

УДК 004.942+ 518.6

ПОСТРОЕНИЕ ОПТИМАЛЬНОГО УПРАВЛЕНИЯ В ЗАДАЧЕ ЗАЩИТЫ КОМПЬЮТЕРНОЙ СЕТИ ОТ ВРЕДОНОСНОГО КОДА

Н.А. СЕМЫКИНА

В статье рассматривается математическая модель защиты компьютерной сети от вируса, которая формализована в виде задачи оптимального управления нелинейной системой. Для построения задачи оптимального управления делается выбор целевого функционала, определяющего общую стоимость нанесенного ущерба от атаки вредоносным кодом, при этом учитывается дополнительное требование – максимизация числа защищенных компьютеров. Формулируются необходимые условия оптимальности поставленной задачи в виде принципа максимума Понтрягина. Определяется количество точек переключения оптимального управления. Используя метод множителей Лагранжа, выписывается вид оптимального управления.

Ключевые слова: компьютерный вирус, математическая модель, нелинейная система дифференциальных уравнений, оптимальное управление.

ВВЕДЕНИЕ

На данном этапе технического развития защита компьютеров и сетей от вирусов является одной из важных задач в IT-области. Число вредоносного программного обеспечения постоянно растет, а создание патча для нового вируса занимает достаточное количество времени. Это порождает, в свою очередь, глобальные сетевые эпидемии. Поэтому создание максимально защищенных систем от проникновения вредоносного кода является одним из актуальных направлений в научных исследованиях в сфере информационной безопасности.

Для создания защищенных систем надо использовать все теоретические исследования в области компьютерной безопасности, известные на данный момент, с целью детального исследования этого явления. Это позволит выявить различные свойства и факторы, влияющие на распространение вируса. Одним из аналитических исследований является математическое моделирование.

Основной этап моделирования эпидемии вредоносных программ – выбор эпидемиологической модели, адекватно описывающей этот процесс. Большинство исследователей в области компьютерных вирусов проводят аналогию между вредоносным программным обеспечением и природными вирусами, сетевой эпидемией и биологической эпидемией. С математической точки зрения органические и компьютерные вирусы имеют одинаковые характеристики и свойства, распространение описывается сходными дифференциальными уравнениями. Исследование статистических данных также показывает адекватность применения модели эпидемии инфекционных заболеваний для описания процесса развития вирусной атаки. Поэтому использование теории математического моделирования биологических систем получило большое развитие в научных исследованиях по компьютерной безопасности.

1. МАТЕМАТИЧЕСКАЯ МОДЕЛЬ

Воспользуемся эпидемиологической терминологией для описания модели [1–2]. Все узлы компьютерной сети $N(t)$ делятся на 3 группы: $S(t)$ – число неинфицированных хостов, восприимчивых к заражению вирусом в единицу времени t , $I(t)$ – число зараженных машин в единицу времени t , $R(t)$ – число хостов, невосприимчивых к вредоносному коду, т.е. невосприимчивых хостов в единицу времени t . Таким образом, $S(T) + I(T) + R(T) = N(T)$, где $t \in [0, T]$, T – фиксировано.

Введем функции управления $u(t)$ и $v(t)$, которые будут характеризовать иммунизацию и лечение восприимчивых и инфицированных компьютеров в единицу времени t .

В соответствии с вышеперечисленными обозначениями процесс распространения вирусов в компьютерной сети описывается следующей системой дифференциальных уравнений с начальными условиями

$$\begin{aligned}\frac{dS}{dt} &= -\beta S(t)I(t) + bN(t) - \mu S(t) - u(t)S(t) + \sigma R(t), \quad S(0) = S_0, \\ \frac{dI}{dt} &= \beta S(t)I(t) - \mu I(t) - v(t)I(t), \quad I(0) = I_0, \\ \frac{dR}{dt} &= u(t)S(t) + v(t)I(t) - (\mu + \sigma)R(t), \quad R(0) = R_0.\end{aligned}\tag{1}$$

Здесь коэффициент β , характеризует темп распространения вредоносного кода в сети, b – параметр, характеризующий скорость прироста новых уязвимых узлов, μ – коэффициент, характеризующий постоянную скорость отключения компьютеров от сети, при этом отключение не связано с вирусной атакой. При создании нового вида вредоносной программы антивирусная защита не действует, и узел опять становится уязвимым с частотой заражения σ .

