется интерпретация реализуемости угрозы следующим образом:

если $0 \le Y \le 0{,}3$, то возможность реализации угрозы признается низкой;

если $0{,}3 < Y \le 0{,}6$, то возможность реализации угрозы признается средней;

если $0{,}6 < Y \le 0{,}8$, то возможность реализации угрозы признается высокой;

если $Y > 0{,}8$, то возможность реализации угрозы признается очень высокой [3].

На основе экспертной оценки оценивается опасность каждой угрозы. Этот показатель имеет три значения: низкая; средняя; высокая опасности.

На основе предложенного подхода авторами создана автоматизированная система предпроектного обследования ИСПДн – «АИСТ-П», включающая этапы классификации ИСПДн, определения степени исходной защищенности ИСПДн, модели угроз безопасности ПДн.

Процесс классификации ИСПДн был автоматизирован, окна программы показаны на рис. 2–4.

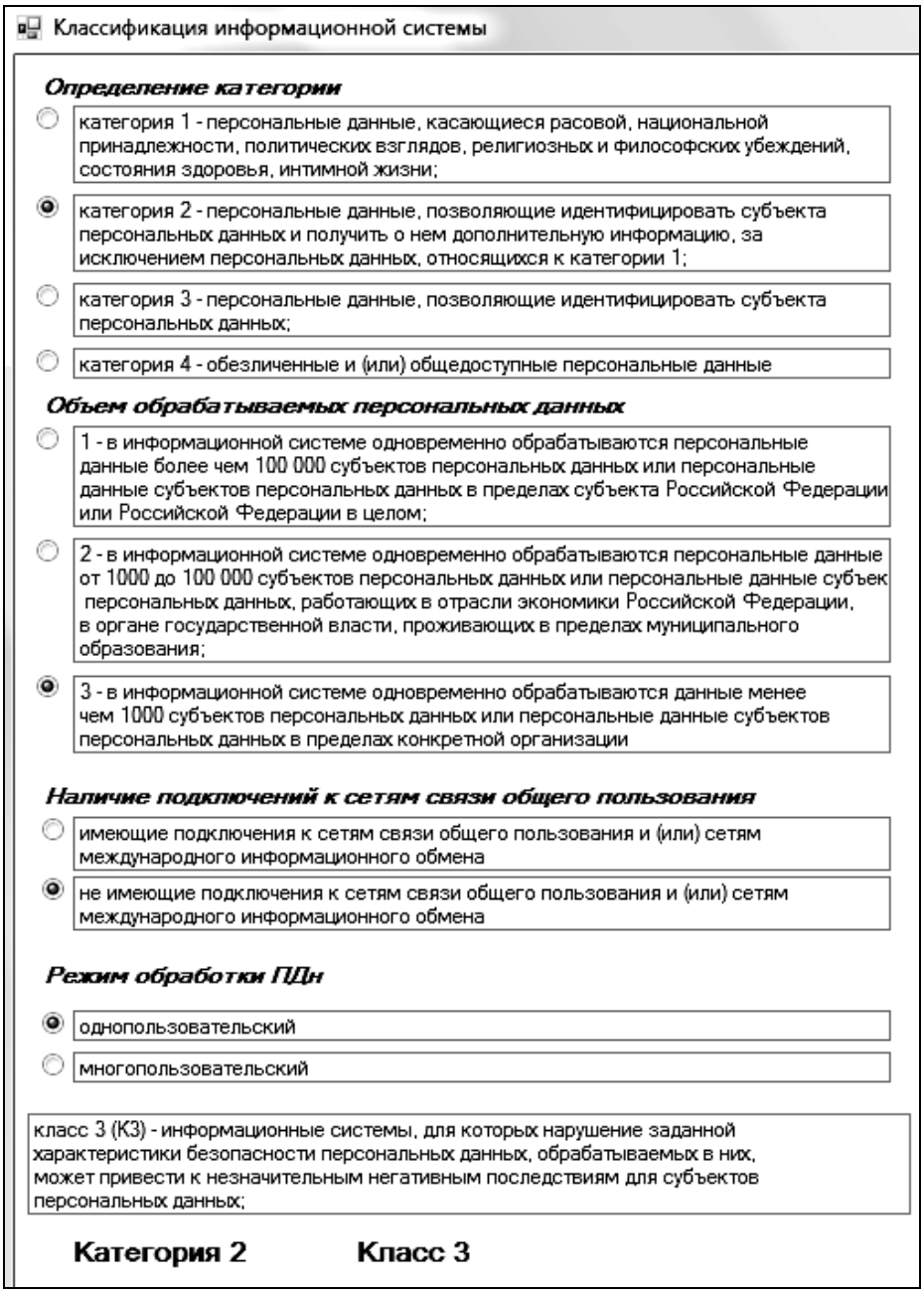

Рис. 2. Классификация ИСПДн

Процесс определения степени исходной защищенности был автоматизирован, окно программы показано на рис. 5–7.

