УДК 004.056.5

В.Г. Миронова, А.А. Шелупанов

Предпроектное проектирование информационных систем персональных данных как этап аудита информационной безопасности

Рассмотрен этап аудита информационной безопасности для стадии предпроектного обследования информационной системы персональных данных.
Ключевые слова: персональные данные, аудит, информационная система.

Информационные системы подвергаются всевозможным угрозам, порождая угрозы безопасности государству, обществу и личности. В связи с этим необходимо обеспечить защиту конфиденциальной информации, а именно, персональных данных (ПДн) граждан, обрабатываемых в информационных системах персональных данных (ИСПДн).

В Федеральном законе №152-ФЗ «О персональных данных» определены понятия «персональные данные», «субъект персональных данных», «оператор персональных данных» и «информационная система персональных данных». Согласно [1], все ИСПДн не позднее 1 января 2011 г. должны быть приведены в соответствии с требованиями нормативно-методической документации и законодательства РФ, а каждый оператор ПДн – владелец ИСПДн – обязан провести необходимые организационные и технические мероприятия для защиты ПДн от неправомерных действий.

В перечень мероприятий по приведению ИСПДн в соответствии с требованиями нормативно-методической документации и законодательства по защите ПДн включается:

– предпроектное обследование ИСПДн;
– проектирование системы защиты персональных данных (СЗПДн);
– ввод в действие СЗПДн.

Среди этих этапов именно предпроектное обследование ИСПДн является отправной точкой для создания СЗПДн и проведения последующих мероприятий. Поэтому данный этап, являясь по существу этапом аудита информационной безопасности, требует особого рассмотрения.

Выбор и реализация методов и способов защиты информации в ИСПДн основываются на результатах, полученных при проведении предпроектного обследования.

Предпроектное обследование ИСПДн включает:

– классификацию ИСПДн;
– разработку организационно-распорядительной документации;
– определение исходной степени защищенности ИСПДн;
– разработку частной модели угроз безопасности ПДн;
– создание частного технического задания.

Согласно [2], классификация ИСПДн проводится каждым оператором ПДн отдельно для установления методов и способов защиты информации, необходимых для обеспечения безопасности ПДн. Результаты классификации оформляются соответствующим актом классификации, в соответствии с типовой формой.

Организационно-распорядительная документация – положение о защите ПДн, различные инструкции, приказы, регламенты, нормативные документы и т.д. – является базой для построения ИСПДн.

Основным моментом предпроектного обследования является построение частной модели угроз безопасности ПДн, состоящее в определении перечня актуальных угроз безопасности ПДн [3]. Согласно [3–4] выявляется исходная степень защищенности ИСПДн и строится частная модель угроз безопасности ПДн. Для этого рассматриваются эксплуатационные и технические характеристики. На основе модели угроз и будет создаваться СЗПДн. Классификация угроз безопасности ПДн представлена на рис. 1. Кроме того, необходимо рассматривать модели нарушителей безопасности ПДн согласно [4–5].

На основе перечня актуальных угроз составляется частное техническое задание [6], в котором отражаются основные критерии построения СЗПДн.

Автоматизированная система, реализованная авторами [7], позволяет оперативно проводить следующие этапы предпроектного обследования ИСПДн: классификации ИСПДн, определение исходной степени защищенности ИСПДн и построения частных моделей угроз безопасности ПДн.

