ния данного метода удовлетворяет неравенству

$$T \le C_1 \cdot \sqrt{p} \cdot \log(1/rp) \cdot \log\log(1/rp) \cdot \\ \cdot \log\log\log(1/rp) + C_2,$$

где C_1, C_2-константы. Полученная оценка показывает, что средняя скорость кодирования и декодирования в $\sqrt{p}$ раз лучше времени ранее известных методов кодирования длин серий. Оценим общий объем памяти кодера и декодера. Так как на втором этапе алгоритма в памяти не нужно хранить кодеры, соответствующие каждой длине блока, то память второго этапа не превосходит C/r, где C - константа. Однако на первом и втором этапах кодирования в памяти необходимо хранить окно длины ω и $\widehat{\omega}$, что приводит к существенному увеличению общего объема памяти.

Построим теперь адаптивный метод кодирования β, для которого общий объем памяти кодера и декодера существенно меньше, чем в методе α. Пусть $\nu_i(x_1 \dots x_\omega)$ - частота встречаемости буквы $a_i \in A$ в слове $x_1 \dots x_\omega$, где $A = \{a_1, \dots a_k\}$. Определим оценки вероятностей $\widehat{p}(a_i)$ как

$$\widehat{p}(a_i) = \frac{\nu_i(x_1 \dots x_\omega) + 1}{\omega + k}.$$

Метод β основан на описанном выше алгоритме α, но на первом и втором этапах этого алгоритма вместо скользящего окна используются только счетчики частот встречаемости букв в окне $x_1 \dots x_\omega$, то есть в памяти хранятся только частоты. На втором этапе кодирования метода β вновь используется адаптивный арифметический код из [5]. Так как для записи частоты встречаемости одной буквы достаточно $\lceil \log \omega \rceil$ бит, то для метода β общий объем памяти кодера и декодера $V \le C_3 \cdot \log(1/r)$, где C_3 - константа.

Скорость кодирования и декодирования для метода β такая же, как и для метода α.

Работа частично поддержана Российским фондом фундаментальных исследований (грант № 11-07-00183а)

СПИСОК ЛИТЕРАТУРЫ

1. Capon, J. A probabilistic model for run-length coding of pictutes // J. Capon. – IRE Trans. Inform. Theory. - 1959, vol. IT-5. - P. 157-163.
2. Rothgordt, U., Intermediate ternary code: A redundancy reducing run-length code for digital facsimile/ U. Rothgordt, G. Renelt// Electron. Lett. – 1997, vol. 13. - P. 747-750.
3. Takagi, M. A highly efficient run-length coding scheme for facsimile transmission // M.Takagi, T.Tsuda – Electron. Commun. Jap. – 1975, vol.58 A, N 2. - P. 30-38.
4. Хантер, Р. Международные стандарты кодирования для цифровой факсимильной связи // Р. Хантер, А. Х. Робинсон – ТИИЭР – 1980, Т. 68, № 4 – С. 112-129.
5. Witten, I. H. Arithmetic coding for data compression // I. H. Witten, R. Neal, J. G. Cleary – Comm. ACM.- 1987, vol.30, N 6. – P. 520-540.

к.ф.-м.н. ***Бакулина М.П.*** *, научный сотрудник, тел. 8-961-215-79-36, marina@rav.sscc.ru - Институт Вычислительной Математики и Математической Геофизики СО РАН*

УДК: 004.052

МЕТОДИКА КЛАССИФИКАЦИИ ИС, ОБРАБАТЫВАЮЩИХ КОНФИДЕНЦИАЛЬНУЮ ИНФОРМАЦИЮ

Миронова В.Г.

Одним из этапов проведения предпроектного обследования информационных систем обработки конфиденциальной информации является их классификация. В статье предложен оригинальный способ определения классификационных признаков и формирования класса информационной системы обработки конфиденциальной информации.

Ключевые слова: конфиденциальная информация, информационная система, критерии классификации, класс.

В настоящее время проблема обеспечения информационной безопасности (ИБ) в информационных системах (ИС) обработки конфиденциальной информации стоит очень остро. Это обусловлено, прежде всего, большим количеством потенциальных угроз ИБ,

как случайного, так и преднамеренного характера, реализация которых может привести к значительным негативным последствиям.

Для нейтрализации возможных угроз безопасности информации (УБИ) и повышения уровня ИБ необходимо построить систему защиты информации (СЗИ). Первым этапом при построении СЗИ является предпроектное обследование ИС.

