УДК 004.942

ИССЛЕДОВАНИЕ УСТОЙЧИВОСТИ СИСТЕМЫ, МОДЕЛИРУЮЩЕЙ РАСПРОСТРАНЕНИЕ ВРЕДОНОСНОГО КОДА

Н. А. Семыкина

ANALYSIS OF THE STABILITY OF THE MALWARE PROPAGATION MODEL

N. A. Semykina

В статье исследована устойчивость нелинейной системы обыкновенных дифференциальных уравнений, которая моделирует процесс распространения вируса в компьютерной сети. Анализ проводился с помощью первого и второго методов Ляпунова. Получены условия существования устойчивого положения равновесия. Приведены результаты численных экспериментов, подтверждающие аналитические выводы.

The paper focuses on the stability of nonlinear system of differential equations. The system simulates the process of computer virus propagation into the network. The Lyapunov methods are used for analysis. The research revealed the conditions of the stability of virus infection equilibrium. Numerical simulations are provided to support the theoretical conclusions.

Ключевые слова: математическая модель, компьютерный вирус, устойчивость системы, нелинейная система дифференциальных уравнений, метод Ляпунова.

Keywords: mathematical model, computer virus, stability of the system, nonlinear system of differential equations, Lyapunov method.

Введение

С помощью математических моделей распространения компьютерных вирусов и последующего исследования эволюции системы можно изучить динамику численности зараженных узлов и условия распространения эпидемии вредоносного кода. Большинство математических моделей описано с помощью управляемых систем дифференциальных уравнений с ограничениями. Анализируя устойчивость стационарных точек данных систем, можно сделать выводы о характере развития эпидемии и способах ее погашения. Это позволяет оценить эффективность и скорость различных мер противодействия.

Построение модели

Процесс защиты сети от распространения вредоносного кода на фиксированном промежутке времени [0, T], будем описывать с помощью эпидемиологической модели в следующих предположениях [1, 2]:

1) $N(t)$ – общее количество машин в сети;

2) произвольный узел локальной сети может находиться в трех состояниях: уязвимом $S(t)$, инфицированном $I(t)$ и невосприимчивом $R(t)$;

3) вирус самопроизвольно размножается по сети без участия пользователя;

4) распространение копии вредоносной программы происходит с постоянной частотой, характеризуемой коэффициентом β. В общем случае данный коэффициент можно рассматривать как функцию от времени $\beta(t)$;

5) количество компьютеров в сети является переменным числом и параметр *b,* характеризует скорость прироста новых уязвимых узлов;

6) в реальных условиях «лечение» происходит за счет установки антивирусного программного обеспечения или межсетевых экранов. При этом иммунитет приобретают не только инфицированные компьютеры, но и уязвимые со средней скоростью иммунизации u для восприимчивых узлов и v для инфицированных компьютеров;

7) часть компьютеров отключаются от сети, при этом отключение не связано с вирусной атакой. μ – коэффициент, характеризующий скорость отключения;

8) на практике антивирусная защита работает для определенного вредоносного ПО. При появлении нового вида вируса узел опять становится уязвимым с частотой заражения σ.

Схематичное представление этой модели отражено на рисунке 1.

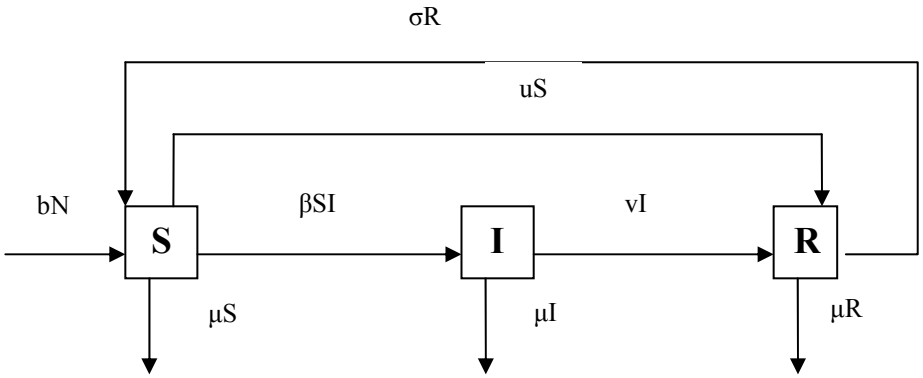

Рис. 1. ***Представление модели***

В соответствии с вышеперечисленными предположениями имеем следующую систему дифференциальных уравнений с начальными условиями:

