УДК 004.942 DOI: 10.26102/2310-6018/2019.26.3.012

Н. А. Семыкина

ПРОГНОЗИРОВАНИЕ ПОСЛЕДСТВИЙ РАСПРОСТРАНЕНИЯ ВИРУСА В КОМПЬЮТЕРНОЙ СЕТИ С ПОМОЩЬЮ БАЗОВОГО ПОРОГОВОГО ЧИСЛА

ФГБОУ ВО «Тверской государственный университет», Тверь, Россия

В современном мире Интернет является одним из самых распространённых инструментов для общения людей, поиска информации, покупки товаров и услуг и т.д. Большинство компьютеров обычно используют одно и то же программное обеспечение операционной системы и взаимодействуют со всеми другими компьютерами, используя стандартный набор протоколов. Это породило новое поколение преступников. Интернет является основным средством, используемым злоумышленниками для совершения компьютерных преступлений. Из-за большого сходства между распространением компьютерного вируса и распространением биологического вируса многие исследователи применяют математические модели эпидемиологии к компьютерной среде. Этот подход является наиболее эффективным для описания распространения вредоносного кода в сети. В статье для анализа SIRS-модели используются результаты теории математической эпидемиологии. Динамика распространения влияния вируса на компьютерную сеть описывается с помощью системы дифференциальных уравнений. Исследуется устойчивость сети к распространению вредоносных программ. Найдены положения равновесия при отсутствии заражения в сети и при эпидемии. В рамках исследуемой модели определяется базовое пороговое число. В зависимости от величины базового порогового значения можно предсказать эволюцию вирусной атаки и подобрать наилучшие противовирусные меры защиты сети. Приведены результаты численных экспериментов, подтверждающие аналитические выводы.

Ключевые слова: математическая модель, компьютерный вирус, динамика вирусов, базовое пороговое число, нелинейная система дифференциальных уравнений, устойчивость системы.

Введение. Одной из частных задач стратегической цели обеспечения информационной безопасности в области обороны страны является исследование и анализ устойчивости сетей в условиях распространения вредоносных программ, нарушающих функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации [1-2]. Решение данной задачи предполагает разработку новых моделей и методов прогнозирования, обнаружения и оценки информационных угроз.

Для исследования и решения задачи защищенности компьютерной сети активно используется аналитическое моделирование. Наиболее адекватно процесс деструктивного воздействия вредоносного ПО на компьютерную сеть описывают модели, основанные на математических моделях эпидемиологии. Одним из важнейших результатов теории

математической эпидемиологии является понятие базового порогового (репродуктивного) числа вируса R_0 [3]. Применительно к компьютерной эпидемии данная величина будет описывать среднее число компьютеров, зараженных от одного инфицированного узла, помещенного в полностью свободную от вируса компьютерную сеть.

Для широкого круга биологических моделей была сформулирована пороговая теорема [4], в которой сформулированы условия предотвращения эпидемии в зависимости от величины базового порогового числа (или порогового значения). Если базовое пороговое число R_0, меньше или равно единице, то со временем в пределе $t \to \infty$ инфекция не превращается в эпидемию и быстро исчезает. Если R_0 больше единицы, то происходит резкое увеличение количества инфицированных, переходящее в эпидемию.

Материалы и методы. Рассмотрим аналитическую модель распространения вредоносного кода в сети и оценим вирусную атаку с помощью базового порогового числа. Процесс эволюции эпидемии исследуем на фиксированном промежутке времени [0,T]. Все множество объектов компьютерной системы делится на подмножества, характеризующие состояния узлов сети: уязвимое $S(t)$, инфицированное $I(t)$ и невосприимчивое $R(t)$ к вирусу. Таким образом, $S(t)+I(t)+R(t) = N(t)$ – обще количество компьютеров, где $t \in [0, T]$. В общем виде схематичное представление модели отражено на Рисунке 1.

Для формализации модели будем использовать следующие обозначения: β – коэффициент, характеризующий темп распространения вредоносного кода в сети; μ – постоянная скорость отключения компьютеров от сети, при этом отключение не связано с вирусной атакой; b – скорость подключения к сети новых компьютеров; u –коэффициент, характеризующий «иммунизацию» восприимчивых узлов; γ – скорость обнаружения и лечения инфицированных компьютеров. Так как антивирусная защита работает для выявленного определенного вредоносного программного обеспечения, то при появлении нового вида вируса узел переходит в подмножество уязвимых с частотой заражения σ.

