21. *Varajão J., Lourenço J.C., Gomes J.* Models and methods for information systems project success evaluation, *A review and directions for research*, 2022, 8 (12), e11977.
22. *Bozhenyuk A., Belyakov S., Knyazeva M., Rozenberg I.* Searching Method of Fuzzy Internal Stable Set as Fuzzy Temporal Graph Invariant, *Communications in Computer and Information Science*, 2018, 583, pp. 501-510.

Розенберг Игорь Наумович – Российский университет транспорта; e-mail: avb@itt.net.ru, yaroshinna@gmail.com; г. Москва, Россия; тел.: +79166652310; д.т.н.; зав. кафедрой «Геодезия, геоинформатика и навигация».

Дубчак Ирина Александровна – Российский университет транспорта; e-mail: iri-dubchak@yandex.ru; г. Москва, Россия; тел.: +79166652310; заместитель директора.

Rozenberg Igor Naumovich – Russian University of Transport; e-mail: avb@itt.net.ru, yaroshinna@gmail.com; Moscow, Russia; phone: +79166652310; dr. of eng. sc.; head of the Department of Geodesy, Geoinformatics and Navigation.

Dubchak Irina Alexandrovna – Russian University of Transport; e-mail: iri-dubchak@yandex.ru; Moscow, Russia; phone: +79166652310; deputy director.

УДК 004.056 DOI 10.18522/2311-3103-2025-6-145-157

Е.В. Карачанская, О.В. Рыбкина

ПОСТРОЕНИЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ ЗАЩИЩЕННОЙ ОТ ЗАРАЖЕНИЯ ВИРУСАМИ ИНФОРМАЦИОННОЙ СИСТЕМЫ НА ОСНОВЕ SIR-МОДЕЛИ

Представлен анализ детерминированных моделей распространения эпидемии компьютерных вирусов (SIR-модели) и их классификация. Выделены основные направления исследований данных моделей. Приведен анализ существующих стохастических моделей на основе SIR-модели и их разнообразие. Предлагается метод построения стохастической SIR-модели на основе классической SIR-модели в виде системы стохастических дифференциальных уравнений Ито с винеровским процессом. Особенностью предложенного метода является сохранение инвариантов, один из которых присутствует в классической модели, а второй связан с постановкой задачи информационной безопасности. Показана возможность построения стохастической и детерминированной модели информационной системы, защищенной с вероятностью 1 от заражения компьютерными вирусами: стохастическая, инфицирование которой вирусами происходит непрерывно, и детерминированная, в которой вирус находится в информационной системе. Математическая стохастическая модель информационной системы, защищенной от эпидемии компьютерных вирусов, строится как система стохастических дифференциальных уравнений, первыми интегралами которой являются инварианты, сохраняющиеся с вероятностью 1. В качестве показателя защищенности системы рассматривается некоторое функциональное соотношение между переменными модели, сохраняющие постоянное значение. Внесение в модель компенсатора (программное управлением с вероятностью 1 (PCP1)), позволяет сохранять с вероятностью 1 заданный показатель защищенности, описанный с помощью переменных модели. Аналогичным образом, на основе предложенного алгоритма, строится детерминированная модель информационной системы, защищенной от заражения компьютерными вирусами. В построенную модель вводится управление, подобное программному управлению с вероятностью 1, которое позволит сохранять значение инвариантов. Особенность предлагаемых моделей состоит в том, что в модели сохраняются инварианты, связанные со свойствами, которые обеспечивают защищенность информационной системы. Исследование поведения построенных моделей проводится с использованием численного моделирования в среде MathCad. По результатам исследований сделаны выводы о возможности применения предложенного метода при построении стохастических моделей на основе других моделей распространения эпидемии, а также для моделей защиты информационной системы от распространения эпидемии компьютерных вирусов.

SIR-модель; информационная безопасность; модель защищенной информационной системы; сохранение свойств.