$$\begin{cases} \dfrac{dS}{dt} = -\beta S(t)I(t) + bN(t) - \mu S(t) - uS(t) + \sigma R(t), \quad S(0) = S_0, \\ \dfrac{dI}{dt} = \beta S(t)I(t) - \mu I(t) - vI(t), \quad I(0) = I_0, \\ \dfrac{dR}{dt} = uS(t) + vI(t) - (\mu + \sigma)R(t), \quad R(0) = R_0. \end{cases} \tag{1}$$

Здесь $N(t) = S(t) + I(t) + R(t)$, тогда $\dfrac{dN}{dt} = (b - \mu)N(t)$.

Для описания модели использованы следующие переменные и постоянные величины, приведенные в таблице.

Таблица

Параметр	***Описание***
$N(t)$	Общее количество машин в сети
$S(t)$	Количество уязвимых узлов в момент времени t
$I(t)$	Количество инфицированных узлов в момент времени t
$R(t)$	Количество невосприимчивых узлов в момент времени t
β	Коэффициент, характеризующий скорость заражения уязвимых узлов
b	Коэффициент, характеризующий скорость прироста новых уязвимых узлов
μ	Коэффициент, характеризующий скорость отключения узлов от сети, независящая от вируса
σ	Коэффициент, характеризующий скорость, с которой невосприимчивые хосты вновь становятся уязвимыми
u	Параметр, характеризующий скорость «иммунизации» уязвимых узлов
v	Параметр, характеризующий скорость лечения инфицированных узлов

Функции $S(t)$, $I(t)$, $R(t)$ будем считать фазовыми переменными. Если коэффициенты u и v рассматривать как управляющие параметры, то задача (1) представляет собой систему с обратной связью (замкнутую систему). Замкнутые системы при своей деятельности стремятся к состоянию равновесия. С помощью обратной связи модель адаптируется к изменениям при внешних воздействиях, т. е. реализуется механизм автокоррекции системы.

Управляющие параметры удовлетворяют условиям (2), которые характеризуют ограничения в технических и экономических возможностях:

$$0 \le u \le U_{\max} \le 1,\ 0 \le v \le V_{\max} \le 1. \tag{2}$$

Исследуем динамику и устойчивость системы (1).

Исследование устойчивости

Пусть существуют положения равновесия, которые обозначим через $x_i^* = \left(S_i^*, I_i^*, R_i^*\right)$, $i = 1,2,\ldots$, у системы (1). Предполагая, что $u = \text{const} \in \left[0, U_{\max}\right]$ и $v = \text{const} \in \left[0, V_{\max}\right]$, удовлетворяющие условию (2), найдем стационарные точки. Для этого требуется решить следующую систему нелинейных уравнений:

$$\begin{cases} -\beta SI + (b - \mu - u)S + (b + \sigma)R + bI = 0, \\ \left(\beta S - \mu - v\right)I = 0, \\ uS + vI - (\mu + \sigma)R = 0. \end{cases} \tag{3}$$

Рассматривая различные варианты равенства нулю множителей второго уравнения системы (3), можно найти различные стационарные решения.

В результате получаем следующие нетривиальные точки равновесия:

$$x_1^* = \left(S_1^*, I_1^*, R_1^*\right) = \left(\frac{\mu+v}{\beta}, I_1^*, \frac{u(\mu+v)+v\beta I_1^*}{\beta(\mu+\sigma)}\right),$$

при условии $b = \mu$;

$$x_2^* = \left(S_2^*, I_2^*, R_2^*\right) = \left(S_2^*, 0, \frac{uS_2^*}{\mu+\sigma}\right),$$

при условии $b = \mu$;

$$x_3^* = \left(S_3^*, I_3^*, R_3^*\right) = \left(\frac{\mu+v}{\beta}, \frac{-(\mu+v)(\mu+\sigma+u)}{\beta(\mu+\sigma+v)}, \frac{(\mu+v)(u(\mu+\sigma+v)+v(\mu+\sigma+u))}{\beta(\mu+\sigma)(\mu+\sigma+v)}\right).$$

Из физического смысла задачи следует, что точка равновесия неотрицательна, т. е.:

$$S_i^* \geq 0, I_i^* \geq 0, R_i^* \geq 0, \ i = 1,2,\ldots.$$

Точка x_3^* не удовлетворяет этому условию и далее рассматриваться не будет.

