Отслеживание и подавление угроз в компьютерных сетях

Если сделать упор на реакцию при возникновении угроз, то можно выделить два типа прокси:

1. IDSes (Intrusion Detection Systems) -- своеобразные сенсоры, которые отслеживают вредоносный трафик по сигнатурам и различными способами оповещают при его обнаружении. Обычно трафик через них не «пропускается», а копируется в их сторону для параллельного анализа (promiscuous).

2. IPSes (Intrusion Prevention Systems) -- не просто отслеживают вредоносный трафик, а и способны самостоятельно его заблокировать. Обычно трафик «пропускается» через них (inline).

Существует много видов и способов атак, но также есть и достаточное количество способов защиты от них. При работе в Интернете рекомендуется выполнять следующие требования:

- Пользуйтесь паролями
- Работайте на компьютере под учетной записью с ограниченными правами
- Используйте шифрование данных
- Регулярно выполняйте обновления программного обеспечения
- Используйте и регулярно обновляйте антивирусные программы
- Используйте межсетевой экран