Функции $S(t)$, $I(t)$, $R(t)$ будем считать фазовыми переменными. Задача (1) представляет собой замкнутую систему с функциями управления $u(t)$ и $v(t)$, т.е. систему с обратной связью.

Управляющие параметры удовлетворяют ограничениям (2), представленным в виде системы нестрогих неравенств:

$$u(t) \geq 0, \quad v(t) \geq 0, \quad u(t) + v(t) \leq U.\tag{2}$$

Здесь U – максимальная норма управления, которая характеризуется техническими и экономическими возможностями.

Потребуем выполнения условия – в конечный момент времени рассматриваемого периода не менее 80 % компьютеров являются невосприимчивыми к заражению.

$$0,8N(T) \leq R(T),\tag{3}$$

где $N(T) = S(T) + I(T) + R(T)$ – общее количество компьютеров в сети в конечный момент времени.

Цель управления состоит в отыскании минимума функционала $J(u, v)$ на множестве допустимых процессов (1), (3) при ограничениях на управление (2).

$$J(u, v) = \int_0^T [cI(t) + \omega u(t)S(t) + \varpi v(t)I(t)] dt,$$

где c – относительная стоимость урона, нанесенного одной единицей инфицированного компьютера, ω – средняя стоимость установки антивирусного программного обеспечения, ϖ – средняя стоимость лечения инфицированного компьютера.

Учтем граничное условие (3) в минимизируемом функционале с помощью штрафной функции – положительной срезки [3]

$$J(u, v) = \int_0^T [cI(t) + \omega u(t)S(t) + \varpi v(t)I(t)] dt + A[\max\{0; 0,8N(T) - R(T)\}]^2. \quad (4)$$

$A > 0$ – штрафной множитель.

В результате задача управления будет состоять в минимизации функционала (4), представленного интегральным и терминальным слагаемыми, при заданных ограничениях (1) и (2).

2. НЕОБХОДИМЫЕ УСЛОВИЯ ОПТИМАЛЬНОСТИ

Для построения оптимального управления в сформулированной задаче (1)–(2), (4), применим принцип максимума [4]. Введем сопряженные вектор-функции $p_s(t), p_I(t), p_R(t)$, определенные на промежутке $[0, T]$. Данные функции являются непрерывными и почти всюду непрерывно дифференцируемыми.

Функция Понтрягина в регулярном случае будет иметь вид

$$H(t, S, I, R, u, v, p_s, p_I, p_R) = -(cI + \omega uS + \varpi vI) + p_s(t)(-\beta SI + bN - \mu S - uS + \sigma R) + \\ + p_I(t)(\beta SI - \mu I - vI) + p_R(t)(uS + vI - (\mu + \sigma)R).$$

Применяя необходимые условия оптимальности в виде принципа максимума Понтрягина, выпишем уравнения для определения сопряженных функций с условиями трансверсальности на правом конце траектории

$$\begin{aligned} \frac{d\bar{p}_s}{dt} &= (\omega + \bar{p}_s(t) - \bar{p}_R(t))\bar{u}(t) + \bar{p}_s(t)(\mu - b) + \beta\bar{I}(t)(\bar{p}_s(t) - \bar{p}_I(t)), \\ \frac{d\bar{p}_I}{dt} &= (\varpi + \bar{p}_I(t) - \bar{p}_R(t))\bar{v}(t) + c + \mu\bar{p}_I(t) - b\bar{p}_s(t) + \beta\bar{S}(t)(\bar{p}_s(t) - \bar{p}_I(t)), \\ \frac{d\bar{p}_R}{dt} &= \bar{p}_R(t)(\mu + \sigma) - (b + \sigma)\bar{p}_s(t); \\ \bar{p}_s(T) &= \bar{p}_I(T) = -1,6A(\max\{0,8N(T) - R(T); 0\}), \\ \bar{p}_R(T) &= 0,4A(\max\{0,8N(T) - R(T); 0\}). \end{aligned} \quad (5)$$