Основными этапами проведения предпроектного обследования ИС являются:

- классификация ИС;
- построение модели нарушителя ИБ;
- формирование полного перечня УБИ и построение модели УБИ;
- формирование требований к СЗИ.

Первым шагом при проведении предпроектного обследования является классификация ИС. Учитывая как структурные, функциональные особенности, так и месторасположение технических средств обработки конфиденциальной информации (КИ), выделим критерии классификации (таблица 1).

Класс ИС образует декартово произведение

$$\mathbf{X} \subset (\bigcup_{i=1}^{5} \mathbf{T} \times \mathbf{K} \times \mathbf{ST} \times \mathbf{R} \times \mathbf{M} \times \mathbf{V} \times \mathbf{N} \times \mathbf{KR})$$

начальных данных об ИС, векторы которого являются классификационными признаками ИС.

Первым критерием классификации является количество рубежей защиты ИС, обрабатывающей КИ. Типовыми зонами организации, указанными на рисунке 1, являются:

• территория, занимаемая организацией и ограничиваемая забором или условной внешней границей;
• здание на территории;
• коридор или его часть;
• помещение (служебное, кабинет, комната, зал, техническое помещение, склад и др.);
• шкаф, сейф, хранилище.

Соответственно, рубежи защиты:

• забор;
• стены, двери, окна здания;
• двери, окна (если они имеются), стены, пол и потолок (перекрытия) коридора;
• двери, окна, стены, пол и потолок (перекрытия) помещения;
• стены и двери шкафов, сейфов, хранилищ [1].

$\mathbf{T}$ – территориальное расположение компонентов ИС;

$t_i \in \mathbf{T}$, $\mathbf{T}$ ={t_1; t_2; t_3; t_4, t_5}, i= $\overline{1,5}$;

t_1 – в организации существует рубеж 1;
t_2– в организации существует рубеж 2;
t_3 – в организации существует рубеж 3;
t_4 – в организации существует рубеж 4;
t_5 – в организации существует рубеж 5.

Таблица 1. Критерии классификации

№ п/п	Параметры ИС	Классификационные признаки
1.	Территориальное расположение компонентов ИС	1.1 В организации существует рубеж 1.
		1.2 В организации существует рубеж 2.
		1.3 В организации существует рубеж 3.
		1.4 В организации существует рубеж 4.
		1.5 В организации существует рубеж 5.
2.	Перечень сведений конфиденциального характера	2. Перечень сведений конфиденциального характера устанавливается организацией самостоятельно (служебная тайна, персональные данные, коммерческая тайна и др.)
3.	Структура ИС	3.1 Автономная ИС.
		3.2 Локальная ИС.
		3.3 Распределенная ИС.
4.	Пользовательский режим обработки данных	4.1 Однопользовательский.
		4.2 Многопользовательский.
5.	Режим разграничения прав доступа	5.1 ИС без разграничения прав доступа.
		5.2 ИС с разграничением прав доступа.
6.	Наличие подключений ИС к сетям связи общего пользования и (или) сетям международного информационного обмена (ССОП)	6.1 ИС, не имеющие подключения.
		6.2 ИС, имеющие подключения к городской сети (сети в пределах одного города).
		6.3 ИС, имеющая подключения к сети международного информационного обмена.
7.	Использование съемных носителей информации, USB – устройств, CD/DVD	7.1 Съемные носители, USB – устройств, CD/DVD не используются. 7.2 Съемные носители, USB – устройств, CD/DVD используются.
8.	Использование криптографической защиты	8.1 В ИС криптографическая защита информации не используется. 8.2 В ИС криптографическая защита информации используется.

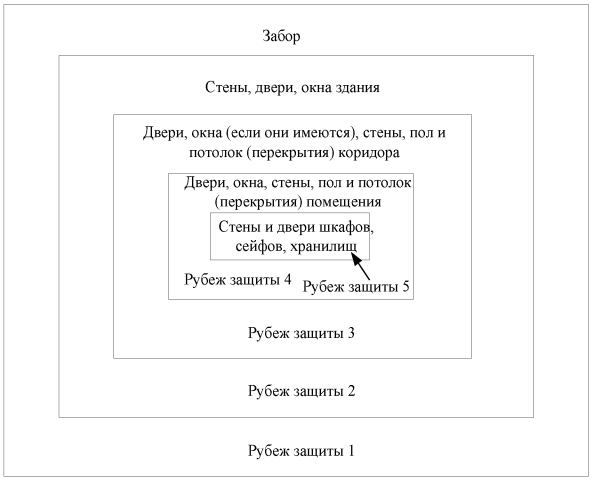

Рисунок 1 – Рубежи защиты организации

В настоящее время в организациях, которые осуществляют обработку КИ, введен режим защиты КИ и определен перечень сведений конфиденциального характера, поэтому вторым критерием классификации является совокупность сведений конфиденциального характера, которые обрабатываются в ИС, k_i, где $k_i \in \mathbf{K}$, i – количество сведений конфиденциального характера, которые установлены в организации.