Для анализа устойчивости полученных стационарных состояний нелинейной системы (1) используем метод Ляпунова по первому приближению – метод линеаризации системы в окрестности точек равновесия [3] – [5]. В нашей задаче матрица коэффициентов линеаризованной системы будет иметь следующий вид:

$$J(x_i^*) = \begin{pmatrix} -\beta I_i^* + b - \mu - u & -\beta S_i^* + b & b+\sigma \\ \beta I_i^* & \beta S_i^* - \mu - v & 0 \\ u & v & -\sigma-\mu \end{pmatrix}.$$

Исследуем состояние системы в окрестности точки равновесия $x_1^* = \left(S_1^*, I_1^*, R_1^*\right)$. Матрица системы первого приближения для данной точки будет иметь вид:

$$J(x_1^*) = \begin{pmatrix} -\beta I_1^* - u & -v & \mu+\sigma \\ \beta I_1^* & 0 & 0 \\ u & v & -\sigma-\mu \end{pmatrix}.$$

Собственные числа матрицы с постоянными коэффициентами являются решением уравнения третьего порядка

$$\lambda^3 + (\beta I_1^* + \sigma + u + \mu)\lambda^2 + \beta I_1^* (\mu + v + \sigma)\lambda = 0.$$

Решая данное характеристическое уравнение, находим собственные числа матрицы устойчивости

$$\lambda_{J(x_1^*)} = \left\{\lambda_1 = 0, \lambda_2 = \frac{1}{2}\left(-\beta I_1^* - \mu - \sigma - u - \sqrt{D}\right), \lambda_3 = \frac{1}{2}\left(-\beta I_1^* - \mu - \sigma - u + \sqrt{D}\right)\right\},$$

где

$$D = \beta^2 I_1^{*2} + 2\beta I_1^* (u - 2v - \mu - \sigma) + (\mu + \sigma + u)^2.$$

Здесь один корень равен нулю, а другие отрицательны. Например, если $u = v$, то

$$\lambda_{J(x_1^*)} = \left\{\lambda_1 = 0, \lambda_2 = -\mu - \sigma - u, \lambda_3 = -\beta I_1^*\right\}.$$

Следовательно, система (1) будет находиться на границе апериодической устойчивости. А. М. Ляпуновым было установлено, если линейная система первого приближения находится на границе устойчивости, то доказать устойчивость или неустойчивость исходной нелинейной системы по уравнениям первого приближения нельзя. Необходимо исследовать исходную нелинейную систему другими методами.

Применим второй метод Ляпунова [3] – [5]. Для этого рассмотрим знакопостоянную функцию:

$$V(S, I, R) = \frac{1}{2}(S + I + R)^2.$$

Функция $V(S, I, R)$ положительно определена для всех фазовых переменных, одновременно не обращающихся в нуль и непрерывна по всем своим частным производным первого порядка.

Производная от функции Ляпунова $V(S, I, R)$ по времени в силу системы нелинейных дифференциальных уравнений (1) записывается в виде:

$$\frac{dV}{dt} = \frac{\partial V}{\partial t} + \frac{\partial V}{\partial S}\dot{S} + \frac{\partial V}{\partial I}\dot{I} + \frac{\partial V}{\partial R}\dot{R} = (b - \mu)(S + I + R)^2.$$

Из последнего равенства видно, что если $b \leq \mu$, то производная функции Ляпунова будет определена условием $\frac{dV}{dt} \leq 0$. А это указывает на устойчивость по Ляпунову системы (1).

