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 всевозможных 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). А поэтому можно ввести множества M_A и M_N – соответственно множества описаний объектов $m(x_i, x_j)$ потоков информации, приводящих узлы в в опасные и нормальные состояния.

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 $x \in X$.

Формальная постановка задачи обнаружения атак в компьютерной сети:

Пусть задано множество $M_{tr} = \{m(x_i, x_j)\}$ описаний взаимодействий узлов x_i и x_j сети, где $m(x_i, x_j)$ можно описать в виде набора признаков $(x_1, x_2, ..., x_n)$.

Про множество M_{tr} известно, что подмножество аномальных взаимодействий $M_{tr_A} \in M_{tr}$ по мощности мало сравнимо с мощностью множества нормальных взаимодействий $M_{tr \in M_{tr}}$ (составляет не более 1-1.5 % от общей мощности множества M_tr).

Множество M_{tr} будем называть обучающим множеством.

Собственно сама постановка задачи: $\forall m(x_i, x_j)$ определить $m(x_i, x_j) \in M_A$ или $m(x_i, x_j) \in M_N$, т.е. для любого взаимодействия $m(x_i, x_j)$ в сети определить, является оно аномальным (несущим угрозу) или нормальным.