DOI: 10.25728/iccss.2023.94.99.022

Кереселидзе Н.Г.

Об одном аспекте информационной безопасности в модели борьбы с дезинформацией

Аннотация: В работе исследована математическая и компьютерная модель эффективной борьбы с дезинформацией. В компартментальной модели распространения ложной информации в обществе имеется группы граждан: – Риска, склонная к восприятию дезинформаций; Адептов – принявшие ложную информацию и с Иммунитетом – отвергнувшие ложную информацию с самого начала или в будущем адептами. Вводится уровень барьера числа адептов, в качестве меры информационной безопасности общества. В результате компьютерного эксперимента выявлены возможности бесконтрольного роста числа адептов, угрожающие безопасности общества в целом.

Ключевые слова: математическая модель, компьютерная модель, дезинформация, информационная безопасность, задача оптимального управления

Введение

Математическая модель эффективной борьбы с дезинформацией предложена в работе [1] в форме задачи оптимального управления:

$$J\left(y_4(t), M_1\right) = \int_0^T \phi(t) y_4(t)\, dt \to inf, \qquad y_4(t) \in C^1, \quad M_1 \in R. \qquad (1)$$

$$\begin{cases} \dfrac{dy_1(x)}{dx} = -\lambda y_4(x) y_1(x) - \kappa y_5(x) y_1(x) - \alpha_1 y_1(x) y_2(x) - \alpha_2 y_1(x) y_3(x), \\ \dfrac{dy_2(x)}{dx} = \alpha_1 y_1(x) y_2(x) + \kappa y_5(x) y_1(x) - \lambda_1 y_4(x) y_2(x) - \gamma y_2(x) - \beta_1 y_2(x) y_3(x), \\ \dfrac{dy_3(x)}{dx} = \gamma y_2(x) + \alpha_2 y_1(x) y_3(x) + \beta_1 y_2(x) y_3(x) + \lambda_1 y_4(x) y_2(x) + \lambda y_4(x) y_1(x), \\ \dfrac{dy_4(x)}{dx} = \omega_1 y_2(x) \left(1 - y_4(x) \Big/ M_1\right), \\ \dfrac{dy_5(x)}{dx} = \omega_2 y_1(x) \left(1 - y_5(x) \Big/ M_2\right). \end{cases} \quad (2)$$

$$\begin{cases} y_1(0) = R_0 > 0, y_2(0) = A_0 > 0, y_3(0) = I_0 \geq 0, \\ y_4(0) = N_0, \quad y_5(0) = F_0. \end{cases} \quad (3)$$

$$y_2(T) \leq 0,05M \quad (4)$$

где $y_1(t)$ – численность группы риска – т.е. тех людей, которые еще не находятся под влиянием ложной информации, но возможно станут ее адептами в силу влияния потоков ложной информации распространяемого неким источником в объеме $y_5(t)$. Численность группы адептов, оказавшихся под влиянием дезинформаций – $y_2(t)$, $y_3(t)$ – численность группы с иммунитетом, которые не восприняли дезинформацию или освободились от нее, в какой то степени под влиянием потоков анти ложной информации распространяемого неким источником в объеме $y_4(t)$.

Динамическая система (2) рассматривается на отрезке времени $[0;T]$. В системе (2) все коэффициенты постоянные и положительные, M_1 и M_2 означают уровни Интернет-технологий, с помощью которых распространяются, соответственно, потоки анти и ложной информации. Коэффициенты системы (2) устанавливаются эмпирически, специалистами, с помощью которых описывается интенсивность перехода граждан из одной группы в другую.

Система (3) – это начальные условия, (4) означает, что в конце интервала времени численность адептов не должна превышать пяти

процентов численности всего общества. Считается, что при таком количестве адептов влияние дезинформации на общество в целом несущественно, и оно в состоянии принимать объективные и адекватные решения на выборах или референдумах.

Ставится задача перевода системы из начального состояния (3) в конечное – (4). При этом, желательно, чтобы расходы на этот перевод были минимальными (1). Расходы рассчитываются от генерациии достоверной информации, взвешенной на некую «цену» – $\phi(t)$, и соответствующего уровня ИТ – M_1. Фактически имеются управляющие параметры: ω_1 – определяющий уровень потока анти ложной информации и M_1.

Задача управляемости

Будем считать, что система закрытая, т.е. количество людей в обществе постоянное в любой момент времени:

$$y_1(t)+y_2(t)+y_3(t)=R_0+A_0+I_0=N=const, \text{ для любого } t\in[0;T], \quad (5)$$

где N численность общества.