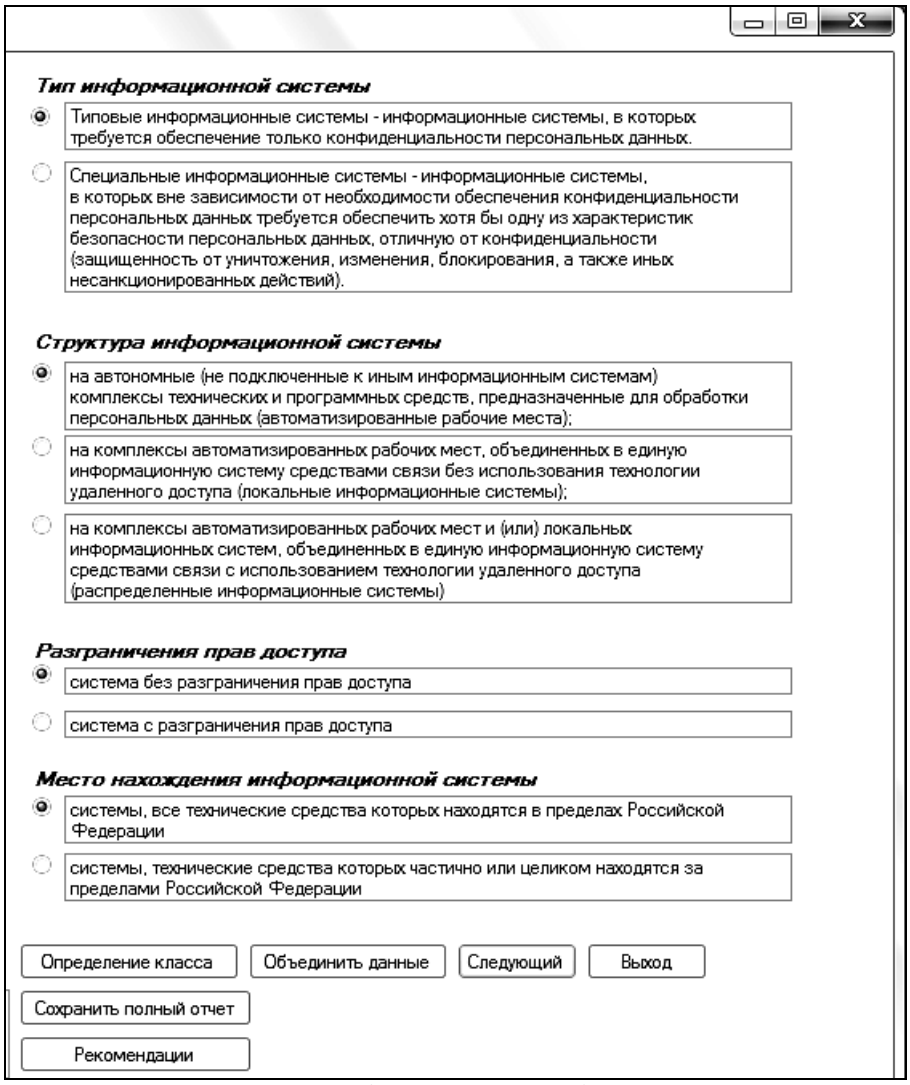

Рис. 3. Классификация ИСПДн

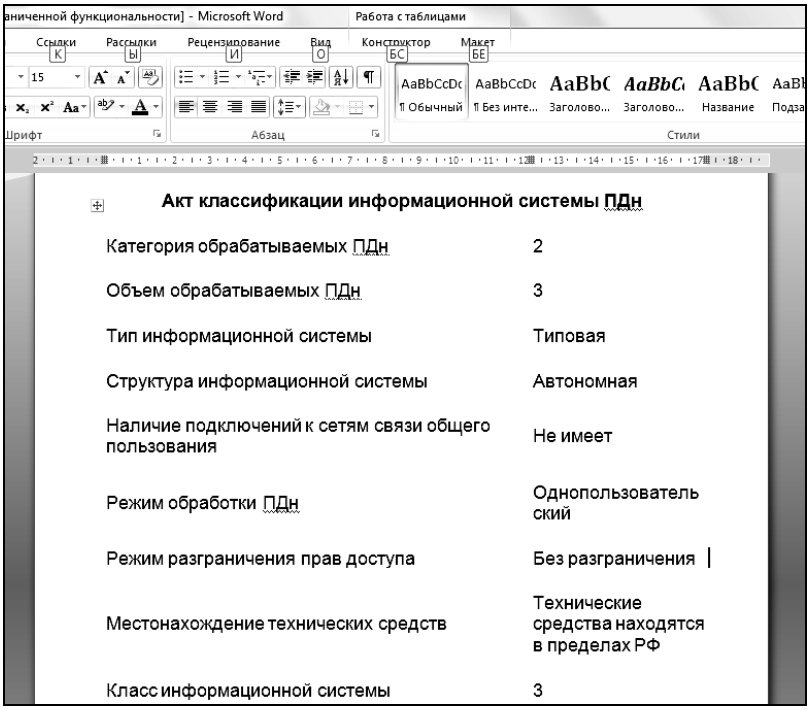

Рис. 4. Получение результата

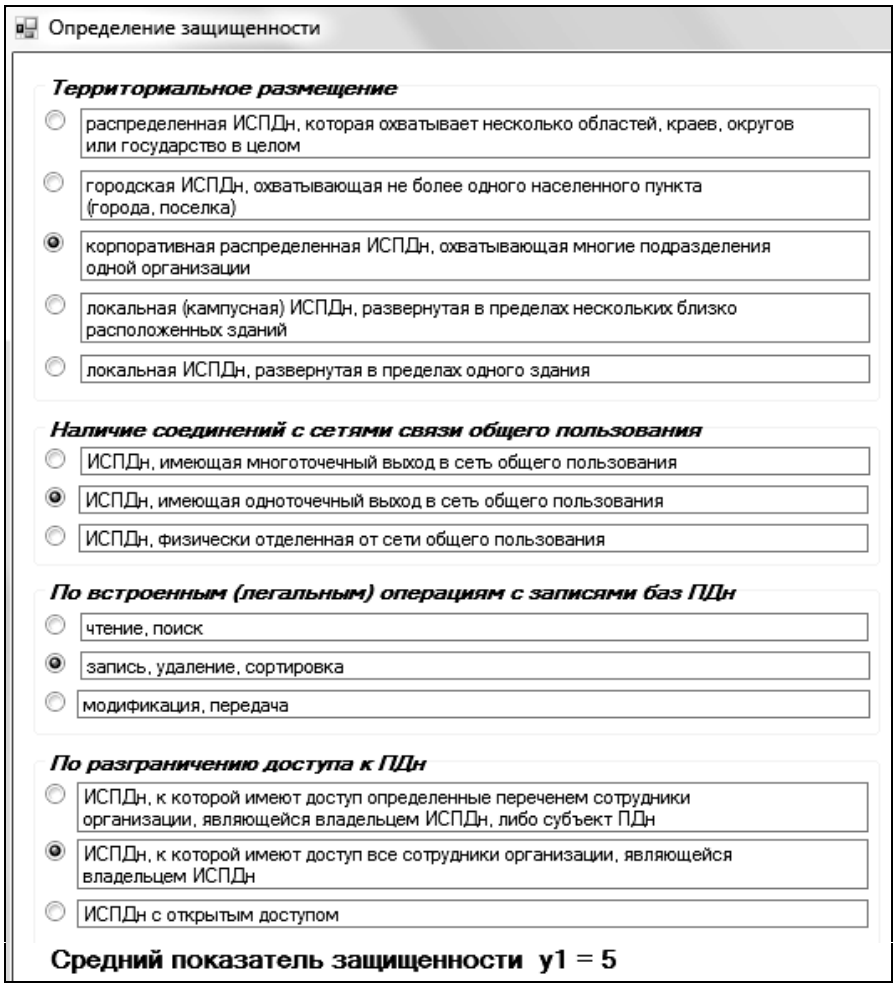

Рис. 5. Определение степени исходной защищенности

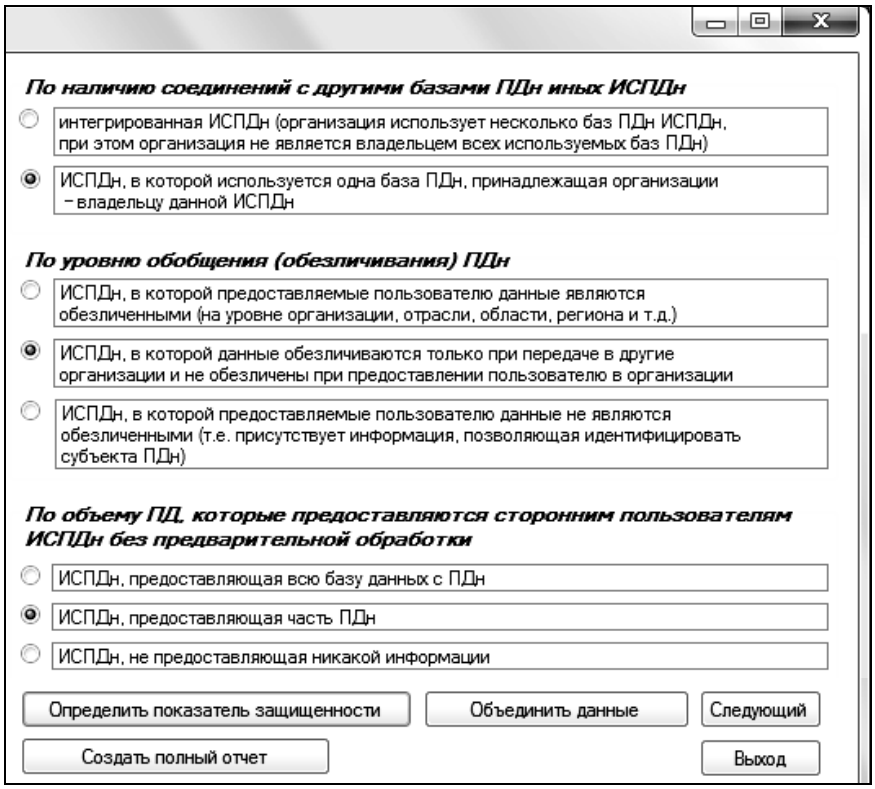

Рис. 6. Определение степени исходной защищенности

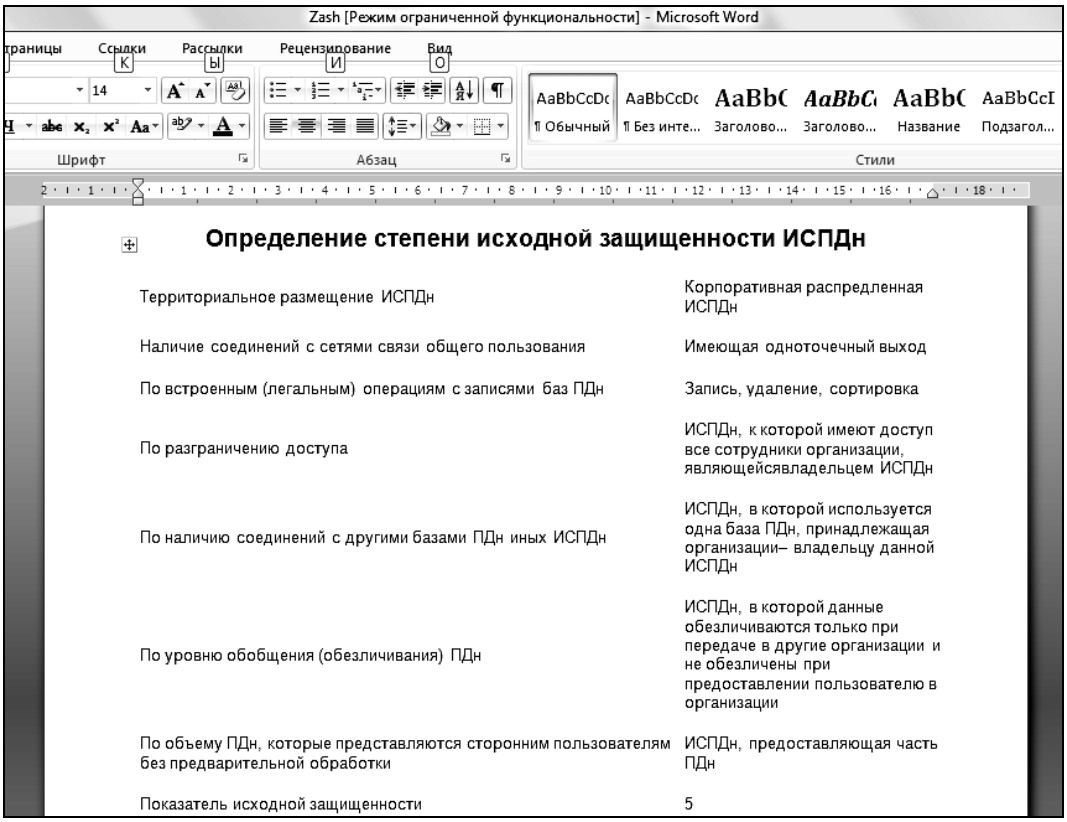

Рис. 7. Получение результата

На рис. 8–10 показана программная реализация модели угроз безопасности ПДн на примере автономной ИСПДн, не имеющей подключения к сетям связи общего пользования и (или) международного информационного обмена.