Заметим, что точки равновесия существуют при выполнении условия $b = \mu$. Данное равенство удовлетворяет условию устойчивости, полученного выше.

Анализируя вид точек равновесия, можно заметить, что количество узлов сети находящихся в невосприимчивом состоянии R будет больше числа уязвимых узлов S, т. е. на начало эпидемии большинство компьютеров должно быть обеспечено антивирусной защитой ($u > \mu + \sigma$). В этом случае распространение вредоносного ПО возможно остановить. Если защиту обеспечить не удалось, то в начальный период большая часть узлов будет уязвима ($\mu + \sigma > u$). Тогда для погашения эпидемии должно быть выполнено условие – количество зараженных компьютеров I не должно превышать определенного числа восприимчивых узлов: $I < \frac{\mu + \sigma - u}{v} S$.

Данные рассуждения можно проиллюстрировать численными экспериментами. Параметры выбраны

таким образом, чтобы условие $b = \mu$ выполнялось и число зараженных узлов *I* не превышает 5 % уязвимых *S*. На рис. 2 представлено численное решение. Рассмотрен случай, когда $b = \mu$ =0,00001. Точка равновесия определяется начальными условиями:

$$S_1^*(0) = \frac{\mu + v}{\beta},\ I_1^*(0) = 2,\ R_1^*(0) = \frac{u(\mu + v) + v\beta I_1^*}{\beta(\mu + \sigma)}.$$

При построении решения использованы следующие параметры: β = 0,000034, σ = 0,002, u = 0,001, v = 0,02.