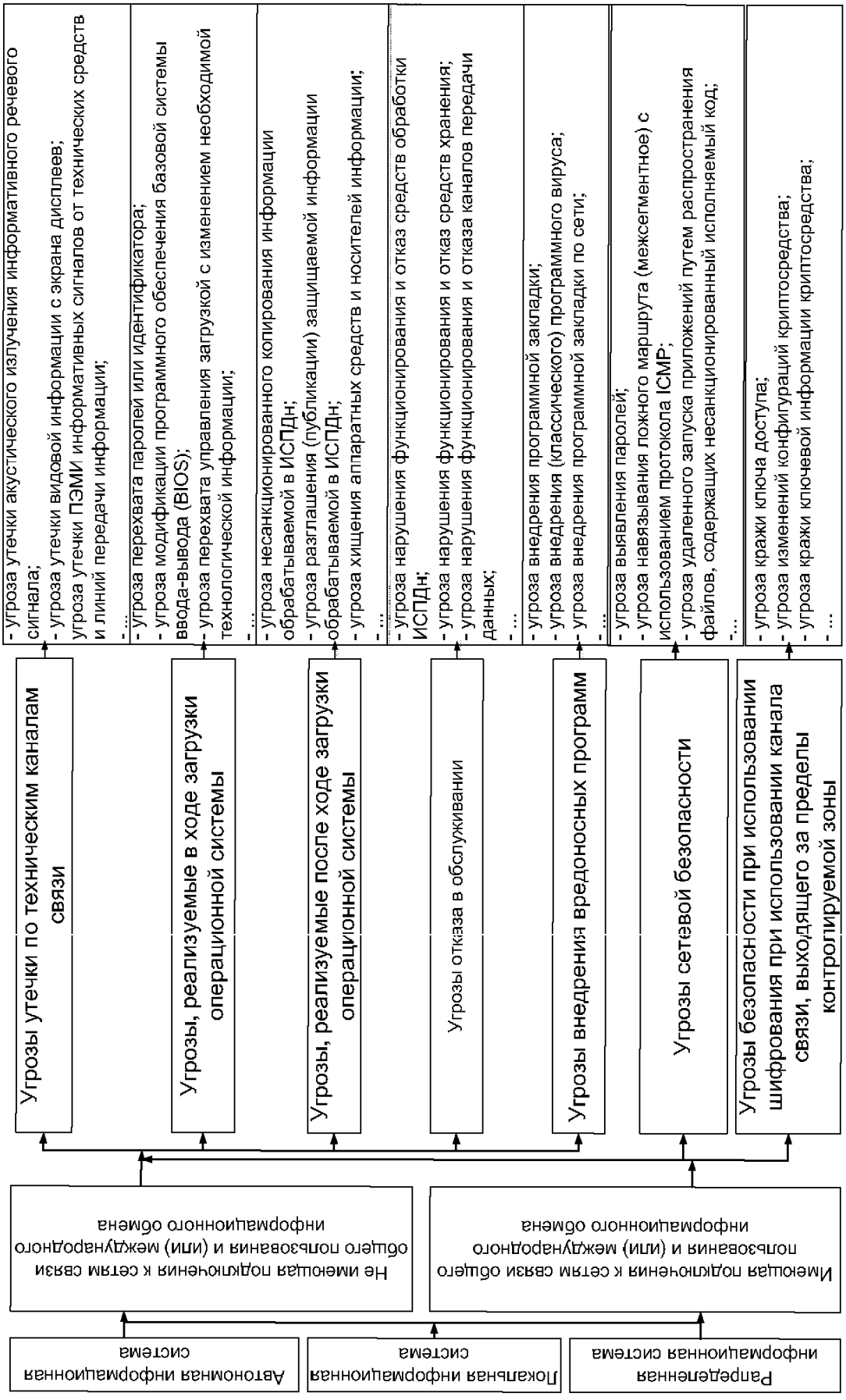

Рис. 1. Классификация угроз безопасности ПД

Выводы

Таким образом, при проведении предпроектного обследования – этапа аудита информационной безопасности – важно помнить, что полученный результат ляжет в основу будущей СЗПДн, обеспечивающей заданный уровень защищенности ПДн.

Авторами сформированы перечни угроз безопасности ПДн для специальных ИСПДн согласно [4–5], а также рассмотрены возможные модели – нарушители для ИСПДн в зависимости от структуры системы.

Литература

1. 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 10.10.2010).

2. 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 10.10.2010).

3. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных / Утверждена заместителем директора ФСТЭК России от 15.02.2008 г. [Электронный ресурс]. – Режим доступа: http://www.fstec.ru/_spravs/metodika.rar, свободный (дата обращения 10.10.2010).

4. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных / Утверждена заместителем директора ФСТЭК России от 15.02.2008 г. [Электронный ресурс]. – Режим доступа: http://www.fstec.ru/_spravs/model.rar, свободный (дата обращения 10.10.2010).

5. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации / Утверждена Руководством 8 Центра ФСБ России от 21 февраля 2008 г. № 149/5-144. [Электронный ресурс]. – Режим доступа: http://pd.rsoc.ru/law/document56.htm?print=1, свободный (дата обращения 10.10.2010).

6. Приказ Федеральной службы по техническому и экспертному контролю Российской Федерации от 5 февраля 2010 г. № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных» [Электронный ресурс]. – Режим доступа: http://www.fstec.ru/_docs/doc_781.htm, свободный (дата обращения 10.10.2010).

7. Шелупанов А.А. Автоматизированная система предпроектного обследования информационной системы персональных данных «АИСТ-П» / А.А. Шелупанов, В.Г. Миронова и др. //Доклады Том. гос. ун-та систем управления и радиоэлектроники. – 2010. – № 1(21). – Ч. 1. – С. 14-22.

Миронова Валентина Григорьевна
Инженер каф. комплексного обеспечения информационной безопасности электронно-вычислительных систем (КИБЭВС) ТУСУРа
Тел.: 8-923-415-16-08
Эл. почта: mvg@security.tomsk.ru

Шелупанов Александр Александрович
Д-р техн. наук, проф., проректор по научной работе ТУСУРа
Тел.: 8 (382-2) 51-43-02
Эл. почта: saa@udcs.ru

Mironova V.G., Shelupanov A.A.

Pre-project design of personal data information systems as a stage of the information security audit

A stage of the information security audit for the pre-project analysis of a personal data information system.

Keywords: personal data, audit, information system.