M. A. Masyuk

ANALYSIS AND VISUALIZATION SYSTEM OF RELATIONS OF NORMATIVE LEGAL DOCUMENTS IN LEGAL-REFERENCE SYSTEMS

In the article the author considers the present situation in the Russian Federation, resulted from rapid growth of quantity of legislative documents have being passed. The significant part of these laws is of corrective nature; it means that such documents contain references to other certificates. Analysis of a great number of documents with their interrelations is a difficult routine work, requiring the presence of highly skilled specialists. The author proposes a complex approach to improvement of the legal-reference systems and electronic databases by integration into them of the system, realizing visual display of documents, and analysis of correlation for the purpose of their conformity to the norms of lawmaking. Theoretical basis and practical implementation features of the system are introduced in this article as well.

Keywords: normative legal document, analysis, visualization.

УДК 004.056

В. Г. Миронова, А. А. Шелупанов

АНАЛИЗ ЭТАПОВ ПРЕДПРОЕКТНОГО ОБСЛЕДОВАНИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Рассмотрены основные этапы, входящие в первую стадию создания системы защиты персональных данных, которая носит название «Предпроектное обследование».

Ключевые слова: персональные данные, информационная система, модель угроз безопасности персональных данных.

Деятельность большинства организаций связана с использованием при обработке и передаче данных информации о сотрудниках, клиентах, поставщиках и т. д.

Персональные данные (ПДн) – это важная информация о человеке, поэтому для соблюдения прав и свобод граждан РФ государство требует от организаций и физических лиц обеспечить надежную защиту ПДн. Федеральный закон № 152-ФЗ от 27 мая 2006 г. «О персональных данных», вступивший в силу в январе 2007 г., четко определяет понятия «персональные данные», «оператор персональных данных» и «информационная система персональных данных» [1].

Ответственность за обеспечение безопасности ПДн ст. 19 этого закона возлагает на оператора ПДн. Обеспечение безопасности ПДн достигается путем построения адекватной системы защиты персональных данных (СЗПДн), исключающей действия, результат выполнения которых может привести к негативным последствиям для субъекта ПДн.

Рекомендуемыми этапами создания СЗПДн являются:

а) предпроектное обследование информационной системы персональных данных (ИСПДн):

– классификация ИСПДн;

– разработка организационно-распорядительной документации;

– определение степени исходной защищенности ИСПДн;

– создание частной модели угроз безопасности ПДн;

– разработка частного технического задания;

б) проектирование СЗПДн;

в) ввод в действие СЗПДн.

Остановимся более подробно на этапе предпроектного обследования информационной системы (ИС) персональных данных, являющегося основой для построения адекватной СЗПДн.

Классификацию ИСПДн (рис. 1) необходимо проводить в соответствии с требованиями [2] с учетом следующих исходных данных:

а) категории обрабатываемых ПДн в ИСПДн:

– категория 1 – ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

– категория 2 – ПДн, позволяющие идентифицировать субъекта ПДн и получить о нем дополнительную информацию, за исключением ПДн, относящихся к категории 1;

– категория 3 – ПДн, позволяющие идентифицировать субъекта ПДн;

– категория 4 – обезличенные и (или) общедоступные ПДн;

б) объема обрабатываемых ПДн (количества субъектов ПДн, ПДн которых обрабатываются в ИС):

– категория 1 – в ИС одновременно обрабатываются ПДн более чем 100 000 субъектов ПДн или ПДн субъектов ПДн в пределах субъекта РФ или РФ в целом;

– категория 2 – в ИС одновременно обрабатываются ПДН от 1 000 до 100 000 субъектов ПДн или

ПДн субъектов ПДн, работающих в отрасли экономики РФ, в органе государственной власти, проживающих в пределах муниципального образования;

– категория 3 – в ИС одновременно обрабатываются данные менее чем 1 000 субъектов ПДн или ПДн субъектов ПДн в пределах конкретной организации.

