

**Н.Г. Булахов**

**МОДЕЛИРОВАНИЕ СИТУАЦИИ ПИКОВОЙ НАГРУЗКИ В  
ИНФОРМАЦИОННОЙ СЕТИ**

Томский государственный университет, г. Томск, Россия

**N.G. Bulakhov**

**MODELING NETWORK PEAK LOAD SITUATION**

Tomsk State University, Tomsk, Russia

Сегодня вирусные атаки являются одной из первостепенных угроз информационной безопасности. Такие действия наносят финансовый ущерб, а также позволяют реализовать многих других опасных угроз. И это – несмотря на то, что для борьбы с такими вредителями уже разработано много сигнатурных, статистических и эвристических методов. В их основе лежат модели функционирования сети, по которой передаётся зловредный трафик в различных ситуациях (например, эпидемиологическая модель и её модификации). Применение этих методов ограничивает приближённость описания функционирования сетей либо малое число релевантных параметров.

Поэтому актуальна разработка модели, устраняющей вышеперечисленные недостатки. Для достижения этой цели предложена виртуальная сеть в виде обобщённого устройства пересылки пакетных данных, структура которого позволяет учесть пиковые нагрузки в сети (рис. 1). Входы и выходы не равноправны между собой: каждому присваивается свой весовой коэффициент  $W=WO+WV$ , который характеризует вероятность появления пакета на данном входе. Вес  $WO$  соответствует загрузке канала полезными пакетами, вес  $WV$  – саморазмножающимися. Входящие пакеты имеют адрес назначения, указывающий выходной порт. Каждый выходной порт рассчитан на очередь длиной  $M$  пакетов. Если число пакетов в очереди достигает  $M$ , то  $M+1$ -й пакет отбрасывается. В заданный такт времени условие того, что на входе  $n$  есть пакет, определяется формулой (1).

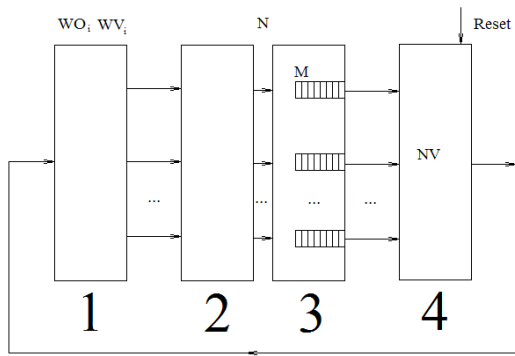


Рис. 1. Структура устройства пересылки пакетов с  $N$  входами и  $N$  выходами: 1 и 2 – блоки распределения пакетов на входе и по выходам, соответственно, 3 – блок очередей, 4 – блок обработки информации о выходных пакетах.

Если на входе  $n$  имеется пакет, то условие того, что он саморазмножающийся либо полезный, есть формула (2)

$$f(n) = \begin{cases} 1, & rnd \leq \frac{WO_i + WV_i}{WO_{\max} + WV_{\max}}, \\ 0, & rnd > \frac{WO_i + WV_i}{WO_{\max} + WV_{\max}}. \end{cases} \quad (1)$$

$$f_1(n) = \begin{cases} 1, & rnd \leq \frac{WV_i}{WO_i + WV_i}, \\ 2, & rnd > \frac{WV_i}{WO_i + WV_i}. \end{cases} \quad (2)$$

В зависимости от порта назначения  $k$  каждый пакет помещается в выходную очередь согласно условию 3. Согласно модели подсчитывается число пакетов каждого типа ( $NO_t$  и  $NV_t$ ) на выходе. Коррекция весового коэффициента  $WV_{i,t}$ , соответствующего входу  $i$ , задаётся соотношением

$$\sum_{i=1}^k (WO_i + WV_i) \leq random(\sum_{i=1}^N (WO_i + WV_i)) < \sum_{i=1}^{k+1} (WO_i + WV_i) \quad (3) \quad WV_{i,t} = WV_{i,t-1} \cdot \frac{NV_t + 1}{NV_{t-1} + 1} \quad (4)$$

Предложенная виртуальная сеть (обобщённое устройство пересылки пакетных данных) и статистическая модель его функционирования позволяет корректно описать работу реальной сети в различных ситуациях, включая случай пиковой нагрузки. Проведённая верификация модели показала её преимущества относительно биологических моделей. Ещё одним достоинством предложенной модели оказывается возможность учёта различных сетевых топологий, т.е. конкретных типовых сетей либо их фрагментов, например, с целью выяснения влияния топологии на распространение саморазмножающихся пакетов. При этом принципы построения исходной модели и соотношения (1)–(4) сохраняются.