침입탐지시스템의 오용탐지 기법이란 시스템 로그, 네트워크 입력정보, 알려진 침입방법, 비정상적인 행위 패턴 등의 특징을 비교하여 탐지하는 방법이다.

기존의 침입방법을 데이터베이스에 저장해 두었다가 사용자 행동 패턴이 기존의 침입 패턴과 일치하거나 유사한 경우 침입이라 판단한다.

새로운 공격이나 침입 방법이 출현하였을 경우에 그에 맞는 공격 패턴을 생성하여 추가한다.

오용탐지 기법 종류는 7가지로 전문가 시스템, 신경망, 시그니처분석, 패트리넷, 상재전이 분석, 유전 알고리즘, 지식기반이 있다.

그중 신경망은 침입탐지방법론 중 오용탐지 방식에서 타당한 방법으로 새로운 입력 출력쌍을 얻기 위해 두 집합의 정보간 관련성을 학습하고 일반화하는데 사용되는 알고리즘 기법이다.