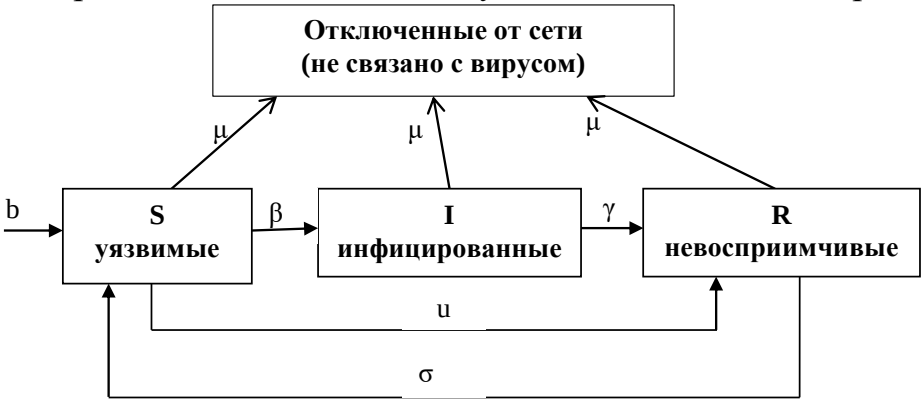

Рисунок 1 – Представление работы модели

С учетом введённых обозначений, модель можно представить в виде системы дифференциальных уравнений (1) – (3).

$$\dot{S}(t) = -\beta SI + b(S + I + R) - \mu S - uS + \sigma R, \quad (1)$$

$$\dot{I}(t) = \beta SI - \gamma I - \mu I, \quad (2)$$

$$\dot{R}(t) = uS + \gamma I - \mu R - \sigma R. \quad (3)$$

Будем считать, что в начальный момент времени количество компьютеров каждого типа состояния определено:

$$S(0) = S^0,\ I(0) = I^0,\ R(0) = R^0. \quad (4)$$

Для вычисления базового порогового числа требуется определить положения равновесия динамической системы. Пусть существуют стационарные точки, которые обозначим через $x_i^* = \left(S_i^*, I_i^*, R_i^*\right),\ i = 1,2,...$

Приравняв к нулю правые части уравнений (1) – (3) и решив систему, получаем следующие нетривиальные точки равновесия:

$$x_1^* = \left(S_1^*, I_1^*, R_1^*\right) = \left(S_1^*, 0, \frac{uS_1^*}{\mu + \sigma}\right), \text{ при условии } b = \mu;$$

$$x_2^* = \left(S_2^*, I_2^*, R_2^*\right) = \left(\frac{\mu + \gamma}{\beta}, I_2^*, \frac{u(\mu + \gamma) + \gamma\beta I_2^*}{\beta(\mu + \sigma)}\right), \text{ при условии } b = \mu;$$

$$x_3^* = \left(S_3^*, I_3^*, R_3^*\right) =$$

$$= \left(\frac{\mu + \gamma}{\beta}, \frac{-(\mu + \gamma)(\mu + \sigma + u)}{\beta(\mu + \sigma + \gamma)}, \frac{(\mu + \gamma)(u(\mu + \sigma + \gamma) + v(\mu + \sigma + u))}{\beta(\mu + \sigma)(\mu + \sigma + \gamma)}\right).$$

Из физического смысла задачи следует, что значения фазовых функций *S*(t), *I*(t), *R*(t) неотрицательны, тогда $S_i^* \geq 0, I_i^* \geq 0, R_i^* \geq 0,\ i = 1,2,3.$ Так как положение равновесия x_3^* не удовлетворяет этому условию, то рассматриваться не будет.

Заметим, что положение равновесия x_1^* соответствует ситуации, когда вредоносное ПО в компьютерной сети со временем уничтожается при любом начальном условии (4). Точка x_2^* описывает положение эндемического равновесия.

Используя второй метод Ляпунова [5], можно доказать, что найденные положения равновесия будут устойчивы по Ляпунову при условии $b \leq \mu$. Для доказательства была построена положительно определенная и непрерывная по всем своим частным производным первого порядка функция Ляпунова:

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

Для построения базового порогового значения для модели (1)– (3) определим классы, в которых происходит прирост зараженных компьютеров. Уравнение (2) модели описывает класс, являющийся распространителем вируса, а уравнения (1) и (3) описывают 2 класса неинфицированных компьютеров. Новые узлы с вредоносным ПО возникают только в классе *I*.