Стоит также выделить особенности обработки и хранения КИ внутри ИС, а именно, режимы обработки и разграничения прав доступа, структурные особенности ИС.

$\mathbf{ST}$ – структура ИС;

$st_k \in \mathbf{ST}$, $\mathbf{ST} = \{st_a, st_л, st_p\}$, $k = \overline{1,3}$;

st_a – автономная структура ИС;

$st_л$ – локальная структура ИС;

st_p – распределенная структура ИС;

$\mathbf{R}$ – режим обработки данных;

$r_l \in \mathbf{R}$, $\mathbf{R} = \{r_o, r_м\}$, $l = \overline{1,2}$;

r_o – однопользовательский режим обработки данных в ИС;

$r_м$ – многопользовательский режим обработки данных в ИС;

$\mathbf{M}$ – наличие разграничения прав доступа пользователей в ИС;

$m_n \in \mathbf{M}$, $\mathbf{M} = \{m_1, m_2\}$, $n = \overline{1,2}$;

m_1 – ИС с разграничением прав доступа;

m_2 – ИС без разграничения прав доступа;

$\mathbf{V}$ – наличие подключений ИС к сетям связи общего пользования и/или сетям международного информационного обмена;

$v_m \in \mathbf{V}$, $\mathbf{V} = \{v_1, v_2, v_3\}$, $m = \overline{1,3}$;

v_1 – компоненты ИС не подключены к сети связи общего пользования и/или сетям международного информационного обмена;

v_2 - компоненты ИС подключены к городской сети (сеть в пределах одного города);

v_3 - компоненты ИС подключены к сети международного информационного обмена;

$\mathbf{N}$ – использование съемных носителей информации, USB – устройств, CD/DVD;

$n_h \in \mathbf{N}$, $\mathbf{N} = \{n_1, n_2\}$, $h = \overline{1,2}$.

n_1 – в ИС используются съемные носители информации, USB – устройства, CD/DVD;

n_2 – в ИС не используются съемные носители информации, USB – устройства, CD/DVD.

$\mathbf{KR}$ - использование криптографических каналов связи, либо шифрования;

$kr_j \in \mathbf{KR}$, $\mathbf{KR} = \{kr_1, kr_2\}$, $j = \overline{1,2}$.

kr_1 – в ИС криптографическая защита информации не используется;

kr_2 – В ИС криптографическая защита информации используется.

Существуют зависимости пользовательского режима обработки КИ и структуры ИС. Для автономных ИС возможны два пользовательских режима обработки данных – однопользовательский и многопользовательский. Обработка данных пользователями при однопользовательском режиме может осуществляться только при условии - отсутствие режима разграничения прав доступа. ИС, имеющие локальную или распределенную структуру, могут осуществлять только многопользовательский режим обработки данных, как с разграничением прав доступа, так и с его отсутствием. В связи с этим в дальнейшем будем рассматривать $\mathbf{X}^* \subset \mathbf{X}$.

Класс ИС $\mathbf{I} = (i_1, i_2, \ldots, i_r)$, $r \in N$ для конкретно заданных начальных классификационных признаков ИС определяется посредством выполнения алгоритма А проведения классификации, блок-схема алгоритма показана на рисунке 2, отображается на множество классов ИС, расположенных на объектах, где обрабатывается КИ.

В таблице 2 выделены основные классы ИС обработки и хранения КИ, определены их обозначения.

При проведении классификации ИС было выделено семь групп классификационных признаков, рассматривая которые для конкретной функционирующей ИС, получим класс ИС.

Отличительной чертой представленного способа классификации ИС является то, что учитываются как структурные, так и физические особенности ИС, расположение ИС и перечень КИ. В зависимости от ряда особенностей ИС различают семь совокупностей

классификационных признаков. Совокупность знаний об ИС и ее классе ИС позволит определить критерии построения адекватной СЗИ.