Исследуя принцип максимума, получаем, что оптимальное управление является решением задачи максимизации с системой ограничений типа неравенств:

$$\begin{aligned} (\omega + p_R - p_s)Su(t) + (\varpi + p_R - p_I)Iv(t) &\rightarrow \max_{u,v}, \\ u(t) \geq 0, v(t) \geq 0, 0 \leq u(t) + v(t) \leq U, &t \in [0, T]. \end{aligned} \quad (6)$$

Так как функции управления входят линейно в функцию Понтрягина, то выписать функции переключения достаточно просто. Они будут иметь вид

$$\phi_1(t) = (\omega + p_R(t) - p_s(t))S(t), \quad \phi_2(t) = (\varpi + p_R(t) - p_I(t))I(t).$$

Делая замену переменных в сопряженной системе (5), получаем линейную систему дифференциальных уравнений для функций переключения

$$\dot{\phi}(t) = F(t)\phi(t) + f(t), \text{ где } \phi(t) = (\phi_1(t), \phi_2(t))^T, \quad (7)$$

$$F(t) = \begin{pmatrix} \frac{bN(t) + \sigma R(t)}{S(t)} & \beta \frac{S(t)}{N(t)} \\ \beta \frac{I(t)}{N(t)} + \sigma \frac{I(t)}{S(t)} & 0 \end{pmatrix}, \quad f(t) = \begin{pmatrix} \left(\omega(\mu + \sigma) + \beta(\omega - \varpi) \frac{I(t)}{N(t)} \right) S(t) \\ \left(\mu\varpi + \sigma\omega - c + \beta(\omega - \varpi) \frac{S(t)}{N(t)} \right) I(t) \end{pmatrix}.$$

Так как $F(t)$ и $f(t)$ непрерывны при $t \in [0, T]$, то решение системы линейных дифференциальных уравнений (7) определяется выражением [5]

$$\phi(t) = e^{-Q} \left(C + \int_0^t f(t) e^{-Q} dt \right), \text{ где } Q(t) = \int_0^t F(t) dt, C - \text{const.}$$

При этом $f(t) \neq 0$, $t \in [0, T]$, а значит, имеет только одну точку τ , в которой $\phi(\tau) = 0$.

Утверждение. Управление $(u(t), v(t))$, отвечающее системе (1) и минимизирующее функционал (4), является кусочно-постоянной функцией и имеет не более одной точки переключения.

3. ПОСТРОЕНИЕ ОПТИМАЛЬНОГО УПРАВЛЕНИЯ

Применим правило множителей Лагранжа [6]. Функция Лагранжа задачи (6) имеет вид (рассматриваем регулярный случай)

$$L(u, v, \lambda) = (\omega + p_S - p_R)Su + (\varpi + p_I - p_R)Iv + \lambda_1(u + v - U) - \lambda_2u - \lambda_3v,$$

где $\lambda_1, \lambda_2, \lambda_3$ – множители Лагранжа.

Так как все функции задачи являются непрерывно дифференцируемыми, то с необходимостью и достаточностью существуют множители Лагранжа $\lambda_1, \lambda_2, \lambda_3$ такие, что выполняются условия:

1) стационарности

$$\frac{\partial L(u, v, \lambda)}{\partial u} = (\omega + p_S - p_R)S + \lambda_1 - \lambda_2 = 0,$$

$$\frac{\partial L(u, v, \lambda)}{\partial v} = (\varpi + p_I - p_R)I + \lambda_1 - \lambda_3 = 0;$$

2) дополняющей нежесткости $\lambda_1(u + v - U) = 0$, $\lambda_2u = 0$, $\lambda_3v = 0$;

3) неотрицательности $\lambda_1 \geq 0$, $\lambda_2 \geq 0$, $\lambda_3 \geq 0$;

4) допустимости $u \geq 0$, $v \geq 0$, $u + v \leq U$.

