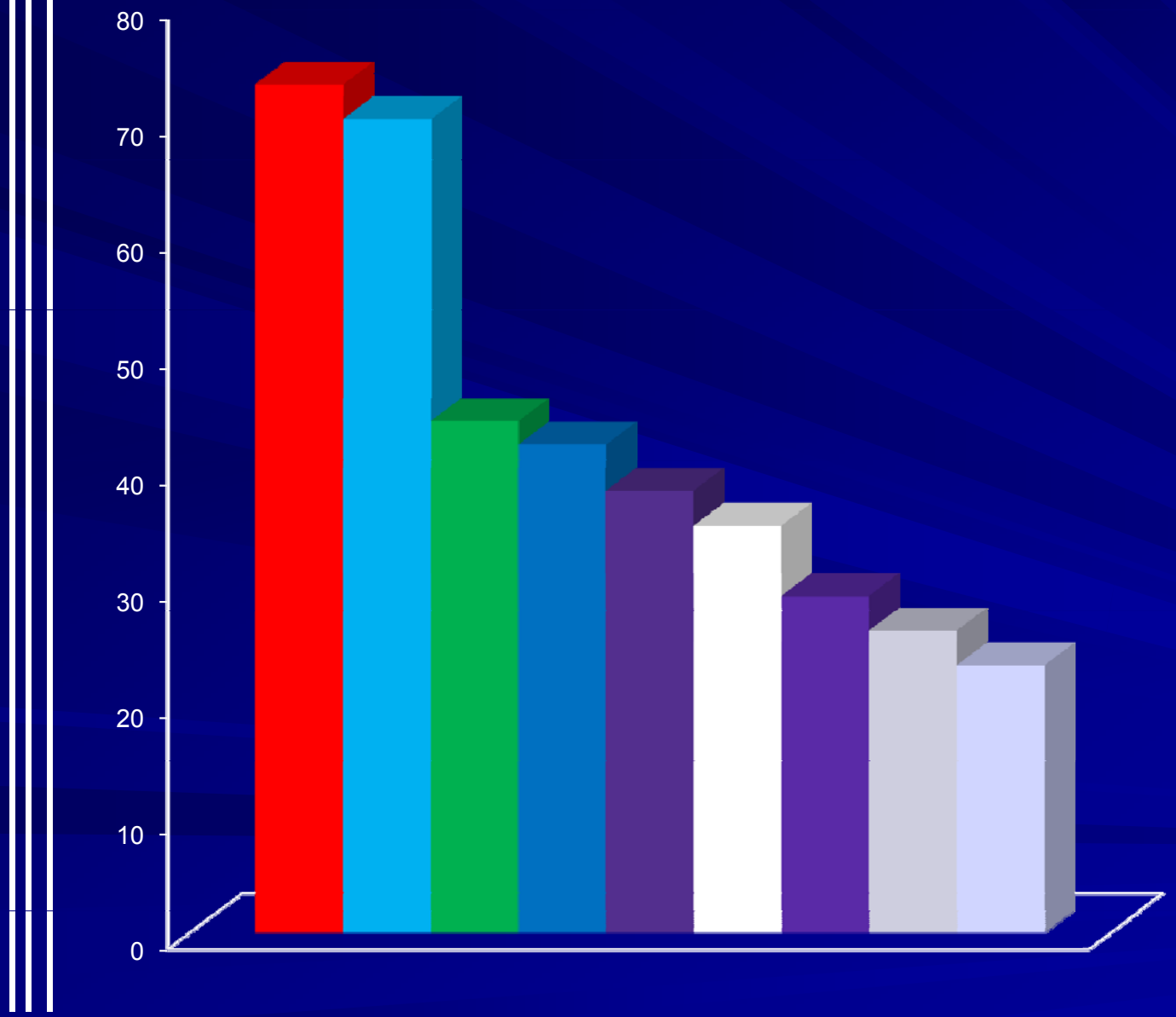
Скрытые методы защиты информации и их применение для противодействия инсайдерам

Гончаров П.И.

Актуальность



Скрытые методы защиты информации

- Скрытая идентификация пользователя по следующим биометрическим признакам:
  - Статические признаки - признаки полученные человеком с рождения:
    - структура лица;
    - термограмма лица;
  - Динамические признаки - признаки, которые приобретаются со временем:
    - клавиатурный почерк;
    - распознавание голоса;
- Идентификация пользователя по принципу его работы на рабочем месте (с каким ПО работает, каким образом, в каком порядке и так далее);
- Идентификация пользователя по его поведению в сети предприятия и интернете.

Реакция на подозрительные действия

- Сообщение на АРМ администратора безопасности с отказом во входе в систему;
- Сообщение на АРМ администратора безопасности о работе на АРМ постороннего лица без блокировки работы АРМ;
- Блокировка работы АРМ с сообщением на АРМ администратора безопасности;
- Включение подозрительного АРМ в сеть-приманку (honeynet), не полностью копирующую сеть предприятия, для анализа поведения подозрительного пользователя с сообщением на АРМ администратора безопасности;

Выводы, планы на будущее