Введем функцию скорости появления новых зараженных узлов в компьютерной сети $\Psi=\beta SI$ и функцию выхода из группы инфицированных $\Omega=(\mu+\gamma)I$.

Линеаризуем выражение (2) в окрестности точки равновесия *x**, для этого определим следующие функции

$$F=\frac{\partial\Psi}{\partial I}(x_i^*)=\beta S^*, V=\frac{\partial\Omega}{\partial I}(x_i^*)=\mu+\gamma,\ \ i=1,2.$$

Если изначально инфицированный узел находился в сети, то функция V^{-1} характеризует среднее время перехода инфицированного компьютера в группу невосприимчивых. А функция *F* показывает скорость передачи вируса машинам в сети одним компьютером. Тогда функция FV^{-1} показывает среднее число инфицированных узлов одним узлом с вредоносным ПО.

Результаты. В работе [6] было доказано, что функция FV^{-1} определяет пороговое базовое значение в неоднородных системах. Для исследуемой модели (1) – (3)

$$FV^{-1}=\frac{\beta S(x_i^*)}{\mu+\gamma},\ i=1,2.$$

Если система состоит из одной локальной сети, то пороговое значение будет определяться выражением

$$R_0=\frac{S^*\beta}{\mu+\gamma}. \qquad (5)$$

Используя определения устойчивости и проведя анализ траектории системы (1) – (3) на фазовой плоскости, можно доказать следующую теорему.

Теорема. Если основное пороговое число $R_0\le 1$, то в пределе при $t\to\infty$ все компьютеры переходят в класс невосприимчивых к вирусу. Если $R_0 > 1$, то в сети всегда присутствует «самоподдерживающиеся» вредоносное ПО.

Результат данной теоремы – с помощью числа R_0 можно определить удастся ли полностью подавить вирусную атаку на компьютерную сеть.

Для иллюстрации теоремы проведем численные эксперименты. Рассмотрим первый случай – безвирусного положения равновесия x_1^*. Пусть *S** = 50, тогда *R** = 35. Параметры модели определим таким образом, чтобы базовое пороговое число R_0 было меньше одного. На Рисунке 2

представлены результаты моделирования: фазовый портрет на плоскости (*S, I*) и графики численности компьютеров в различных классах. Как можно заметить все фазовые кривые сходятся в стационарную точку x_1^*.

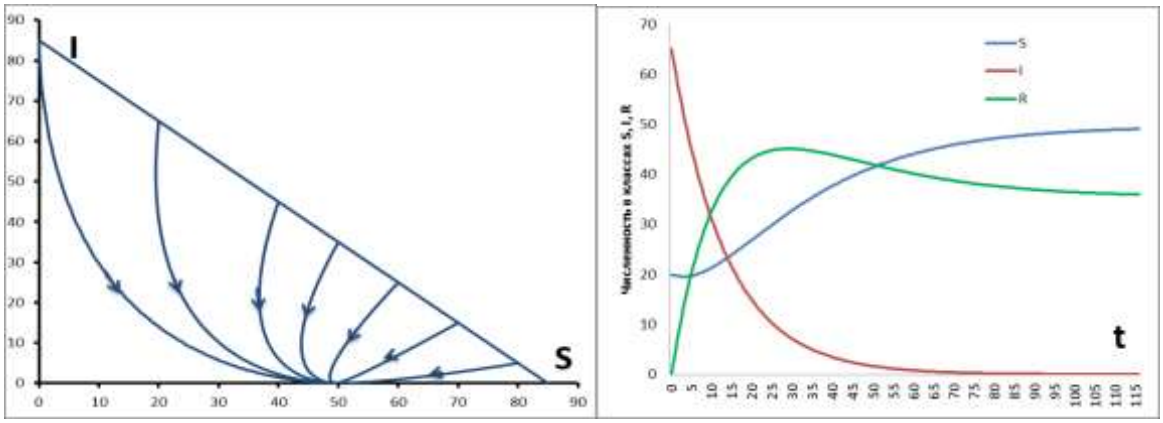

Рисунок 2 – Фазовый портрет и эволюция системы (1) – (4)
для безвирусного положения равновесия $x_1^* = (50, 0, 35)$, R_0 <1.

