

**ОРГАНИЗАЦИЯ ПРОТИВОДЕЙСТВИЯ
ТЕХНИЧЕСКОЙ РАЗВЕДКЕ. ЗАЩИТА
ОТ УТЕЧКИ ИНФОРМАЦИИ,
НЕСАНКЦИОНИРОВАННОГО
ДОСТУПА**

Борисов В.А.

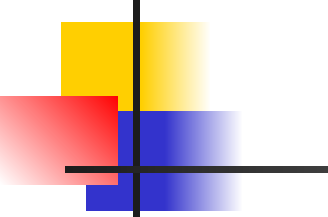
КАСК – филиал ФГБОУ ВПО РАНХ и ГС
Красноармейск 2011 г.



Средства противодействия



- здания и строительные препятствия;
- аппаратура тревожной сигнализации;
- системы связи;
- системы управления;
- персонал охраны;
- процедуры обеспечения безопасности.



Модели защиты технических средств и объектов от утечки информации и НСД

элементарная

многозвенная

многоуровневая

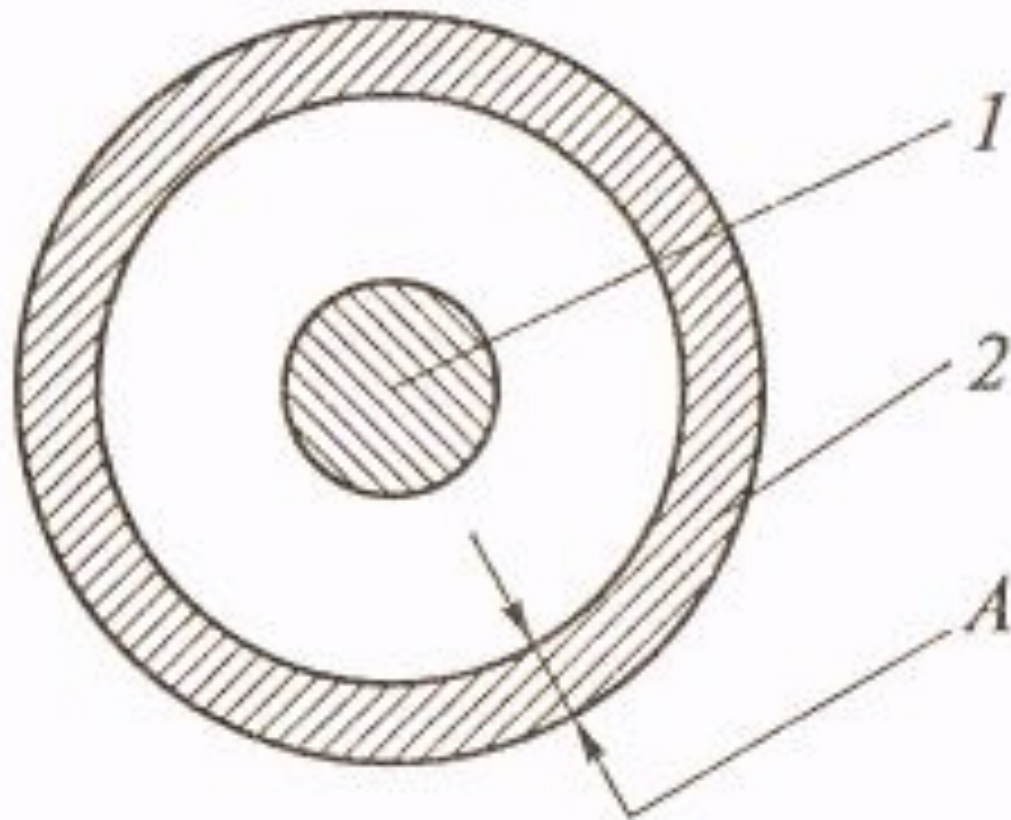


Рис. 5.1. Модель элементарной защиты:

1 — предмет защиты; *2* — преграда;
A — прочность преграды

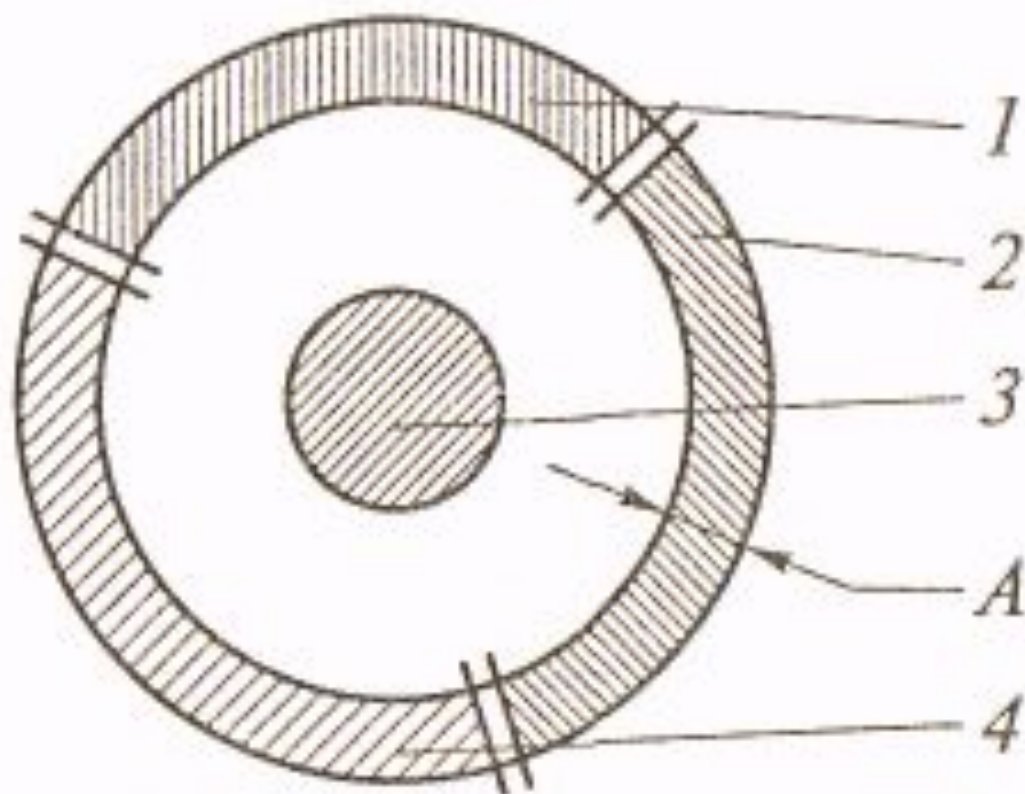


Рис. 5.2. Модель многозвенной защиты:

1, 2, 4 — преграды; *3* — предмет защиты; *A* — прочность преграды

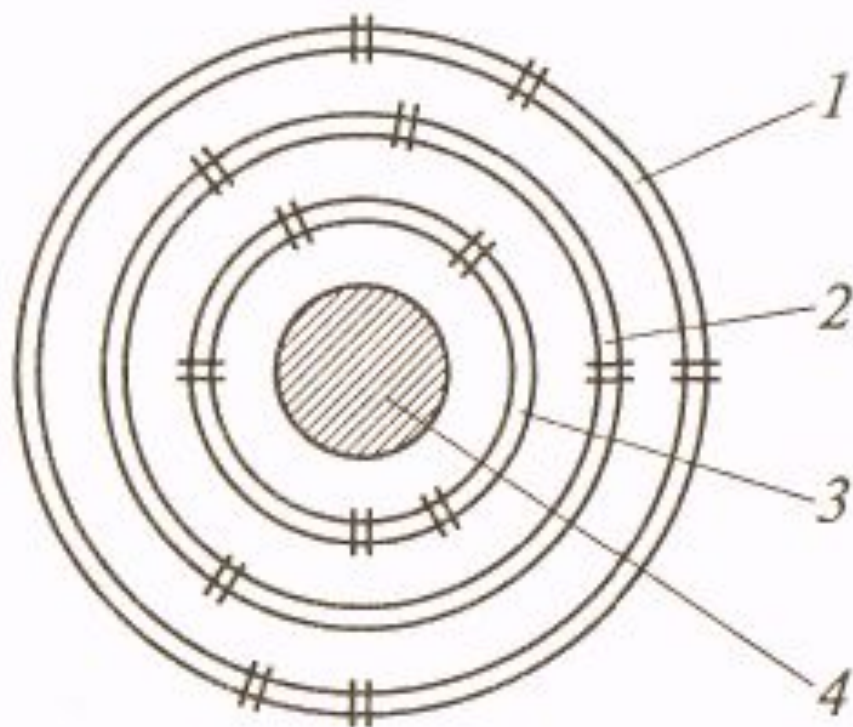


Рис. 5.3. Модель многоуровневой защиты:

1 — 1-й контур защиты; 2 — 2-й контур защиты; 3 — 3-й контур защиты;
4 — предмет защиты



Предмет защиты

- Информация, циркулирующая и хранимая в АСОД в виде данных, команд и сообщений, имеющих какую-либо цену для их владельца и потенциального нарушителя.

Несанкционированное действие (НСД)



- Событие, выражающееся в попытке нарушителя совершить несанкционированные действия по отношению к любой ее части.