Таблица 2. Основные классы ИС

№ п/п	Классификационные признаки	Описание
1.	(t_i, k_i, st_a, r_o, m_2, v_m, n_h, kr_j) $t_i \in \mathbf{T}$, $\mathbf{T}$ ={t_1; t_2; t_3; t_4, t_5}, i=$\overline{1,5}$ k_i, где $k_i \in \mathbf{K}$, i – количество сведений конфиденциального характера, которые установлены в организации $v_m \in V$, V ={v_1, v_2, v_3}, m=$\overline{1,3}$; $n_h \in N$, N ={n_1, n_2}, h =$\overline{1,2}$; $kr_j \in KR$, KR ={kr_1, kr_2}, j=$\overline{1,2}$.	1. Компоненты расположены в организации, где существуют различные рубежи защиты. 2. В ИС обрабатывается КИ, перечень которой установлен в организации. 3. ИС имеет автономную структуру с однопользовательским режимом обработки данных без разграничения прав доступа. 4. С/без наличием(я) подключения к сетям связи общего пользования и/или сетям международного информационного обмена. 5. С/без использованием(я) съемных носителей информации USB – устройств, CD/DVD. 6. С/без использованием(я) криптографической защиты информации.
2.	(t_i, k_i, st_a, $r_м$, m_2, v_m, n_h, kr_j) $t_i \in \mathbf{T}$, $\mathbf{T}$ ={t_1; t_2; t_3; t_4, t_5}, i=$\overline{1,5}$ k_i, где $k_i \in \mathbf{K}$, i – количество сведений конфиденциального характера, которые установлены в организации $v_m \in V$, V ={v_1, v_2, v_3}, m=$\overline{1,3}$; $n_h \in N$, N ={n_1, n_2}, h =$\overline{1,2}$; $kr_j \in KR$, KR ={kr_1, kr_2}, j=$\overline{1,2}$.	1. Компоненты расположены в организации, где существуют различные рубежи защиты. 2. В ИС обрабатывается КИ, перечень которой установлен в организации. 3. ИС имеет автономную структуру с многопользовательским режимом обработки данных без разграничения прав доступа. 4. С/без наличием(я) подключения к сетям связи общего пользования и/или сетям международного информационного обмена. 5. С/без использованием(я) съемных носителей информации USB – устройств, CD/DVD. 6. С/без использованием(я) криптографической защиты информации.

Продолжение таблицы 2

3.	(t_i, k_i, st_a, $r_м$, m_1, v_m, n_h, kr_j) $t_i \in \mathbf{T}$, $\mathbf{T}$ ={t_1; t_2; t_3; t_4, t_5}, i=$\overline{1,5}$ k_i, где $k_i \in \mathbf{K}$, i – количество сведений конфиденциального характера, которые установлены в организации $v_m \in V$, V ={v_1, v_2, v_3}, m=$\overline{1,3}$; $n_h \in N$, N ={n_1, n_2}, h =$\overline{1,2}$; $kr_j \in KR$, KR ={kr_1, kr_2}, j=$\overline{1,2}$.	1. Компоненты расположены в организации, где существуют различные рубежи защиты. 2. В ИС обрабатывается КИ, перечень которой установлен в организации. 3. ИС имеет автономную структуру с многопользовательским режимом обработки данных с разграничением прав доступа. 4. С/без наличием(я) подключения к сетям связи общего пользования и/или сетям международного информационного обмена. 5. С/без использованием(я) съемных носителей информации USB – устройств, CD/DVD. 6. С/без использованием(я) криптографической защиты информации.
4.	(t_i, k_i, $st_л$, $r_м$, m_2, v_m, n_h, kr_j) $t_i \in \mathbf{T}$, $\mathbf{T}$ ={t_1; t_2; t_3; t_4, t_5}, i=$\overline{1,5}$ k_i, где $k_i \in \mathbf{K}$, i – количество сведений конфиденциального характера, которые установлены в организации $v_m \in V$, V ={v_1, v_2, v_3}, m=$\overline{1,3}$; $n_h \in N$, N ={n_1, n_2}, h =$\overline{1,2}$; $kr_j \in KR$, KR ={kr_1, kr_2}, j=$\overline{1,2}$.	1. Компоненты расположены в организации, где существуют различные рубежи защиты. 2. В ИС обрабатывается КИ, перечень которой установлен в организации. 3. ИС имеет локальную структуру с многопользовательским режимом обработки данных без разграничения прав доступа. 4. С/без наличием(я) подключения к сетям связи общего пользования и/или сетям международного информационного обмена. 5. С/без использованием(я) съемных носителей информации USB – устройств, CD/DVD. 6. С/без использованием(я) криптографической защиты информации.
5.	(t_i, k_i, $st_л$, $r_м$, m_1, v_m, n_h, kr_j) $t_i \in \mathbf{T}$, $\mathbf{T}$ ={t_1; t_2; t_3; t_4, t_5}, i=$\overline{1,5}$ k_i, где $k_i \in \mathbf{K}$, i – количество сведений конфиденциального характера, которые установлены в организации $v_m \in V$, V ={v_1, v_2, v_3}, m=$\overline{1,3}$;	1. Компоненты расположены в организации, где существуют различные рубежи защиты. 2. В ИС обрабатывается КИ, перечень которой установлен в организации. 3. ИС имеет локальную структуру с многопользовательским режимом обработки данных с разграничением прав доступа. 4. С/без наличием(я) подключения к сетям связи общего пользования и/или