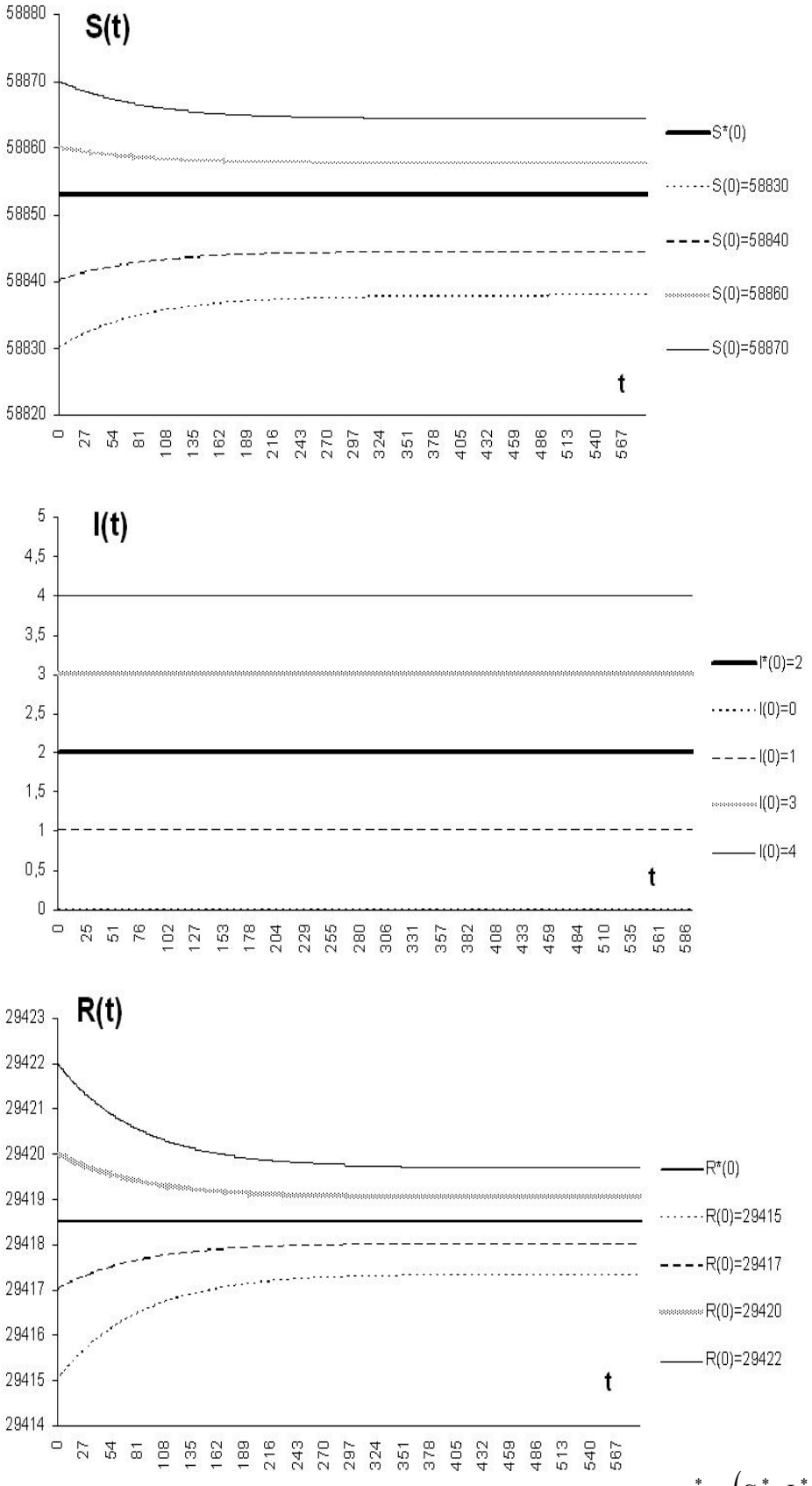

Рис. 2. ***Динамика системы (1) в окрестности точки равновесия*** $x_1^* = \left(S_1^*, I_1^*, R_1^*\right)$

Заметим, что траектория функции $S(t)$ и $R(t)$ асимптотически сходится к равновесному состоянию, а траектории функций $I(t)$ устойчивы.

Особо можно рассмотреть частный случай, когда компьютерная сеть не заражена вирусом, т. е. $I(t) = 0$, $t \in [0, T]$. Точка равновесия имеет вид $x_2^* = \left(S_2^*, I_2^*, R_2^*\right) = \left(S_2^*, 0, \frac{uS_2^*}{\mu + \sigma}\right)$. На рисунке 3 представлены результаты численных экспериментов при следующем наборе параметров: $S_2^*(0) = 1000$, $I_2^*(0) = 0$, $R_2^*(0) = \frac{uS_2^*}{\mu + \sigma}$, $\beta = 0{,}000006$, $\sigma = 0{,}00002$, $u = 0{,}001$, $v = 0{,}02$.

Из полученных графиков видно, что траектории функций S(t) и I(t) асимптотически сходится к равновесному состоянию, а траектории функции R(t) устойчивы.