Увеличив коэффициент, характеризующий темп распространения вредоносного кода в сети β, и сохранив значения всех остальных параметров модели, получим новое базовое пороговое число R_0 >1. В этом случае нарушается устойчивость стационарной точки x_1^*=(50,0,35). Фазовый портрет и траектории динамики функций, характеризующие количество компьютеров разных типов, представлены на Рисунке 3.

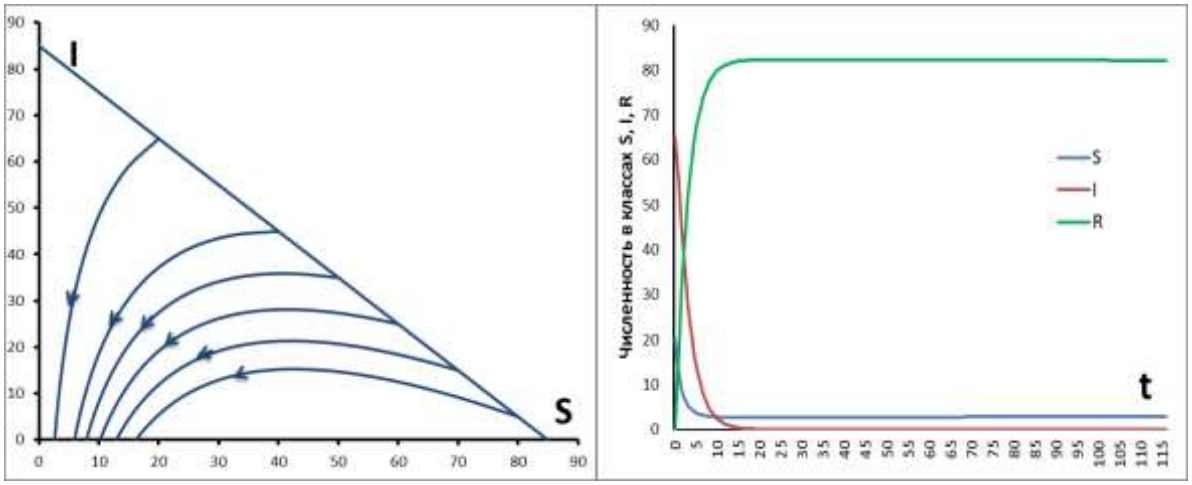

Рисунок 3 – Фазовый портрет и эволюция системы (1) – (4)
при базовом пороговом числе R_0 >1.

Рассмотрим второй случай – эндемического положения равновесия x_2^*, то есть равновесия, при котором компьютерный вирус постоянно находится в сети, «самоподдерживается». Выберем коэффициенты SIRS-

модели, при которых стационарная точка x_2^*=(40, 10, 119) отвечает этому случаю. Тогда по формуле (5) $R_0 > 1$.

На Рисунке 4 представлены фазовый портрет и частный случай эволюции системы (1) – (4) эндемического положения равновесия. Как можно заметить из графиков фазовых кривых, положение равновесия устойчиво. Графики динамики системы так же отображают типичную зависимость. Число инфицированных компьютеров I сначала растет, достигнув максимального значения, затем уменьшается.