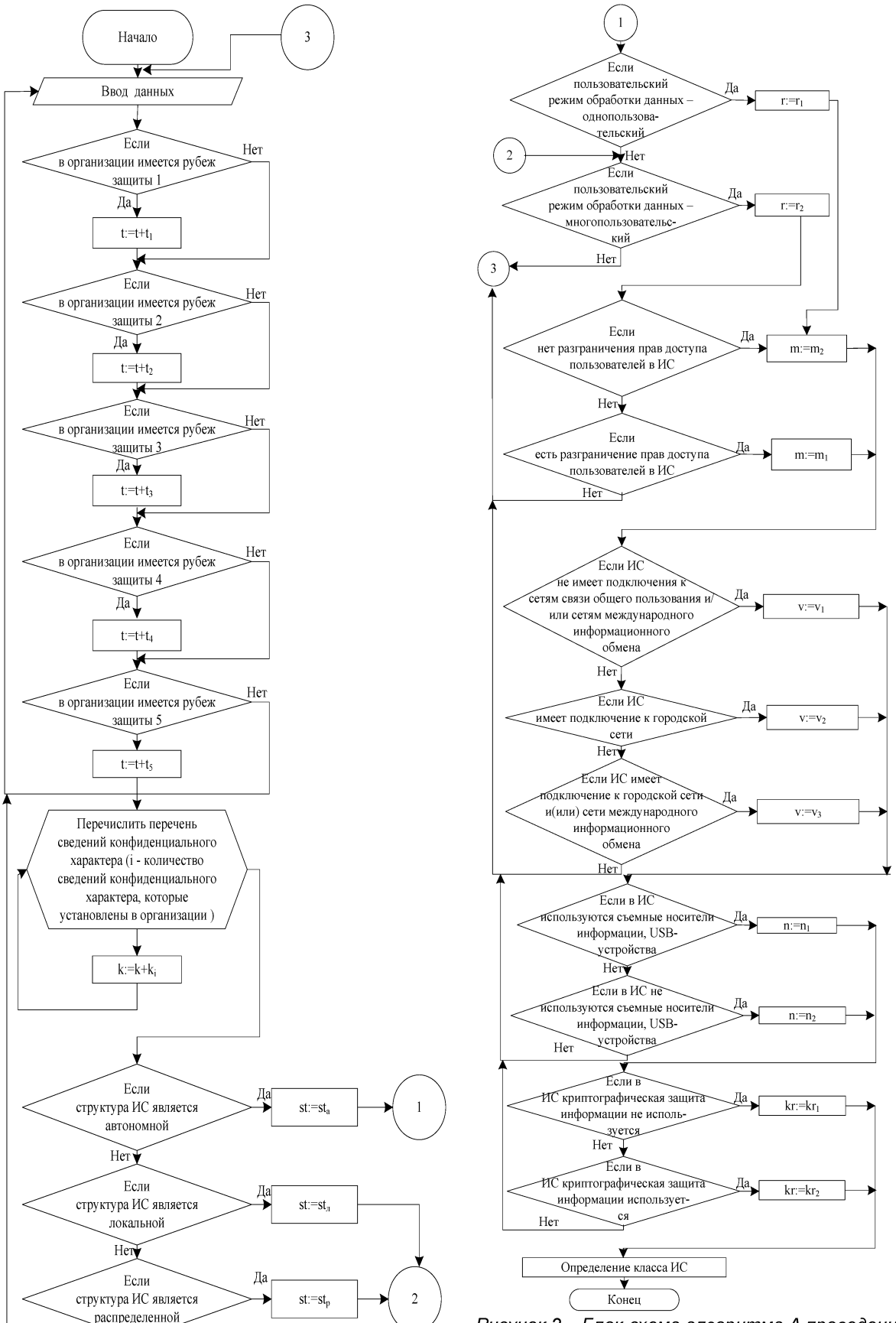

Рисунок 2 – Блок-схема алгоритма А проведения классификации ИС

Продолжение таблицы 2

	$n_h \in N$, $N=\{n_1, n_2\}$, $h=\overline{1,2}$;	сетям международного информационного обмена. 5. С/без использованием(я) съемных носителей информации USB – устройств, CD/DVD. 6. С/без использованием(я) криптографической защиты информации.
6.	(t_i, k_i, st_p, $r_м$, m_2, v_m, n_h, kr_j) $t_i \in \mathbf{T}$, $\mathbf{T}=\{t_1; t_2; t_3; t_4, t_5\}$, $i=\overline{1,5}$ k_i, где $k_i \in \mathbf{K}$, i – количество сведений конфиденциального характера, которые установлены в организации $v_m \in V$, $V=\{v_1, v_2, v_3\}$, $m=\overline{1,3}$; $n_h \in N$, $N=\{n_1, n_2\}$, $h=\overline{1,2}$; $kr_j \in KR$, $KR=\{kr_1, kr_2\}$, $j=\overline{1,2}$.	1. Компоненты расположены в организации, где существуют различные рубежи защиты. 2. В ИС обрабатывается КИ, перечень которой установлен в организации. 3. ИС имеет распределенную структуру с многопользовательским режимом обработки данных без разграничения прав доступа. 4. С/без наличием(я) подключения к сетям связи общего пользования и/или сетям международного информационного обмена. 5. С/без использованием(я) съемных носителей информации USB – устройств, CD/DVD. 6. С/без использованием(я) криптографической защиты информации.
7.	(t_i, k_i, st_p, $r_м$, m_1, v_m, n_h, kr_j) $t_i \in \mathbf{T}$, $\mathbf{T}=\{t_1; t_2; t_3; t_4, t_5\}$, $i=\overline{1,5}$ k_i, где $k_i \in \mathbf{K}$, i –	1. Компоненты расположены в организации, где существуют различные рубежи защиты. 2. В ИС обрабатывается КИ, перечень которой установлен в организации.