E.V. Karachanskaya, O.V. Rybkina

CONSTRUCTING A MATHEMATICAL MODEL OF A VIRUS-PROTECTED INFORMATION SYSTEM BASED ON SIR-MODEL

This article presents an analysis of deterministic models of computer virus epidemic propagation (SIR models) and their classification. The main areas of research into these models are highlighted. An analysis of existing stochastic models based on the SIR model and their diversity are presented. A method for constructing a stochastic SIR model based on the classical SIR model, represented by a system of Ito stochastic differential equations with a Wiener process, is proposed. The possibility of constructing a stochastic and deterministic model of an information system protected against computer virus infection with probability 1 is demonstrated: a stochastic model, in which infection by viruses occurs continuously, and a deterministic model, in which the virus is present in the information system. A mathematical stochastic model of an information system protected from computer virus outbreaks is constructed as a system of stochastic differential equations whose first integrals are invariants preserved with probability 1. A certain functional relationship between model variables, maintaining a constant value, is considered as the system's security indicator. Introducing a compensator (program control with probability 1 (PCP1)) into the model allows the specified security indicator, described by the model variables, to be maintained with probability 1. Introducing a compensator (program control with probability 1 (PCP1)) into the model allows the specified security indicator, described by the model variables, to be maintained with probability 1. Similarly, based on the proposed algorithm, a deterministic model of an information system protected from computer virus infection is constructed. A control similar to programmed control with probability 1 (PCP1) is introduced into the constructed model, which allows the invariants to be maintained. A distinctive feature of the proposed models is that they preserve invariants associated with the properties that ensure the security of the information system. The behavior of the constructed models is studied using numerical simulation in the MathCad environment. Based on the research results, conclusions were drawn on the possibility of using the proposed method in constructing stochastic models based on other models of epidemic spread, as well as for models of protecting an information system from the spread of a computer virus epidemic.

SIR model; information security; model of protected information system; properties preservation.

Введение. Наиболее важным фактором, влияющим на работоспособность и эффективность информационных систем в различных производственных отраслях, является их текущий уровень защищенности от различного вида угроз. Наибольший урон наносят компьютерные вирусы, которые попадая в информационную систему вызывают эпидемии, распространение которых носит случайный характер. Особенно остро этот вопрос возникает на критически важных объектах, где незамедлительное реагирование на распространение эпидемии позволило бы избежать серьезных последствий.

Анализ литературы [1–18] показывает, что для моделирования эпидемии компьютерных вирусов чаще всего используется биологическая модель распространения вирусов, так называемая SIR-модель, предложенная в 1927 г. У. Кермаком и А. МакКендриком [1]. Это связано с тем, что динамика распространения компьютерных вирусов очень схожа с динамикой распространения биологических вирусов. С точки зрения классической эпидемиологической модели распространения эпидемии предполагается, что каждый живой организм может находиться в одном из нескольких состояний и с течением времени это состояние изменяется [1, 2]. Количество таких состояний зависит от вида рассматриваемой модели.

В моделях распространения эпидемий компьютерных вирусов в качестве основных объектов рассматриваются элементы информационной системы и их текущее состояние [3–5].

Объекты информационной системы могут находиться в следующих состояниях (в зависимости от выбранной модели):

- не зараженные объекты или уязвимые;
- зараженные (инфицированные);
- вылеченные или обладающие иммунитетом;
- зараженные, но находящиеся в латентной стадии (т.е. в течении определенного периода времени не заражают другие объекты);

- помещенные на карантин;
- найденные зараженные.

На сегодняшний день существуют следующие виды математических моделей распространения компьютерных вирусов, разработанных на основе биологического подхода [3–5]:

- SI – Suspected (уязвимый)-Infected (зараженный),
- SIR – Suspected (уязвимый)-Infected (зараженный)-Recovered (вылеченный),
- SEIQR – Suspected (уязвимый)-Exposed (латентные)-Infected (зараженный)-Quarantined (карантин)-Recovered (вылеченный),
- PSIDR – Progressive Suspected (уязвимый)-Infected (зараженный)-Detected (найденные зараженные)-Recovered (вылеченный) – в данной модели поведение системы разбивается на два этапа.

Анализ литературы [5–18] показывает, что на основе SIR-модели и ее разновидностей построены различные детерминированные и стохастические модели распространения эпидемий. Выделим основные направления, в которых проводились исследования.