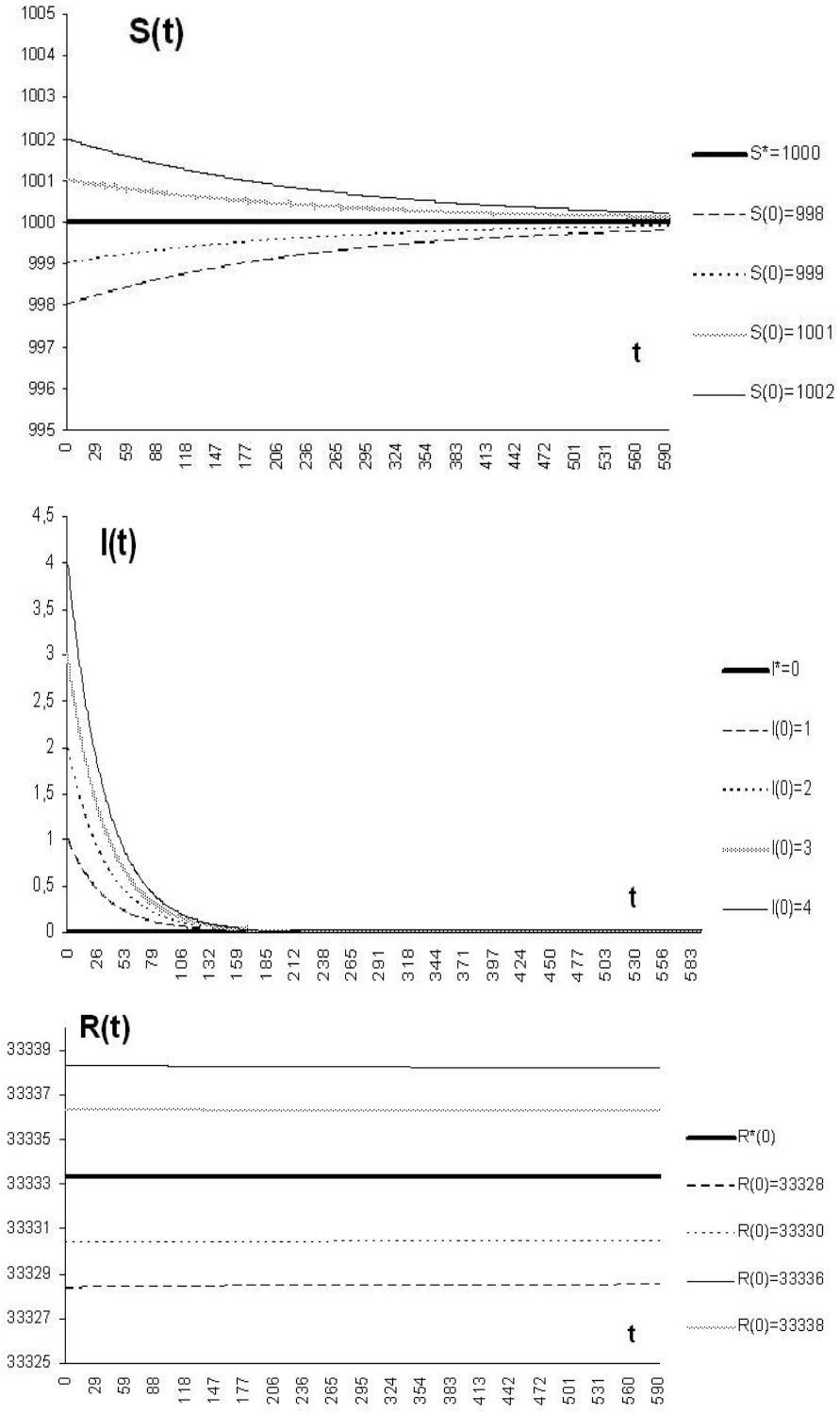

Рис. 3. ***Динамика системы*** **(1)** ***в окрестности точки равновесия*** x_2^* ***при параметрах*** **β = 0,0034, μ = b = 0,001, σ = 0,002, u = 0,2, v = 0,2**

Заключение

В данной статье найдены точки равновесия нелинейной системы дифференциальных уравнений. С помощью второго метода Ляпунова показана устойчивость этих точек при соответствующем условии. Если скорость прироста новых уязвимых узлов будет равна скорость отключения компьютеров от сети, то возмущение, вызванное воздействием вредоносного ПО на сеть, затухает и эпидемия может быть остановлена. Результаты подтверждены численными экспериментами.

Литература

1. Воронцов В. В., Котенко И. В. Аналитические модели распространения сетевых червей // Труды СПИИ-РАН. Вып. 4. СПб.: Наука, 2007. С. 208 – 224.

2. Zhang C., Zhao Y., Wu Y. An impulse model for computer viruses // Discrete Dynamics in Nature and Society. – Vol. 2012, Article ID 260962, 2012. – URL: http://dx.doi.org/10.1155/2012/260962

3. Бесекерский В. А., Попов Е. П. Теория систем автоматического регулирования. М.: Наука, 1975.

4. Демидович Б. П. Лекции по математической теории устойчивости. СПб.: Лань, 2008.

5. Молчанов А. М. Об устойчивости нелинейных систем. Пущено: ИМПБ РАН, 2013.

Информация об авторе:

Семыкина Наталья Александровна – кандидат физико-математических наук, доцент математического факультета кафедры компьютерной безопасности и математических методов управления Тверского государственного университета, semykina.tversu@yandex.ru.

Natalia A. Semykina – Candidate of Physics and Mathematics, Associate Professor, Assistant Professor at the Department of Computer Security and Mathematical Methods of Control, Tver State University.

Статья поступила в редколлегию 03.06.2014 г.