Штатные средства ввода, вывода и хранения информации

терминалы пользователей

средства отображения и документирования информации

средства загрузки программного обеспечения в систему

носители информации

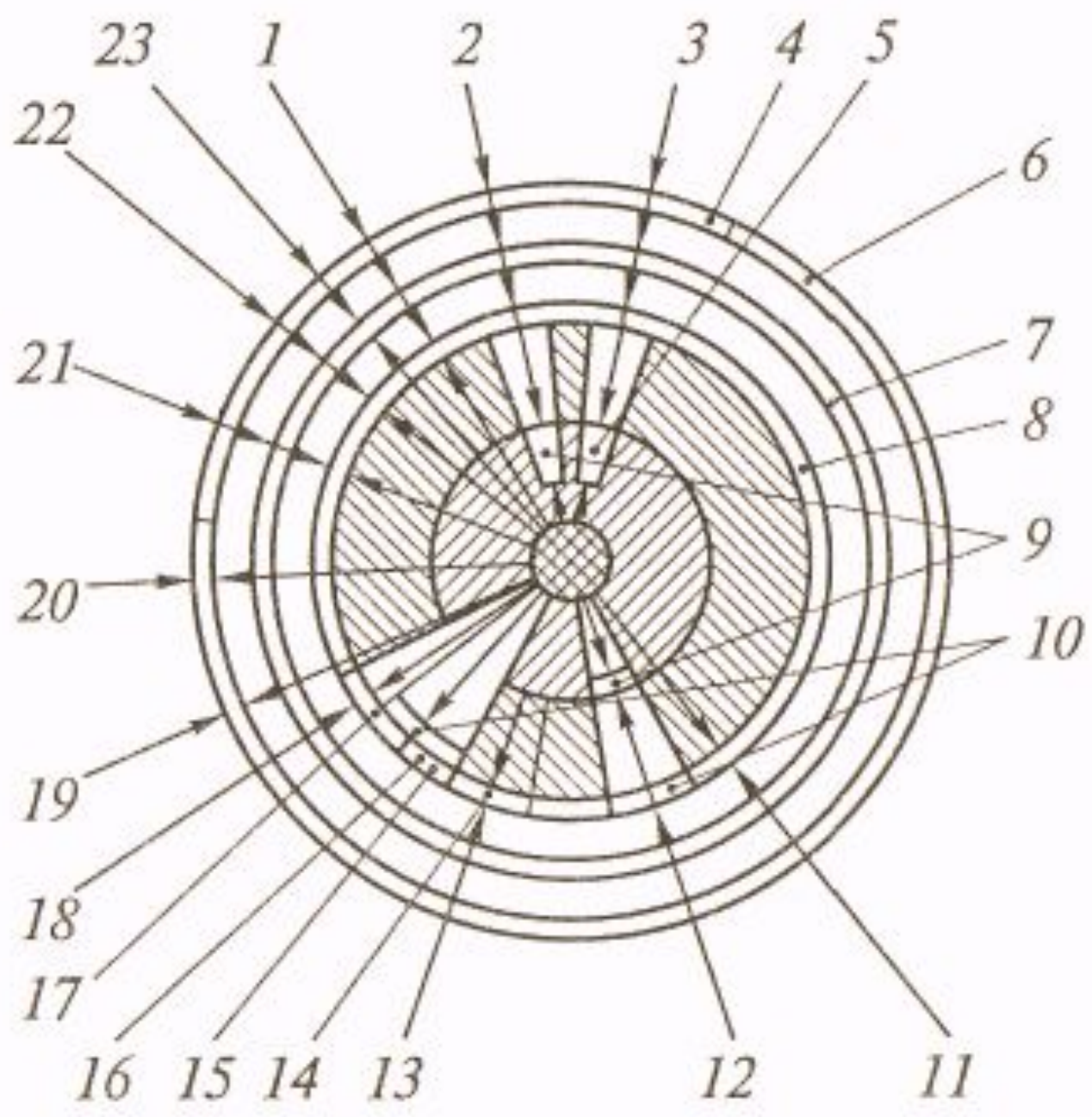
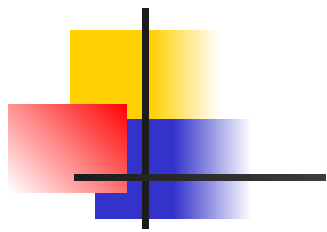
внешние каналы связи

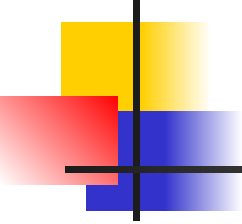


Потенциальные угрозы информации

случайные

преднамеренные





Качественные показатели средств функционального контроля

- время обнаружения и локализации отказа;
- достоверность контроля функционирования;
- полнота контроля;
- время задержки в обнаружении отказа.

Возможные каналы несанкционированного доступа к информации

- все штатные средства при их незаконном использовании;
- технологические пульты и органы управления;
- внутренний монтаж аппаратуры;
- линии связи между аппаратными средствами ВС;
- побочное электромагнитное излучение информационного объекта;
- побочные наводки информации на сетях электропитания и заземления аппаратуры;
- внешние каналы связи.