Авторы работы [6] рассматривают сравнительную характеристику существующих разновидностей SIR-модели и приводят их усовершенствованные версии применимые при распространении эпидемий компьютерных вирусов. В работе [7] рассматривается обобщенная модель распространения сетевых червей, с подробным рассмотрением этапов развития эпидемии и возможные решения проблемы на каждом из этапов. Рассмотрение SIR-модели с точки зрения имитационного моделирования предлагается в работе коллектива авторов [5]. По словам авторов это позволит управлять эпидемией, прогнозировать ее течение, подбирать методы противодействия. Автор работы [8] приводит сравнение результатов численного моделирования с экспериментальными данным для четырех моделей, описывающих распространение вируса в сети при отсутствии возможности лечения зараженных хостов. На основе полученных моделей автором была создана модель, учитывающая возможность лечения зараженных хостов, а также проведен численный эксперимент, позволяющий проследить динамику численности всех групп, участвующих в эпидемиологическом процессе.

Стохастические модели на основе SIR рассматриваются в работах российских [9–10] и зарубежных авторов [11]. В [9] представлена комплексная модель динамики развития эпидемий вирусов в компьютерных сетях, созданная на основе учета их топологических свойств и механизмов распространения вирусов и основанная на методах теории перколяции. Автор рассматривает динамические процессы стохастического распространения в компьютерных сетях эволюционирующих вирусов при устаревании и запаздывании действия антивирусов.

Можно отметить ряд моделей, в которых учитываются случайные составляющие: модель с неопределенностью данных в начальный момент времени [11], эпидемические модели со случайным инфекционным периодом [12], модель, учитывающая случайное влияние среды на модель [13], модель с возмущениями, накладываемыми на параметры, входящие в модель [14].

Ряд авторов рассматривали стохастические модели эпидемии основываясь на марковских и полумарковских случайных средах [15–17]. В этих моделях в коэффициенты вносилась случайность, связанная с дискретным марковским процессом. Стохастические модели, основанные на теории систем СДУ, исследованы в [10, 18]. Сохранение численности популяции в работе [10] обеспечивается специфическим видом стохастической части и несколькими параметрами, в работе [18] – сохранение численности рассматривается как оптимизационная задача.

Несмотря на разнообразие представленных стохастических моделей, применение SIR-модели со случайными составляющими, чаще всего рассматривается на примерах биологических моделей. В области информационной безопасности таких исследований достаточно мало, что подтверждает актуальность выбранного исследования.

Реагирование на угрозу заражения математически можно сопоставить с введением некоторого компенсатора – функции управления, зависящей от состояния информационной системы в каждый момент времени. Как известно, управление производится с какой-либо целью. В качестве такой цели можно рассматривать сохранение наиболее существенных свойств, позволяющих информационной системе находиться в работающем состоянии.

Для дальнейших исследований возьмем за основу SIR-модель. Предлагаемый метод можно использовать и для построения стохастических моделей на основе моделей SEIQR и PSIDR. Использование только трех групп объектов информационной системы (на основе SIR) дает возможность использовать только 3 уравнения и избежать громоздкости при описании метода построения стохастической модели, а для построения моделей на основе других моделей требует большее число уравнений в системе, описывающей модель.

Постановка задачи. В структуре SIR-модели объекты информационной системы находятся в момент времени t образуют три группы, мигрируя между ними: зараженные $I(t)$, не зараженные $S(t)$, вылеченные объекты, обладающие иммунитетом $R(t)$.

Для данной модели предполагается, что общая численность объектов информационной системы – величина постоянная:

$$S(t) + I(t) + R(t) = 1,$$

где S(t) – доля уязвимых объектов; I(t) – доля зараженных объектов; R(t) – доля невосприимчивых или вылеченных объектов, обладающих иммунитетом.

Пусть в начальный момент времени t=0 эти показатели таковы:

$$\mathrm{S}(0) = \mathrm{S}_0,\ \ \mathrm{I}(0) = \mathrm{I}_0,\ \ \mathrm{R}(0) = \mathrm{R}_0. \tag{1}$$

SIR-модель может быть описана с помощью системы дифференциальных уравнений

$$\begin{cases} dS(t) = -\beta I(t)S(t)dt, \\ dI(t) = \big(\beta I(t)S(t) - \delta I(t)\big)dt, \\ dR(t) = \delta I(t)dt, \end{cases} \tag{2}$$

с начальными условиями (1), β – параметр интенсивности заражения, δ – параметр интенсивности выздоровления (скорость «иммунизации»).