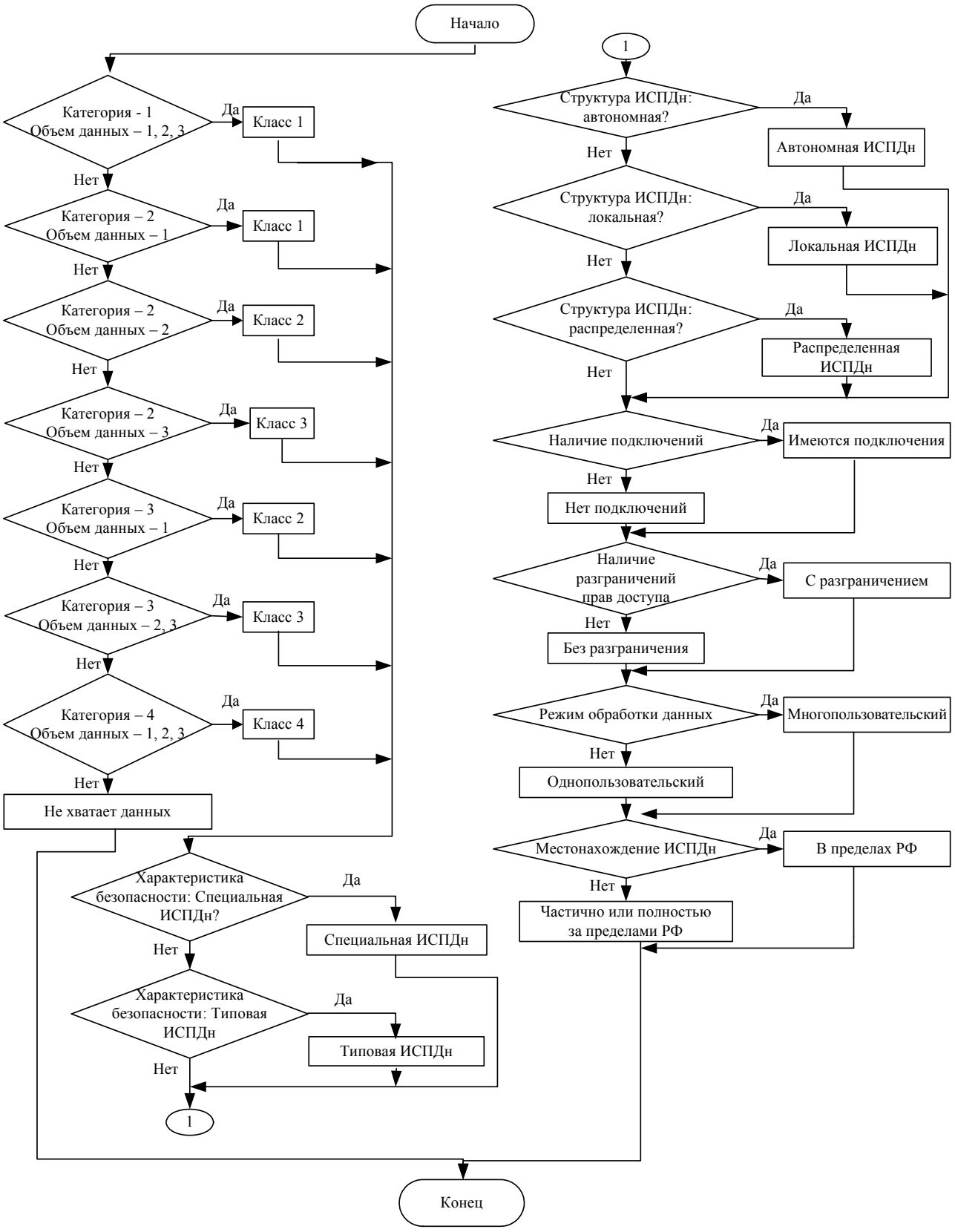

Рис. 1. Алгоритм классификации ИСПДн

В зависимости от категории и объема обрабатываемых ПДн выделяют четыре класса ИСПДн [2], для каждого из которых определены методы и способы защиты информации в информационных системах. К ним относятся:

– методы и способы защиты информации, обрабатываемой техническими средствами ИС, от несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия;

– методы и способы защиты речевой информации, а также информации, представленной в виде информативных электрических сигналов, физических полей, от несанкционированного доступа к ПДн, результатом которого может стать копирование, распространение ПДн, а также иных несанкционированных действий [3].