Специальная автономная информационная система без подключения к сети Интернет

Код	Наименование угрозы
1	угроза утечки акустического излучения информативного речевого сигнала
2	угроза утечки виброакустического сигнала
3	угроза утечки электрического сигнала
4	угроза утечки радиоизлучения
5	угроза утечки оптического излучения
6	угроза утечки видовой информации с экрана дисплеев
7	угроза утечки видовой информации с технических средств обработки графической, видео- и буквенно-цифровой информации
8	угроза внедрения специальных электронных устройств в помещения
9	угроза утечки ПЭМИ информативных сигналов от технических средств и линий передачи информации
10	угроза наводок информативного сигнала на цепи электропитания и линии связи
11	угроза утечки радиоизлучения
12	угроза перехвата паролей или идентификатора
13	угроза модификации программного обеспечения базовой системы ввода-вывода (BIOS)
14	угроза перехвата управления загрузкой с изменением необходимой технологической информации
15	угроза несанкционированного копирования информации обрабатываемой в ИСПДн
16	угроза несанкционированного копирования состава и конфигурации программно-аппаратных средств ИСПДн
17	угроза несанкционированного копирования состава и конфигурации средств защиты ПДн
18	угроза разглашения (публикации) защищаемой информации обрабатываемой в ИСПДн;
19	угроза разглашения (публикации) состава и конфигурации программно-аппаратных средств ИСПДн
20	угроза разглашения (публикации) состава и конфигурации средств защиты ПДн
21	угроза несанкционированного уничтожения защищаемой информации обрабатываемой в ИСПДн

Рис. 8. Программная реализация модели угроз безопасности ПДн

Нарушитель N0	Нарушитель N1	Нарушитель N2	Нарушитель N7	Нарушитель N8	Максимальное значение
5	0	0	0	0	5
0	2	0	0	0	2
0	0	5	0	0	5
0	0	0	10	0	10
0	0	0	2	5	5
0	0	0	0	0	0
0	0	0	0	0	0