Внесем в модель (2) случайность, определяющую внешние воздействия, используя переход к системе стохастических дифференциальных уравнений (СДУ) Ито. При этом необходимо построить такую математическую модель ИС, которая была бы способна оставаться в защищенном состоянии, не допускающем распространения эпидемии компьютерных вирусов. Таким образом, будем строить математическую стохастическую модель информационной системы, защищенной от эпидемии компьютерных вирусов.

Стохастическая модель информационной системы, построенная на основе SIR-модели. Для проведения исследований требуется построить математическую стохастическую модель информационной системы, защищенной от заражения компьютерными вирусами, способную оставаться нечувствительной к внешнему воздействию. В качестве показателя защищенности системы будем рассматривать некоторое функциональное соотношение между переменными модели, сохраняющее постоянное значение.

Положим, что эпидемия объектов информационной системы может быть вызвана случайными внешними воздействиями, которые описываются с помощью случайного (винеровского) процесса $w(t)$ с некоторыми функциональными коэффициентами, зависящими, например, от времени или текущего состояния ИС.

В СДУ Ито случайность описывается винеровским процессом. Напомним его определение.

Винеровским процессом $w(t)$ называется случайный процесс, обладающий свойствами:

1) $w(0) = 0$;
2) математическое ожидание в любой момент времени равно нулю: $M[w(t)] = 0$;
3) приращения $\Delta w(t,s) = w(t) - w(s),\ t > s$ – независимые случайные величины, распределение по нормальному закону $\mathcal{N}\ (0, |t - s|)$.

Тогда стохастическая модель информационной системы, подверженной атаке, построенная с использованием (2), будет определяться следующей системой СДУ Ито

$$\begin{cases} dS(t) = -\beta I(t)S(t)dt + r_1(t)dw(t), \\ dI(t) = \big(\beta I(t)S(t) - \delta I(t)\big)dt + r_2(t)dw(t), \\ dR(t) = \delta I(t)dt + r_3(t)dw(t). \end{cases} \quad (3)$$

с начальными условиями

$$\mathrm{S}(0) = \mathrm{S}_0,\ \ \mathrm{I}(0) = \mathrm{I}_0,\ \ \mathrm{R}(0) = \mathrm{R}_0.$$

Однако в этом случае не выполняется важное свойство модели SIR, а именно, сохранение инварианта:

$$S(t) + I(t) + R(t) = 1.$$

Будем строить стохастическую модель, в которой это свойство будет обязательно сохраняться.

Построение модели стохастического трехмерного процесса с сохраняющимися инвариантами. Рассмотрим метод построения системы СДУ с начальными условиями, и имеющей заданные функции в качестве инвариантов.

Определение 1. [19]. Пусть $\mathbf{x}(t)$ – n-мерный (n>1) случайный процесс, удовлетворяющий системе СДУ Ито

$$dx_i(t) = a_i\big(t, \mathbf{x}(t)\big)dt + \sum_{k=1}^{m} b_{ik}\big(t, \mathbf{x}(t)\big)dw_k(t),\ \ i = 1,2,\dots n;\ \mathbf{x}(0) = \mathrm{x}_0, \quad (4)$$

коэффициенты которого удовлетворяют условиям существования и единственности решения [20], и $\mathbf{x}(t, \mathrm{x}_0)$ – его решение, удовлетворяющее заданному начальному условию. Неслучайная функция, непрерывно дифференцируемая по t и дважды непрерывно дифференцируемая по $\mathbf{x}$ ($u(t, \mathbf{x}) \in C_{t,x}^{1,2}$) называется первым интегралом системы СДУ, если она с вероятностью 1 на любой из траекторий решения системы (4) принимает постоянное значение, зависящее только от x_0: $u\big(t, \mathbf{x}(t, \mathrm{x}_0)\big) = u(0, \mathrm{x}_0)$.

Согласно [19], количество линейно-независимых первых интегралов для системы (4) не превышает *(n-1)*.

Не вдаваясь глубоко в теорию стохастических дифференциальных уравнений с инвариантами [21], покажем практическое ее применение на примере построения системы из трех СДУ, имеющей заданный набор первых интегралов, которые далее будем называть инвариантами.

Пусть система СДУ должна иметь функции $u(t, \mathbf{x}), v(t, \mathbf{x})$ в качестве первых интегралов: $u\big(t, \mathbf{x}(t, \mathrm{x}_0)\big) = u(0, \mathrm{x}_0)$ и $v\big(t, \mathbf{x}(t, \mathrm{x}_0)\big) = v(0, \mathrm{x}_0)$, где $\mathrm{x}_0 = \mathbf{x}(0)$ – начальные условия.

