П. А. Коновалов А. В. Квитченко

МОДЕЛЬ ДЛЯ СЕТЕВОЙ АНТИВИРУСНОЙ ЗАЩИТЫ НА ОСНОВЕ РЕГЕНЕРАТИВНОГО ПРОЦЕССА

Строится математическую модель антивирусной защиты локальных сетей. Модель относится к классу регенеративных процессов.

Введение

Для защиты сети от внешних атак вирусов и распространения вирусов внутри сети применяются два метода:
1.Обновление сигнатур антивирусов
2.Переустановка операционных систем (ОС).

Операционные системы переустанавливаются в случае сбоя любого из компьютеров (нерегулярная аварийная переустановка) или в запланированные моменты времени. Рассматривается задача максимизации среднего единичного дохода. Функция распределения(далее — ФР) в запланированные интервалы времени между полной переустановкой ОС рассматривается как элемент управления. Доказывается, что оптимальная ФР является вырожденной, т. е. должна быть локализована в точке t.

I. Функционирование локальной сети с антивирусной защитой

Рассматривается локальная сеть (LAN), состоящая из N компьютеров (узлов). Если узел заражен, то он окажется "здоровым"после обновления с вероятностью p_0. После переустановки ОС все узлы оказываются "здоровыми". Ожидаемое время переустановки равно T. Решение об очередной переустановке ОС берется в момент регенерации системы по ФР $G(t)$. Прибыль определяется следующими параметрами: c_0 — прибыль одного узла за единицу времени; c_1 — скрытый ущерб от вирусов за единицу времени; c_2 — стоимость переустановки ОС за единицу времени; c_3 — стоимость нового антивирусного программного обеспечения, установленного при переустановке ОС. Рассматривается задача нахождения ФР G(t) такой, что средняя прибыль сети за единицу времени максимальна для сетей, работающих достаточно долго.

II. Математическая модель

Период регенерации состоит из 2-х интервалов: Времени до следующей плановой или аварийной ситуации переустановки ОС. Время переустановки. Пусть Z — Продолжительность периода регенерации; t_1 - время между обновлением и запланированной переустановки ОС; $G(t) = P(t_1 < t)$, Y - время между обновлением и аварийной переустановкой ОС. Тогда

$$\mathbf{E}Z = \mathbf{E}\min(t_1, Y) + T = \int_0^\infty \min(t, Y)\mathrm{d}G(t) + T$$

Пусть $Q_{i,j,k}(t)$ - среднее время до переустановки ОС при условии, что $X(t)$ начинается с состояния (i, j, k) и в момент t ОС переустанавливают запланировано. Пусть $R_{i,j,k}(t)$ — средняя прибыль сети от начального момент до начала переустановки ОС при условии, что X начинается с (i, j, k), а время до следующей запланированной установки ОС равно t.

III. Оптимальное распределение интервалов между переустановками ОС

Пусть $S(T)$ – средняя прибыль от сети, функционирующей на интервале $(0; t)$ и $\rho = \log_{t\to\infty} \frac{S(t)}{t}$. Из теории регенерации $\rho = \mathbf{E}R(Z)/\mathbf{E}Z$. Следовательно,

$$\rho = \frac{\int_0^\infty R_{0,0,0}\mathrm{d}G(t) - c_2T - c_3}{\int_0^\infty Q_{0,0,0}\mathrm{d}G(t) + T}$$

Функционал ρ является линейным дробным с относительностью распределения $G(t)$.
Теорема. Оптимальное решение $(\rho \to \max)$(т. е. распределение t_1) вырождается: $= \begin{cases} 0, t \le r; \\ 1, t > r \end{cases}$

IV. Выводы

Построена математическая модель вирусной защиты LAN. Рассмотрели два способа защиты сети: обновление сигнатур антивируса и переустановка ОС. Доказали, что оптимальная ФР запланированных интервалов между полными переустановками ОС должна быть вырожденной.

1. A Model for Network Virus Protection Based on Regenerative Process Yu.Grishunina L.Manita

Коновалов Павел Андреевич, студент 2 курса факультета информационных технологий и управления Белорусского государственного университета информатики и радиоэлектроники,, RORORundead@gmail.com.

Квитченко Артем Вячеславович, студент 2 курса факультета информационных технологий и управления Белорусского государственного университета информатики и радиоэлектроники, miarvod@yandex.ru.