

К ЗАДАЧЕ УПРАВЛЕНИЯ ПО БЫСТРОДЕЙСТВИЮ ОДНОЙ МОДЕЛЬЮ ВИРУСНОГО ЗАРАЖЕНИЯ В СЕТИ

Борзенков А. В., Гусак Я. О., Саскевич А. В.

УО «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь, e-mail: borzenkov_a@mail.ru

Рассмотренное на предыдущей конференции поведение антагонистического программного обеспечения типа вирус-антивирус в Internet [1], исследуется на предмет моделирования отражения вирусной атаки. Начинается атака на сеть – вброс вирусов $\omega(t, x) = \omega(t)$. Выпишем уравнение [2], моделирующее поведение вирусов $x(t)$ в сети $dx/dt = f(t, x, y) + \omega(t)$, $x(0) = x^0$, $0 \leq \omega(t) \leq \omega^*$, где $\omega(t)$ некоторая функция возмущения без априорной информации о ней. Наша цель противодействовать заражению – построить функцию $u(t, y) = u(t)$, которая, управляя поведением антивирусов $y(t)$ в сети $dy/dt = g(t, x, y) + u(t)$, $y(0) = y^0$, $0 \leq u(t) \leq u^*$, обеспечивает за кратчайшее время $t^* \rightarrow \min$ минимальное количество вирусов (или их полное уничтожение) $x(t^*) = \varepsilon$, гарантирующее устойчивое функционирование компьютерной сети. Это задача синтеза оптимального управления по быстродействию на состоянии нелинейной системы дифференциальных уравнений. Построенную математическую модель можно детализировать, рассматривая не только эффекты взаимодействия вируса и антивируса, но и программного антивирусного обеспечения сети. В этом случае [2] добавляется уравнение вида $dn/dt = f(t, x, y, n)$, $n(0) = n^0$, описывающее количество $n(t)$ неинфицированных компьютеров в сети, а требование к критерию качества таково $n(t^*) = N$. Еще более усложняет задачу учет бэкдоров и системных патчей [2]. Для решения задач используется принцип максимума Л.С. Понтрягина.

Литература

1. Борзенков А.В., Коновалов О. Л., Анисеев А. А., К моделированию поведения вирусов в WWW при наличии антивирусного ПО и системных патчей. / Сборник материалов WebConf 2012. – Минск, 2012. – С. 130.