В системе (2) неизвестные функции будем искать в классе непрерывно дифференцируемых функции на $[0;T]$ – $C^1[0;T]$. Таким образом, для задачи Коши (2), (3) существует единственное решение. Что же касается граничной задачи (2), (3), (4) то ее будем исследовать численными методами на предмет управляемости системы.

Компьютерный эксперимент проведен с использованием системы MatLab. Пусть имеем следующие граничные условия: $T=15$, $y_1(0)=400$, $y_2(0)=50$, $y_3(0)=10$, $y_4(0)=1$, $y_5(0)=17$, $y_2(15)\le 460/20=23$. Коэффициенты системы (2) имеют значения: $\lambda=0,015$; $\lambda_1=0,011$; $\kappa=0,009$; $\alpha_1=0,013$; $\alpha_2=0,014$; $\beta_1=0,013$; $\gamma=0,0092$ $\omega_1=0,018$; $\omega_2=0,017$; $M_1=45$; $M_2=60$.

Для решения задачи Коши (2), (3) при значениях указанных выше используем решатель ode15s, составлен программный код:

Листинг – [X,Y]=ode15s(@adsys,[0 15],[400 50 10 1 17]);
plot(X,Y,'linewidth',2); legend('y1','y2','y3','y4','y5')
function dydx=adsys(x,y)
l=0.015; l1=0.011; k=0.009; a1=0.031; a2=0.014; b=0.013;g=0.0092;
o1=0.018;o2=0.77; m1=45; m2=60;
dydx=[-l*y(1)*y(4)-k*y(1)*y(5)-a1*y(1)*y(2)-a2*y(1)*y(3)
a1*y(1)*y(2)+k*y(1)*y(5)-l1*y(2)*y(4)-g*y(2)-b*y(2)*y(3)
g*y(2)+a2*y(1)*y(3)+b*y(2)*y(3)+l1*y(2)*y(4)+l*y(1)*y(4)
o1*y(2)*(1-y(4)/m1)
o2*y(1)*(1-y(5)/m2)]
end

Источник распространяющий ложную информацию назовем второй стороной, первой назовет источник распространяющую анти ложную информацию. Компьютерный эксперимент показывает, что у первой стороны при малых усилиях удается нейтрализовать влияние ложной информации к концу интервала времени – число адептов фактически равно нулю, хотя, достаточно, чтобы численность адептов была меньше пяти процентов численности общества [2] (рисунок 1).

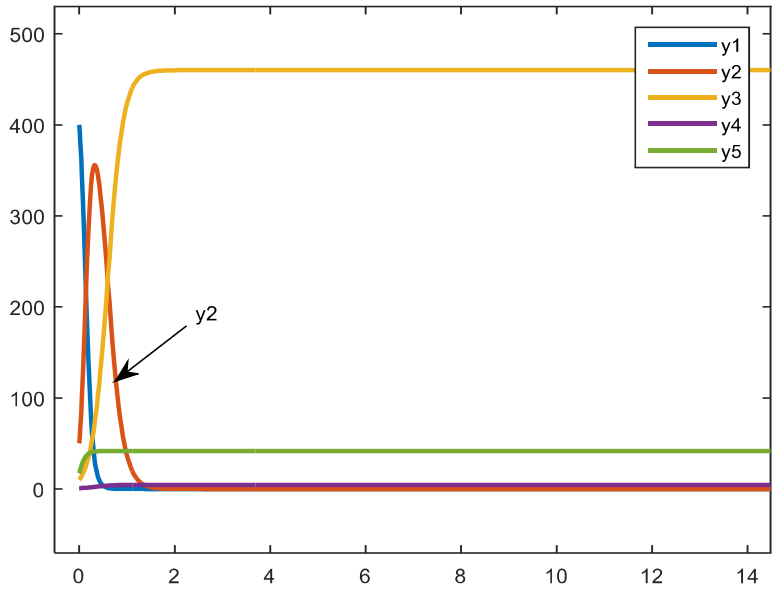

Рисунок 1 – Управляемость модели борьбы с дезинформацией

Аналогичный результат достигается и для других значений параметров системы – информационная безопасность обеспечивается к концу интервала. Однако, тем не менее информационная безопасность уязвима, но не в конце интервала, а в начале. Если обратить внимание на значение численности адептов в начале интервала, то оказывается, что, например, в нашем примере, ее максимальное значение равно 355,947924151334 в момент времени 0,335176470970211. Что приблизительно составляет 77% численности общества (рисунок 2).