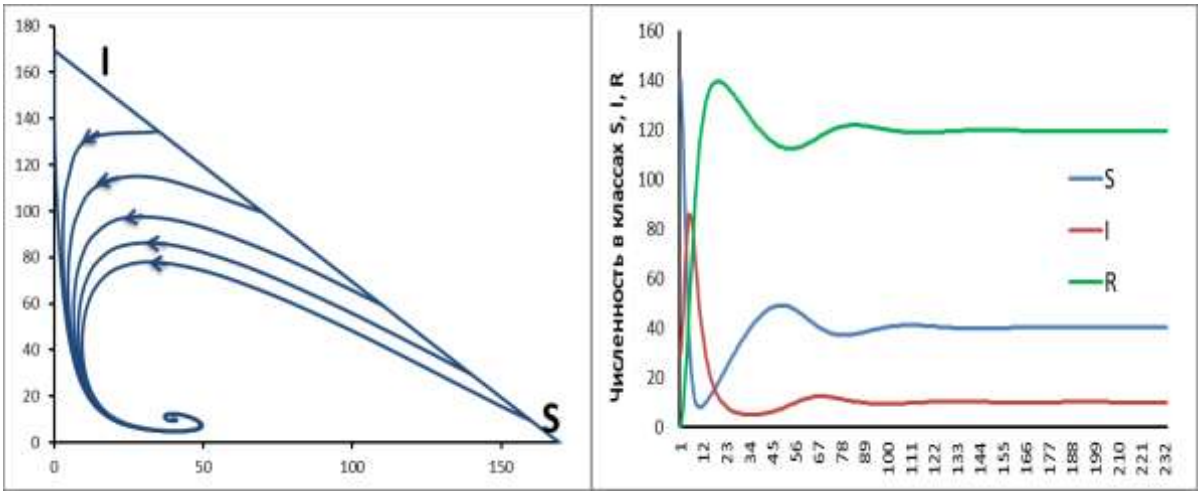

Рисунок 4 – Фазовый портрет и эволюция системы (1) – (4)
для эндемического положения равновесия x_2^*=(40, 10, 119), R_0 >1.

Ниже на Рисунке 5 рассмотрен пример динамики системы (1) – (4) для эндемического положения равновесия x_2^*=(667, 10, 431) при базовом пороговом числе R_0 = 1.

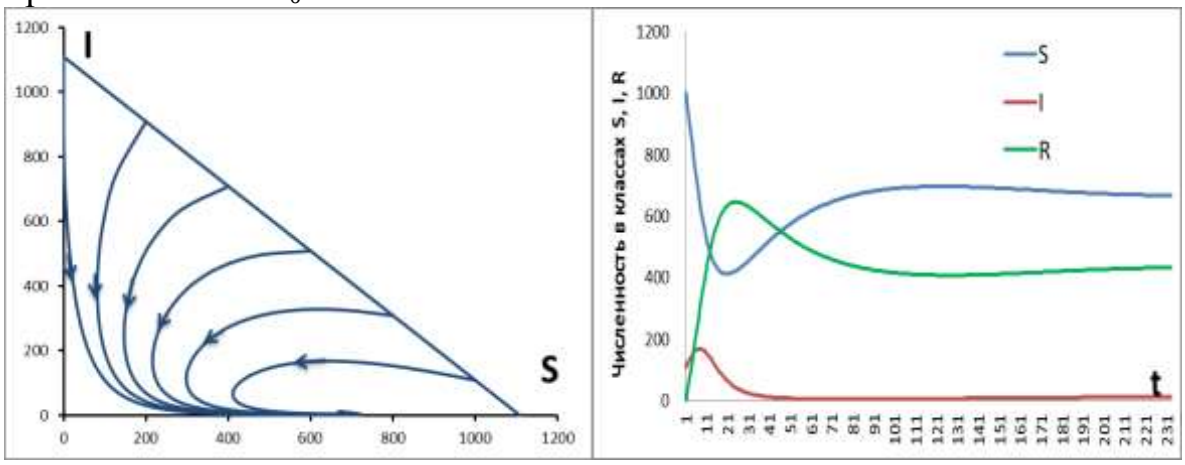

Рисунок 5 – Фазовый портрет и эволюция системы (1) – (4).

В данном примере получены типичные зависимости SIRS – модели и отображают реальную динамику эпидемии.

Обсуждение. Устранения последствий вирусной атаки происходит в несколько этапов, требуют достаточное количество времени и много ручного труда технического персонала. Поэтому своевременное использование противовирусных мер может предотвратить заражение операционной системы, сохранить важные данные и документы, а в результате сохранить деньги и время.

В практическом плане основное пороговое число R_0 можно использовать для прогнозирования и планирования мероприятий по защите информации. Зная оценку основного порогового значения, можно определить какую часть узлов следует «вакцинировать», чтобы R_0 стало меньше 1, тем самым предотвратить возможную эпидемию.

Слагаемое uS в уравнении (1) характеризует количество протестированных компьютеров, на которые установили обновленную антивирусную базу, т. е. эти компьютеры перешли в класс невосприимчивых к вирусам. Формула (5) перепишется в следующем виде

$$\frac{\beta(S^* - uS)}{\mu + \gamma} < 1.$$

Выполнив преобразования получим

$$u > \frac{R_0 - 1}{R_0}. \qquad (6)$$

Таким образом, для исключения последствий вирусной атаки и уменьшению затрат на покупку и установку антивирусного ПО, достаточно обеспечить защитой только часть компьютеров uS, где u вычисляется по формуле (6).

