Положим $X = \{x_1, x_2, ..., x_n\}$ - множество узлов в компьютерной сети.

Пусть каждый узел $x_i \in X$ в момент времени $t \in T$ характеризуется *состоянием* $S(x_i, t)$.

Состоянием сети $S(X, t)$ будем называть множество состояний её узлов в момент времени t

$$S(X, t) = \{S(x_i, t) | x_i \in X\} \quad (1)$$

Будем считать, что узлы взаимодействуют между собой посредством передачи сообщений, используя сетевой протокол. Тогда положим $m(x_i, x_j)$ - управляющая информация от объекта x_i к x_j. Назовём *переходом* изменение состояния узла в результате взаимодействия с участием этого узла.

Введём множества состояний A и N (от. Attack и Normal соответственно).

A - множество состояний узлов, каждое из которых представляет состояние узла после произведения над ним какой-либо компьютерной атаки, или другими словами множество опасных состояний узлов

N - множество нормальных состояний узлов

Состояние сети будем называть *опасным*, если состояние хотя бы одного узла в этой сети принадлежит множеству A.

Таким образом для обнаружения атак в такой сети достаточно наблюдать за состояниями узлов этой сети, а точнее за изменением состояний этих узлов.

В рамках данной работы будем предполагать, что состояния узлов изменяются только в результате взаимодействия узлов между собой (ввиду того, что предметом исследования являются атаки на компьютерные сети).

Зафиксируем узел сети $x \in X$. Пусть в момент времени t произошло взаимодействие узлов x и y в сети, в результате которого на узел x поступила управляющая информация I. В ответ на это узел x выполняет действия, которые в дальнейшем будем называть *реакцией* узла и обозначать $R = f(I)$, где f - функция реагирования с областью определения $D(f)$ - {множество всех возможных входов}. По сути эта функция реализована в виде механизма работы конкретного узла x сети и вообще говоря может отличаться для разных узлов. Она и реализует смену состояний узла $x \in X$.

Задачу обнаружения атак в компьютерной сети можно теперь записать в следующем виде:

$$F(X) \to min$$

где $F(X) = |A_s|$, $A_s = \{x | x \in X, S(x) \in A\}$. Т.е. задачи обнаружения атак - задача минимизации числа атакованных узлов в сети