Безпека операційних систем і комп'ютерних мереж

Лекція 22

Анотація

В лекції розглядаються системи виявлення атак (СВА): їх можливості, класифікація за різними характеристиками, недоліки. Описані основні підходи, які застосовуються для виявлення атак: виявлення зловживань та виявлення аномалій. Серед головних можливостей СВА виділяють: можливість блокування джерела атаки, можливість здійснювання реакції на атаку, можливість визначення преамбул атаки, виконання документування існуючих загроз та контроль за якістю розробки й адміністрування безпеки в інформаційно-телекомунікаційних системах (ІТС). Класифікацію СВА проводять за таким характеристиками: етап здійснення атаки, інформаційні джерела атаки, метод аналізу для виявлення атак, швидкість реакції СВА, характер відповіді, архітектура СВА та способи керування СВА. Всі наведені в класифікаціях різновиди СВА розглянуті в лекції більш детально, для кожної виділені її переваги та недоліки. Далі більше уваги приділено методам виявлення атак, виокремленні їх слабкі та сильні сторони. Розглянуті метрики та технології, що використовуються при виявленні аномалій.