Из выписанных условий составляем систему нелинейных уравнений, решая которую относительно u и v , получаем вид оптимального управления, зависящий от следующих условий:

- 1) $u = 0$, $v = 0$, если одновременно нарушаются ограничения $u \geq 0$ и $u \geq 0$ (т.е. $\lambda_2 > 0, \lambda_3 > 0$);
- 2) $u = U$, $v = 0$, если не выполнено условие $v \geq 0$ (т.е. $\lambda_3 > 0$);
- 3) $u = 0$, $v = U$, если нарушено условие $u \geq 0$ (т.е. $\lambda_2 > 0$);
- 4) $u = U - v$, $0 \leq v \leq U$, если не выполнено условие $u + v \leq U$ (т.е. $\lambda_1 > 0$).

Если все три ограничения не нарушаются (т.е. $\lambda_1 = 0, \lambda_2 = 0, \lambda_3 = 0$), то функции переключений тождественно равны нулю. Тогда возникает особый режим оптимального управления и для нахождения вида функции управления требуется применить соответствующие необходимые условия.

СПИСОК ЛИТЕРАТУРЫ

1. **Leveille J.** Epidemic spreading in technological networks // Technical Report HPL-2002-287, HP Laboratories Bristol, October 2002. URL: <http://www.hpl.hp.com/techreports/2002/HPL-2002-287.pdf>
2. **Воронцов В.В., Котенко И.В.** Аналитические модели распространения сетевых червей // Труды СПИИРАН, Вып. 4. – СПб.: Наука, 2007. – С. 208–224.
3. **Евтушенко Ю.Г.** Методы решения экстремальных задач и их применение в системах оптимизации. – М.: Наука, 1982. – 432 с.
4. **Анреева Е.А., Цирулева В.М.** Вариационное исчисление и методы оптимизации. – М.: Высшая школа, 2006. – 584 с.
5. **Камке Э.** Справочник по обыкновенным дифференциальным уравнениям. – М.: Наука. Гл. ред. физ-мат. лит., 1971. – 584 с.
6. **Васильев Ф.П.** Численные методы решения экстремальных задач. – М.: Наука. Гл. ред. физ-мат. лит., 1988. – 552 с.

THE OPTIMAL CONTROL IN THE MODEL OF NETWORK SECURITY FROM MALICIOUS CODE

Semykina N.F.

The paper deals with a mathematical model of network security. The model is described in terms of the nonlinear optimal control. As a criterion of the control problem quality the price of the summary damage inflicted by the harmful codes is chosen, under additional restriction: the number of recovered nodes is maximized. The Pontryagin maximum principle for construction of the optimal decisions is formulated. The number of switching points of the optimal control is found. The explicit form of optimal control is given using the Lagrange multipliers method.

Key words: computer virus, mathematical model, nonlinear system of differential equations, optimal control.

REFERENCES

1. **Leveille J.** Epidemic spreading in technological networks. Technical Report HPL-2002-287, HP Laboratories Bristol, October 2002. URL: <http://www.hpl.hp.com/techreports/2002/HPL-2002-287.pdf>
2. **Voroncov V.V., Kotenko I.V.** Analiticheskie modeli rasprostraneniya setevykh chervej. Trudy SPIIRAN. Issue 4. SPb.: Nauka. 2007. Pp. 208–224.

3. Evtushenko Yu.G. Metody resheniya ehkstremal'nyh zadach i ih primeneniye v sistemah optimizatsii. Moscow: Nauka. 1982. 432 p.

4. Andreeva E.A., Ciruleva V.M. Variacionnoye ischisleniye i metody optimizatsii. M.: Vysshaya shkola. 2006. 584 p.

5. Kamke E. Spravochnik po obyknovennym differentsial'nym uravneniyam. Moscow: Nauka. Gl. red. fiz-mat. lit. 1988. 584 p.

6. Vasil'ev F.P. Chislennyye metody resheniya jekstremal'nyh zadach. Moscow: Nauka. Gl. red. fiz-mat. lit. 1988. 552 p.

СВЕДЕНИЯ ОБ АВТОРЕ

Семыкина Наталья Александровна, окончила Тверской государственный университет, кандидат физико-математических наук, доцент кафедры компьютерной безопасности и математических методов управления Тверского государственного университета, область научных интересов – математическое моделирование, численные методы решения задач оптимального управления, электронный адрес: semykina.tversu@yandex.ru.