Н.Г. Топольский, Д.Н. Гришечкин
(ГУ МЧС России по Пензенской области; e-mail: grishechkin.76@mail.ru)

ПОРЯДОК ОПРЕДЕЛЕНИЯ КЛАССА ЗАЩИЩЁННОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ И ВЫБОРА СРЕДСТВ ЗАЩИТЫ

Разработан порядок определения класса защищённости автоматизированных систем и последующего выбора средств защиты.

Ключевые слова: автоматизированная система, обрабатываемая информация, средства защиты.

N.G. Topolsky, D.N. Grishechkin

THE PROCEDURE FOR DETERMINING THE CLASS OF SECURITY AUTOMATED SYSTEMS AND SELECTION MEANS OF PROTECTION

Designed procedure for determining class of security of the automated systems and the subsequent choice of means of protection.

Key words: automated system, processed information, means of protection.

Статья поступила в редакцию Интернет-журнала 8 ноября 2015 г.

Несмотря на то, что законодательство в области защиты автоматизированных систем появилось достаточно давно, защита персональных данных в них как процесс появился сравнительно недавно. Ввиду того, что автоматизированные системы нашли своё применение в каждой организации и обеспечивают (полностью или частично) её деятельность в настоящее время особую актуальность приобретают вопросы классификации существующих в организации автоматизированных систем и последующего выбора для них средств защиты.

Порядок определения класса защищённости автоматизированной системы (далее по тексту АС) и выбора средств защиты можно представить следующим образом (рис.1).

Параметрами определения класса защищённости являются:

- вид обрабатываемой в АС информации;
- тип АС: однопользовательская или многопользовательская;
- уровни конфиденциальности информации: один уровень конфиденциальности или разные уровни конфиденциальности [1].

Для однозначного определения класса автоматизированной системы можно сформировать следующую опросную анкету:

1. АС является многопользовательской?
   а) да б) нет.
2. Все пользователи имеют одинаковые права доступа к информации?
   а) да б) нет.
3. В АС обрабатывается информация под грифом "Особой важности"?
   а) да б) нет.

4. В АС обрабатывается информация под грифом "Совершенно секретно"?

а) да б) нет.

5. В АС обрабатывается информация под грифом "Секретно"?

а) да б) нет.

6. В АС обрабатывается конфиденциальная информация?

а) да б) нет.

7. В АС обрабатываются персональные данные?

а) да б) нет.

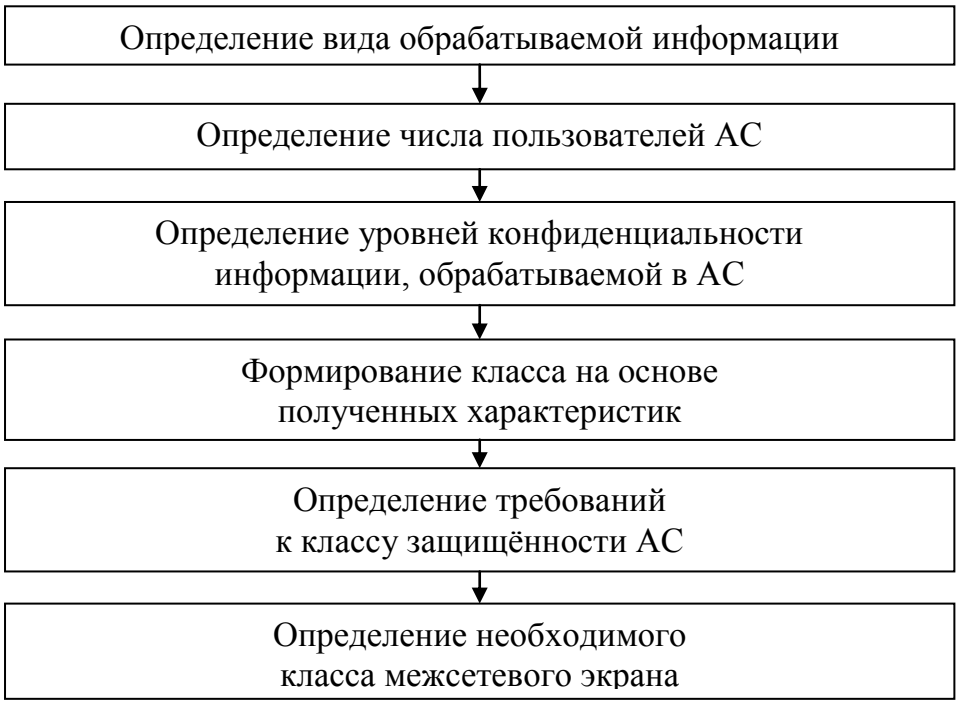

Рис. 1. Порядок определения класса защищённости АС и выбора средств защиты

Результаты ответов на вопросы можно представить в виде следующих комбинаций:

1.а∧2.б∧3.а = класс 1А;

1.а∧2.б∧3.б∧4.а = класс 1Б;

1.а∧2.б∧3.б∧4.б∧5.а = класс 1В;

1.а∧2.б∧3.б∧4.б∧5.б∧6.а = класс 1Г;

1.а∧2.б∧3.б∧4.б∧5.б∧6.б∧7.а= класс 1Д;

1.а∧2.а∧ (3.а∨4.а∨5.а) = класс 2А;

1.а∧2.а∧3.б∧4.б∧5.б∧ (6.а∨7.а) = класс 2Б;

1.б∧ (3.а∨4.а∨5.а) = класс 3А;

1.б∧3.б∧4.б∧5.б∧ (6.а∨7.а) = класс 3Б,

где ∧ – логическое "И", ∨ – логическое "ИЛИ".

В соответствии с пунктом 5.2.3 Специальных требований и рекомендаций по защите конфиденциальной информации " …АС, обрабатывающие персональные данные, должны быть отнесены по уровню защищённости к классам 3Б, 2Б и не ниже 1Д..." [2].

На основании данных требований можно сформировать таблицу, отражающую требования и средства защиты, соответствующие данным требованиям [3] (табл. 1).

Таблица 1

Выбор средств защиты в соответствии с классом АС

Подсистемы и требования	Наименование класса			Средства защиты
	3Б	2Б	1Д	
1	2	3	4	5
1. Подсистема управления доступом				
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:				
в систему	+	+	+	Система защиты информации от несанкционированного доступа "Dallas Lock 7.7" StoneGateIPS TrafficMonitor 3.3 ПАНЦИРЬ-С SecretNet-K 6 SecurityStudioEndPoint Protection
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	-	-	-	-
к программам	-	-	-	-
к томам, каталогам, файлам, записям, полям записей	-	-	-	-
1.2. Управление потоками информации	-	-	-	-
2. Подсистема регистрации и учёта				
2.1. Регистрация и учёт:				
входа (выхода) субъектов доступа в (из) систему(ы) (узел сети)	+	+	+	Программно-аппаратный комплекс "Соболь"
выдачи печатных (графических) выходных документов	-	-	-	-
запуска (завершения) программ и процессов (заданий, задач)	-	-	-	-
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	-	-	-	-

Продолжение табл. 1

1	2	3	4	5
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	-	-	-	-
изменения полномочий субъектов доступа	-	-	-	-
создаваемых защищаемых объектов доступа	-	-	-	-
2.2. Учёт носителей информации	+	+	+	Kaspersky Business Space Security Certified Media Pack
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	-	-	-	-
2.4. Сигнализация попыток нарушения защиты	-	-	-	-
3. Криптографическая подсистема				
3.1. Шифрование конфиденциальной информации	-	-	-	-
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	-	-	-	-
3.3. Использование аттестованных криптографических средств	-	-	-	-

Окончание табл. 1

1	2	3	4	5
4. Подсистема обеспечения целостности				
4.1. Обеспечение целостности программных средств и обрабатываемой информации	+	+	+	Программно-аппаратный комплекс "Соболь" DeviceLock 6.4 TrafficMonitor 3.3 ЧОП "Страж 32", Kaspersky Crystal 3.0 Diamond ACS ПЛУТОН-М Flagman-Z
4.2. Физическая охрана средств вычислительной техники и носителей информации	+	+	+	
4.3. Наличие администратора (службы) ЗИ в АС	-	-	-	
4.4. Периодическое тестирование СЗИ НСД	+	+	+	
4.5. Наличие средств восстановления СЗИ НСД	+	+	+	
4.6. Использование сертифицированных средств защиты	-	-	-	

Средства защиты, рекомендованные для указанных классов автоматизированных систем, чаще всего целесообразно устанавливать при проведении процедуры аттестации автоматизированных рабочих мест, обрабатывающих персональные данные [4].

Литература

1. ***Руководящий документ*** "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации", утверждён решением председателя Государственной технической комиссии при Президенте Российской Федерации 30 марта 1992 г.

2. ***Нормативно-методический документ*** "Специальные требования и рекомендации по технической защите конфиденциальной информации", утверждён приказом Гостехкомиссии России от 30 августа 2002 г.

3. ***Руководящий документ*** "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации", утверждён решением председателя Государственной технической комиссии при Президенте Российской Федерации 25 июля 1997 г.

4. ***Голембиовская О.М., Рытов М.Ю., Шинаков К.Е.*** Формализация подходов к обеспечению защиты персональных данных: монография. Брянск: БГТУ, 2014.