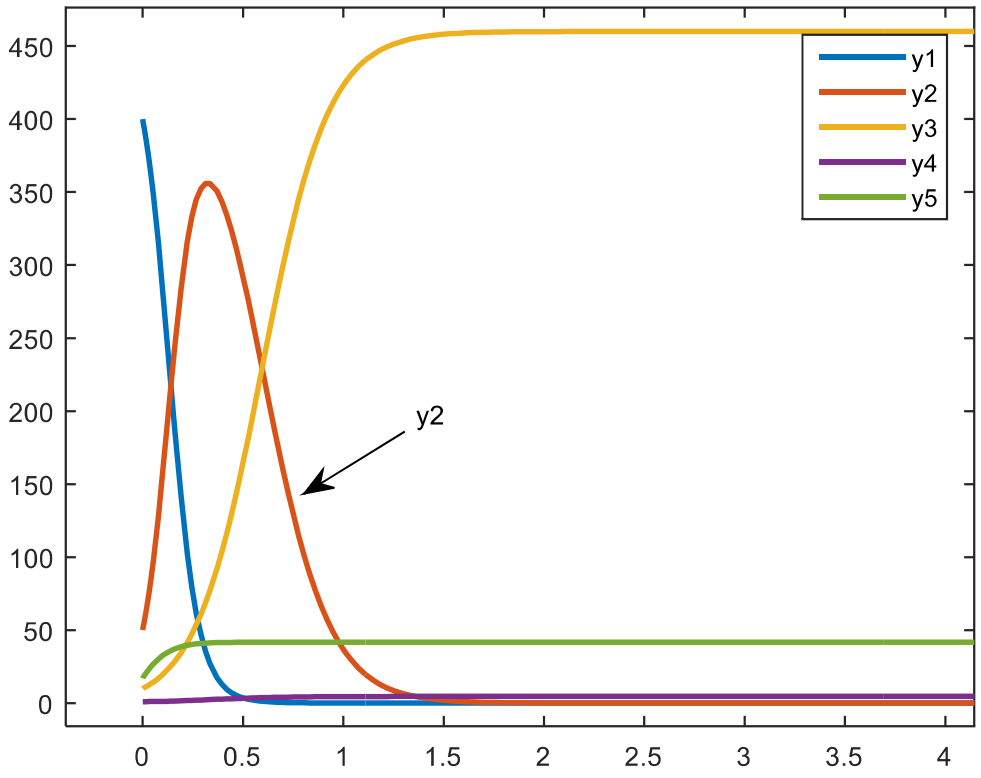

Рисунок 2 – Уязвимость информационной безопасности

При этом на достаточном большом интервале времени число адептов больше 50% численности общественности.

Выводы

Для информационной безопасности общества не является достаточным уменьшение численности адептов дезинформации только к определенному моменту времени, например, перед каким

либо голосованием. Так как в некоторые моменты влияние дезинформации на общество может столь сильным, что общество в целом может легитимировать революционные, внеочередные парламентские, президентские выборы и т.п. Поэтому, в задаче оптимального управления борьбы с дезинформацией следует внести коррективы и заменить (4) на следующее выражение:

$$y_2(t) \le 0,05 \times N \text{, для } \forall t \in [0;T]. \qquad (6)$$

Иначе, модель может «пропустить» не только критическое нарушение информационной безопасности, но и безопасности государства.

Литература:

1. *Kereselidze N.* About Optimal Control Task of the Fight Against Disinformation // Proceedings of Tskhum-Abkhazian Academy of Sciences. – 2022. – Vol. 22. – P. 23-29. – DOI: 10.52340/ptaas.2022.22.02.

2. *Kereselidze N.* The Issue of Manageability of the Task of Optimal Fight Against Disinformation / Book of abstracts XIII International Conference of the Georgian Mathematical Union, Batumi, September 4-9, 2023. – Batumi Shota Rustaveli State University, 2023. – P. 147.

DOI: 10.25728/iccss.2023.77.71.023

Курако Е.А., Асратян Р.Э., Орлов В.Л.

Об одном подходе к обеспечению технологического суверенитета в разработках распределенных информационных систем

Аннотация: Рассмотрены способы импортозамещения распределенных информационных систем, основанных на применении языка программирования C#. Описаны методы преобразования таких систем с целью возможности их выполнения в среде, компоненты которой включены в реестр российского программного обеспечения. Основу рассматриваемой среды составляют операционные