Продолжение таблицы 2

	количество сведений конфиденциального характера, которые установлены в организации $v_m \in V$, $V=\{v_1, v_2, v_3\}$, $m=\overline{1,3}$; $n_h \in N$, $N=\{n_1, n_2\}$, $h=\overline{1,2}$; $kr_j \in KR$, $KR=\{kr_1, kr_2\}$, $j=\overline{1,2}$. $kr_j \in KR$, $KR=\{kr_1, kr_2\}$, $j=\overline{1,2}$.	3. ИС имеет распределенную структуру с многопользовательским режимом обработки данных с разграничением прав доступа. 4. С/без наличием(я) подключения к сетям связи общего пользования и/или сетям международного информационного обмена. 5. С/без использованием(я) съемных носителей информации USB – устройств, CD/DVD.формации USB – устройств, CD/DVD. 6. С/без использованием(я) криптографической защиты информации.

СПИСОК ЛИТЕРАТУРЫ

1. Миронова, В.Г. Предпроектное проектирование информационных систем персональных данных как этап аудита информационной безопасности / В.Г. Миронова, А.А. Шелупанов. // Докл. Том. гос. ун-та систем управления и радиоэлектроники.- 2010.-№2(22), Ч1.-С.257-259.
2. Шелупанов, А.А.. Автоматизированная система предпроектного обследования информационной системы персональных данных «АИСТ-П»/ А.А. Шелупанов, В.Г. Миронова и др. // Докл. Том. гос. ун-та систем управления и радиоэлектроники.-2010.-№1(21), Ч1.-С.14-22.
3. «Методические рекомендации ФСБ»
4. Миронова, В.Г. Анализ этапов предпроектного обследования информационной системы персональных данных / В.Г. Миронова, А.А. Шелупанов // Периодический научный журнал «Вестник СибГАУ им.М.Ф.Решетнева».-2011 - №2(35), С. 45-48.

***Миронова В.Г.**, аспирант каф. КИБЭВС ТУСУР*