Заключение. В зависимости от величины базового порогового числа (или порогового значения) можно сделать вывод о возможности предотвращения эпидемии. Если базовое пороговое число R_0, меньше или равно единице, то со временем в пределе $t \to \infty$ распространение вируса затухает, и все компьютеры становятся невосприимчивыми к вредоносному коду. Если R_0 больше единицы, то вирусная атака в компьютерной сети приведет к резкому увеличению зараженных узлов и наличие вирусов будет постоянно. Зная оценки основного порогового числа R_0, можно вычислить наилучший параметр u, характеризующий противовирусную защиту сети, для уменьшения последствий атаки вредоносным ПО.

ЛИТЕРАТУРА

1. Доктрина информационной безопасности Российской Федерации, Москва, 2016 г., (утверждена Президентом Российской Федерации В. Путиным 5 декабря 2016 г., № 646. URL: http://www.consultant.ru/document/cons_doc_LAW_208191/4dbff9722e14f63a309bce4c2ad3d12cc2e85f10/).

2. Бородакий Ю. В., Добродеев А. Ю., Нащекин П. А., Бутусов И. В. О подходах к реализации централизованной системы управления информационной безопасностью АСУ военного и специального назначения// Вопросы кибербезопасности. Москва 2014, 2 (3), С. 2 -9.
3. Эпидемиологический словарь. – Москва: Открытый Институт Здоровья, 2009.
4. Братусь А. С., Новожилов А. С., Платонов А. П. Динамические системы и модели биологии. М.: ФИЗМАТЛИТ, 2009.
5. Молчанов, А. М. Об устойчивости нелинейных систем. Пущено: ИМПБ РАН, 2013.
6. O. Diekmann, J.A.P. Heesterbeek, J.A.J. Metz, On the definition and the computation of the basic reproduction ratio R0 in models for infectious diseases in heterogeneous populations, J. Math. Biol. 28 (1990) 365. URL: https://link.springer.com/article/10.1007/BF00178324.

N. A. Semykina

PREDICTION OF THE CONSEQUENCES OF THE PROPAGATION OF THE VIRUS IN A COMPUTER NETWORK USING A BASIC REPRODUCTION NUMBER

Tver State University, Tver, Russia

Today, Internet is considered to be one of the most useful tools for people to communicate, find information and to buy goods and services. Most computers are connected to each other in some way. The Internet is the primary medium used by attackers to commit computer crimes. They share the same operating system software and communicate with all other computers using the standard set of protocols. This has spawned a new generation of criminals. The similarity between the spread of a biological virus and worm propagation encourages researchers to adopt an epidemic model to the network environment. This approach is most effective for describing the computer viruses propagation on the network. The article uses the results of the theory of mathematical epidemiology to analyze the SIRS model. The dynamics of the virus propagation to the computer network is described using a system of differential equations. The stability of the network to the spread of malware is investigated. An equilibrium position is found. The basic reproduction number is determined. The dependence of the virus attack evolution on the basic reproduction number is analyzed. Numerical simulations are provided to support our theoretical conclusions.

Keywords: mathematical model, computer virus, virus dynamics, basic reproduction number, nonlinear system of differential equations, stability of the system

REFERENCES

1. Doktrina informacionnoj bezopasnosti Rossijskoj Federacii, Moskva, 2016. URL:http://www.consultant.ru/document/cons_doc_LAW_208191/4dbff9722e14f63a309bce4c2ad3d12cc2e85f10/).
2. Borodakij YU. V., Dobrodeev A. YU., Nashchekin P. A., Butusov I. V. O podhodah k realizacii centralizovannoj sistemy upravleniya informacionnoj

bezopasnost'yu ASU voennogo i special'nogo naznacheniya// Voprosy kiberbezopasnosti. Moskva 2014, 2 (3), C. 2 -9.
3. Epidemiologicheskij slovar'. – Moskva: Otkrytyj Institut Zdorov'ya, 2009.
4. Bratus' A. S., Novozhilov A. S., Platonov A. P. Dinamicheskie sistemy i modeli biologii. Moskva: FIZMATLIT, 2009.
5. Molchanov A. M. Ob ustojchivosti nelinejnyh sistem (On Stability of Nonlinear Systems) Pushchino : Institute of Mathematical Problems of Biology, Russian Academy of Sciences, 2013.
6. O. Diekmann, J.A.P. Heesterbeek, J.A.J. Metz, On the definition and the computation of the basic reproduction ratio R0 in models for infectious diseases in heterogeneous populations, J. Math. Biol. 28 (1990) 365. URL: https://link.springer.com/article/10.1007/BF00178324.