

# Безпека операційних систем і комп'ютерних мереж

## Лекція 8

### Анотація

Продовжуючи розгляд Windows, в даній лекції наводиться детальний опис моделі захисту цієї системи. Для цього розглядається структура та принцип призначення ідентифікаторів захисту SID. Детально описується структура маркера доступу, що використовується для ідентифікації контексту захисту SRM. Також наведено атрибути дескриптора захисту. Розібрані два алгоритми з'ясування прав доступу до об'єкта (максимальних прав доступу та доступу з заданими правами), а також виділено їх особливості. Наведена схема архітектури підсистеми автентифікації Windows та проаналізовано її особливості. Детально розглядається система аудиту та наводиться схема взаємодії її елементів. Як підсумок даної лекції виділено причини вразливості Windows NT та надана загальна оцінка системи Windows.