5 Классификация компьютерных атак и систем их обнаружения

Типы сетевых атак

- удаленное проникновение (от англ. remote penetration) — это тип атак, которые позволяют реализовать удаленное управление компьютером через сеть; например, атаки с использованием программ NetBus или BackOrifice;

- локальное проникновение (от англ. local penetration) — это тип атак, которые приводят к получению несанкционированного доступа к узлу, на который они направлены;

- удаленный отказ в обслуживании (от англ. remote denial of service) — тип атак, которые позволяют нарушить функционирование системы в рамках глобальной сети;
- локальный отказ в обслуживании (от англ. local denial of service) — тип атак, позволяющих нарушить функционирование системы в рамках локальной сети.

- атаки с использованием сетевых сканеров
- атаки с использованием взломщиков паролей
- атаки с использованием анализаторов протоколов

Классификация приведена в книге Милославской и Толстого

- по поведению после обнаружения (на активные и пассивные),
- по расположению источника результатов аудита (регистрационные файлы хоста либо сетевые пакеты),
- по методу обнаружения (поведенческие либо интеллектуальные).

Технологии построения систем обнаружения атак

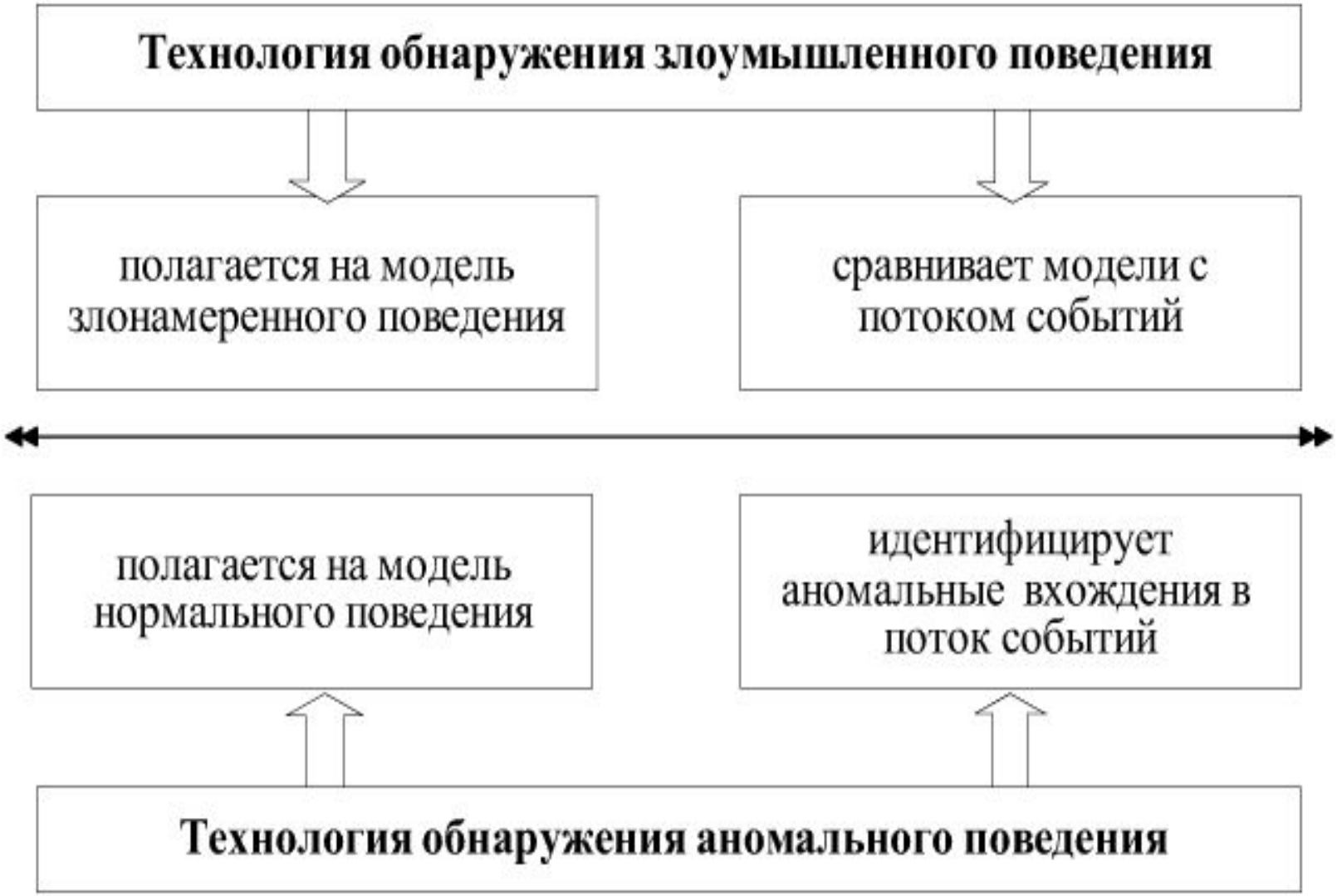
Требования к системам обнаружения атак (СОА)

- современные технологии разработки,
- ориентировка на особенности современных информационных сетей,
- совместимость с другими программами.

Принципы обнаружения компьютерных атак.

- СОА известны некоторые признаки, характеризующие правильное или допустимое поведение объекта наблюдения
- признаки, характеризующие поведение злоумышленника.

Существующие технологии СОА



Меры и методы, обычно используемые в обнаружении аномалии

- пороговые значения: наблюдения за объектом выражаются в виде числовых интервалов.
  - В качестве наблюдаемых параметров могут быть, например, такие: количество файлов, к которым обращается пользователь в данный период времени,
  - число неудачных попыток входа в систему, загрузка центрального процессора и т.п.

Пороги могут быть статическими и динамическими (т.е. изменяться, подстраиваясь под конкретную систему);

- **статистические меры**: решение о наличии атаки делается по большому количеству собранных данных путем их статистической предобработки;
- **параметрические**: для выявления атак строится специальный "профиль нормальной системы" на основе шаблонов (т.е. некоторой политики, которой обычно должен придерживаться данный объект);

- **непараметрические:** здесь уже профиль строится на основе наблюдения за объектом в период обучения;
- **меры на основе правил (сигнатур):** они очень похожи на непараметрические статистические меры. В период обучения составляется представление о нормальном поведении объекта, которое записывается в виде специальных "правил". Получаются сигнатуры "хорошего" поведения объекта;