Методы и способы защиты информации, например, для ИСПДн 3-го класса (однопользовательский режим) могут быть представлены в следующем виде:

– управление доступом: идентификация и проверка подлинности пользователя при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

– регистрация и учет: регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешный или неуспешный), учет всех защищаемых носителей информации с помощью их маркировки, занесение учетных данных в журнал учета;

– обеспечение целостности: обеспечение целостности программных средств системы защиты ПДн, обрабатываемой информации, а также неизменность программной среды. Целостность программных средств проверяется при загрузке системы по наличию имен компонентов системы защиты ПДн, а целостность программной среды обеспечивается отсутствием средств разработки и отладки программ во время обработки и (или) хранения ПДн. Физическая охрана предусматривает контроль доступа в помещения, наличие надежных препятствий для несанкционированного проникновения в помещения и хранилище носителей ПДн, периодическое тестирование функций СЗПДн при изменении программной среды и пользователей с помощью тест-программ, наличие средств восстановления СЗПДн, предусматривающих ведение двух копий, их периодическое обновление и контроль. Необходимость в контроле наличия (отсутствия) недекларированных возможностей программного обеспечения средств защиты информации, применяемых в информационных системах 3-го класса, определяется уполномоченным лицом – оператором ПДн.

Согласно [3], перечисленные выше методы и способы защиты информации для информационных систем 3-го класса представлены в виде рекомендаций. Для того чтобы определить, какие именно методы и способы защиты должны быть реализованы для конкретной ИСПДн, необходимо составление перечня актуальных угроз безопасности ПДн. Актуальность угрозы определяется на основе данные об эксплуатационных и технических характеристиках ИСПДн, а также экспертной оценки опасности каждой угрозы (рис. 2).

Заключительным этапом предпроектного обследования является разработка частного технического задания на построение СЗПДн, в котором отражаются основные требования к СЗПДн и ее характеристикам. При составлении технического задания на создание СЗПДн необходимо руководствоваться результатами, полученными при проведении классификации ИСПДн и построении модели угроз безопасности ПДн.

Таким образом, авторами проведен анализ первого этапа создания СЗПДн – предпроектного обследования, в ходе которого обозначены основные стадии проведения предпроектного обследования ИСПДн: классификация ИСПДн; разработка организационно-распорядительной документации; определение степени исходной защищенности ИСПДн; разработка частной модели угроз безопасности ПДн; разработка частного технического задания. Необходимо отметить, что представленный подход удовлетворяет требованиям законодательства в области защиты ПДн и является основополагающим для построения адекватной СЗПДн.

Библиографические ссылки

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

2. Об утверждении Порядка проведения классификации информационных систем персональных данных [Электронный ресурс] : приказ Федер. службы по техн. и экспорт. контролю, Федер. службы безопасности Рос. Федерации и М-ва информ. технологий и связи Рос. Федерации № 55/86/20 от 13 февр. 2008 г. URL: http://www.fstec.ru/_docs/doc_781.htm.

3. Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных [Электронный ресурс] : приказ Федер. службы по техн. и эксперт. контролю Рос. Федерации № 58 от 5 февр. 2010 г. URL: http://www.fstec.ru/_docs/doc_781.htm.