Рис. 9. Программная реализация модели угроз безопасности ПДн

Коэффициент реализации	Возможность реализации	Опасность реализации	Актуальность реализации
0,5	Средняя	Низкая	Актуальная
0,35	Средняя	Средняя	Актуальная
0,5	Средняя	Средняя	Актуальная
0,75	Высокая	Высокая	Актуальная
0,5	Средняя	Низкая	Актуальная
0,25	Низкая	Низкая	Неактуальная
0,25	Низкая	Средняя	Неактуальная
0,25	Низкая	Средняя	Неактуальная

Рис. 10. Программная реализация модели угроз безопасности ПДн

Многообразие существующих ИСПДн вызывает необходимость систематизации знаний об объекте ПДн и ИСПДн. При этом определяющим фактором систематизации является наличие законодательства Российской Федерации и нормативно-правовой и методической базы.

Наличие большого объема рутинной работы, данных и информации об ИСПДн диктует потребность создания автоматизированной системы предпроектного обследования ИСПДн – «АИСТ-П».

Создание системы «АИСТ-П» позволяет оперативно проводить этапы классификации, определения степени исходной защищенности, создания частных моделей угроз.

Безусловно, уязвимым моментом при оценке каждой угрозы является наличие эксперта и экспертных оценок, противодействием этому авторы считают присутствие в автоматизированной системе «АИСТ-П» максимального перечня угроз, что позволяет однозначно учитывать вероятностные угрозы.

Литература

1. Приказ Федеральной службы по техническому и экспортному контролю, ФСБ РФ и Министерства информационных технологий и связи РФ от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных» [Электронный ресурс]. – Режим доступа: http://www.itsec.ru/articles2/Inf_security/porjadok-klassifikatsii-personalnyh-dannyh, свободный (дата обращения: 21.05.2010).

2. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных // Утверждена заместителем директора ФСТЭК России 15 февраля 2008 г. [Электронный ресурс]. – Режим доступа: http://www.fstec.ru/_spravs/model.rar,свободный (дата обращения: 21.05.2010).

3. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных // Утверждена заместителем директора ФСТЭК России 15 февраля 2008 г. [Электронный ресурс]. – Режим доступа: http://www.fstec.ru/_spravs/metodika.doc,свободный (дата обращения: 21.05.2010).

4. Шелупанов А.А. Специальные вопросы информационной безопасности / А.А. Шелупанов, Р.В. Мещеряков. – Томск: Изд-во ин-та оптики атмосферы СО РАН, 2003. – 224 с.

5. Мещеряков Р.В. Комплексное обеспечение информационной безопасности автоматизированных систем / А.А. Шелупанов, Р.В. Мещеряков. – Томск: В-Спектр, 2007. – 278 с.

6. О персональных данных: Федеральный закон № 152-ФЗ, утвержден Президентом Российской Федерации 27 июля 2006 г. [Электронный ресурс]. – Режим доступа: http://www.rg.ru/2006/07/29/personaljnye-dannye-dok.html, свободный (дата обращения: 21.05.2010).

Шелупанов Александр Александрович
Доктор техн. наук, профессор, проректор по научной работе ТУСУРа
Эл. адрес: saa@udcs.ru

Миронова Валентина Григорьевна
студентка 5-го курса каф. комплексного обеспечения информационной безопасности электронно-вычислительных систем факультета вычислительных систем, ТУСУРа
Эл. адрес: mvg@security.tomsk.ru

Ерохин Сергей Сергеевич
Инженер каф. комплексной информационной безопасности ТУСУРа
Эл. адрес: ess@security.tomsk.ru

Мицель Артур Александрович
Доктор техн. наук, профессор, каф. автоматизированных систем управления ТУСУРа
Эл. адрес: maa@asu.tusur.ru

A.A. Shelupanov, V.G. Mironova, S.S. Erokhin, A.A. Mitcel
Computer-based system for vetting information system of personal data – «AIST-P»

We consider the automation of the first phase of the system of protection of personal data, which is called «Pre-Survey».
Keywords: personal data, information system, model of security threats of personal data.
