# МОДЕЛЬ ЦИС ДЛЯ ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ ЧЕРВЕЙ

Н. Г. Булахов
Томский государственный университет

Обнаружение факта вторжения зловредного программного кода на сетевые компьютеры и предотвращение его дальнейшего распространения представляет практический интерес. В этом контексте автором построена модель цифровой информационной сети (ЦИС) [1], которая позволяет оценить влияние распространения саморазмножающихся пакетов на качество передачи информации по сети, а именно загруженность канала, соотношение объёма полезного трафика к вредоносному, величину потерь, вызванных перегрузкой оборудования, и степень заполнения буферов коммутаторов, маршрутизаторов

Характеристиками передаваемого по ЦИС трафика, пригодными для выявления потенциально опасной активности, являются: интенсивность пересылки отдельных пактов, пересылки небольших очередей пакетов и попыток установить соединение отдельными хостами; распределение IP- и MAC-адресов источника и назначения в передаваемых пакетах; их размеры и типы (принадлежность к определённым протоколам). Однако для достаточно надёжного детектирования вредоносной активности и сведения риска ложного срабатывания к минимуму в данном случае часто требуется некоторая «калибровка», составление сигнатур распространения известных червей. Это сужает область применения данных алгоритмов обнаружения сетевых атак и делает уязвимыми сети для новых (не внесённых в базу) червей.

Автор предлагает исключить параметры, варьирующиеся для конкретных реализаций червя, и добавить характеристики пересылки информационных пакетов внутри маршрутизаторов и коммутаторов: количество отбрасываемых пакетов в единицу времени, заполненность буферов пересылки, нагрузка оборудования. Тогда можно увеличить количество параметров, идентифицирующих сетевую атаку, и в случае опознания пакетов с отсутствующей возможностью дальнейшей пересылки игнорировать их, освобождая мощности оборудования для пересылки нормального трафика.

---

1. Н. Г. Булахов и др. Статистическая модель ЦИС, учитывающая возможность пиковых нагрузок // Материалы международной научной конф. "Статистические методы в естественных, гуманитарных и технических науках" (апрель 2006 г., г. Таганрог). Ч. 3. Таганрог: «Антон», ТРТУ, 2006. С. 7–11.

Научный руководитель – д-р техн. наук, проф. В. Т. Калайда