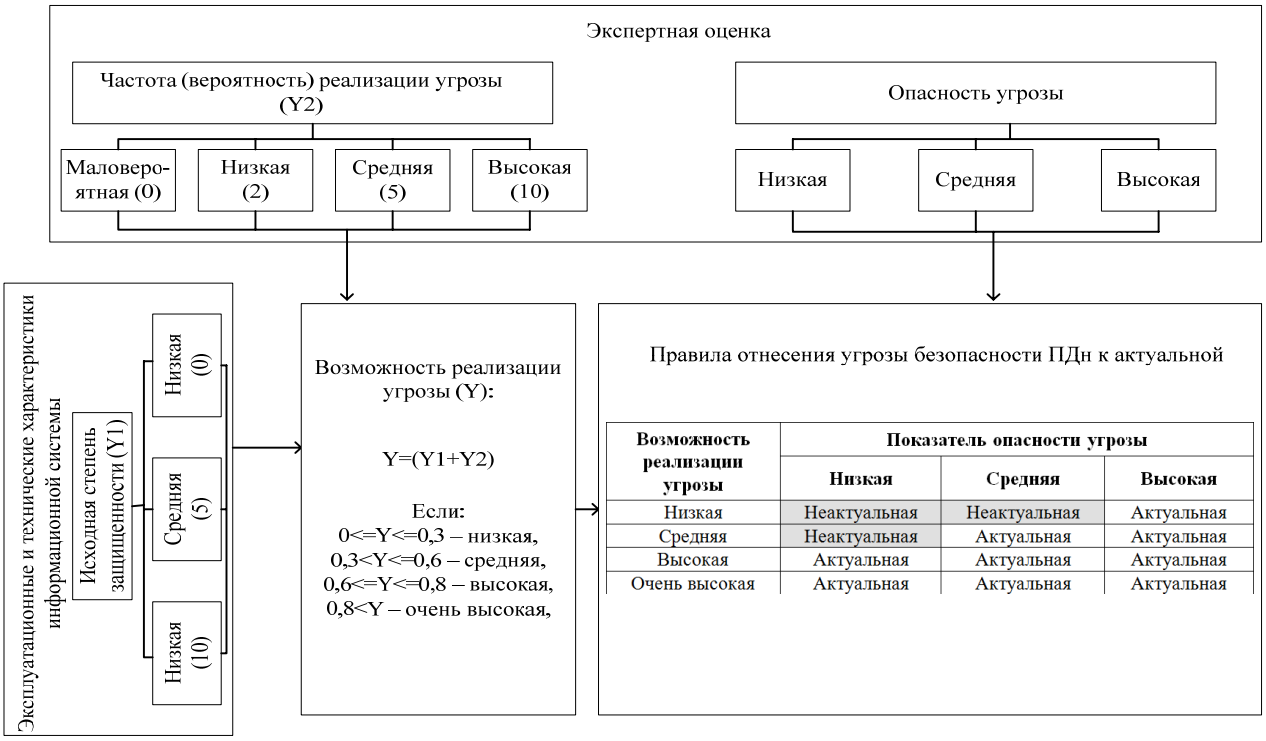

Рис. 2. Схема отнесения к актуальной угрозе безопасности ПДн

V. G. Mironova, A. A. Shelupanov

ANALYSIS OF STAGES PREPROJECT SURVEY INFORMATION SYSTEM OF PERSONAL DATA

This article describes and analyzes the main stages included in the first stage of creation of a system of protection of personal data, which is called "Preproject". The article examines the stages of audit information security for the stage of pre-survey information system of personal data.

Keywords: personal data, audit, information system.

УДК 519.62

В. А. Нестеров

КОНЕЧНО-ЭЛЕМЕНТНЫЙ РАСЧЕТ ТРЕХСЛОЙНОЙ БАЛКИ

Рассматривается новый конечный элемент балки, в расчетах которой учитывается трансверсальный сдвиг. При этом в каждом из узлов конечного элемента в качестве основных кинематических параметров присутствуют осредненные по толщине углы трансверсального сдвига. Представлены результаты численного исследования, демонстрирующие отсутствие эффекта сдвигового запирания в новой балочной конечно-элементной модели.

Ключевые слова: балка, трансверсальный сдвиг, метод конечных элементов, эффект сдвигового запирания.

В последнее время в авиационной и ракетно-космической отрасли все чаще применяются новые конструкционные материалы, позволяющие изготавливать технику разнообразного назначения с высокими удельными характеристиками. Среди прочих особое место занимают композиционные материалы. Обладая высокой удельной прочностью и жесткостью, композиты, кроме того, позволяют проектировать конструкции с требуемыми механическими свойствами в зависимости от их назначения и условий экс-