Будем строить систему СДУ в матричном виде [21]:

$$d\mathbf{x}(t) = A_0(t, \mathbf{x}(t)) \cdot dt + B(t, \mathbf{x}(t))dw(t). \quad (5)$$

Определим коэффициенты-матрицы системы (5).

Пусть $\overrightarrow{e_0}, \overrightarrow{e_1}, \overrightarrow{e_2}, \overrightarrow{e_3}$ ортонормированный базис расширенного фазового пространства $[0, \mathrm{T}) \times R^3$, в котором описывается динамика информационной системы.

1. Сначала строим матрицу $B(t, \mathbf{x}(t))$. Для этого рассмотрим матрицу

$$D_1(t, \mathbf{x}) = \begin{pmatrix} \overrightarrow{e_1} & \overrightarrow{e_2} & \overrightarrow{e_3} \\ \frac{\partial u(t,\mathbf{x})}{\partial x_1} & \frac{\partial u(t,\mathbf{x})}{\partial x_2} & \frac{\partial u(t,\mathbf{x})}{\partial x_3} \\ \frac{\partial v(t,\mathbf{x})}{\partial x_1} & \frac{\partial v(t,\mathbf{x})}{\partial x_2} & \frac{\partial v(t,\mathbf{x})}{\partial x_3} \end{pmatrix} \quad (6)$$

и вычислим миноры $d_i(t, \mathbf{x})$, соответствующие элементам $\overrightarrow{e_i}\ (i = 0,1,2,3)$ матрицы (6), которые образуют вспомогательную матрицу столбец

$$D(t, \mathbf{x}) = (d_1(t, \mathbf{x}), d_2(t, \mathbf{x}), d_3(t, \mathbf{x}))^T. \quad (7)$$

Коэффициент $B(t, \mathbf{x})$ – множитель в стохастической части определяется по формуле:

$$B(t, \mathbf{x}(t)) = q(t, \mathbf{x}(t)) \cdot D(t, \mathbf{x}(t)) = \big(b_1(t, \mathbf{x}(t)), b_2(t, \mathbf{x}(t)), b_3(t, \mathbf{x}(t))\big)^T, \quad (8)$$

где $q(t, \mathbf{x})$ – некоторая произвольная функция.

2. Определяем коэффициент $A_0(t,\mathbf{x}(t))$. Рассмотрим матрицу

$$L(t,\mathbf{x})=\begin{pmatrix} \overrightarrow{e_0} & \overrightarrow{e_1} & \overrightarrow{e_2} & \overrightarrow{e_3} \\ \frac{\partial u(t,\mathbf{x})}{\partial t} & \frac{\partial u(t,\mathbf{x})}{\partial x_1} & \frac{\partial u(t,\mathbf{x})}{\partial x_2} & \frac{\partial u(t,\mathbf{x})}{\partial x_3} \\ \frac{\partial v(t,\mathbf{x})}{\partial t} & \frac{\partial v(t,\mathbf{x})}{\partial x_1} & \frac{\partial v(t,\mathbf{x})}{\partial x_2} & \frac{\partial v(t,\mathbf{x})}{\partial x_3} \\ \frac{\partial h(t,\mathbf{x})}{\partial t} & \frac{\partial h(t,\mathbf{x})}{\partial x_1} & \frac{\partial h(t,\mathbf{x})}{\partial x_2} & \frac{\partial h(t,\mathbf{x})}{\partial x_3} \end{pmatrix}, \quad (9)$$

в которой $u(t,\mathbf{x}), v(t,\mathbf{x})$ – первые интегралы, $h(t,\mathbf{x})$ – произвольная дифференцируемая функция, независимая с функциями $u(t,\mathbf{x})$ и $v(t,\mathbf{x})$. Вычислим $M_i(t,\mathbf{x})$ – миноры, соответствующие элементам $\overrightarrow{e_i}\,(i=0,1,2,3)$ матрицы (9). Последовательно проводим следующие вычисления

$$C_i(t,\mathbf{x})=(-1)^i\cdot M_i(t,\mathbf{x}),\quad (i=0,1,2,3),\qquad A_i(t,\mathbf{x})=\frac{C_i(t,\mathbf{x})}{C_0(t,\mathbf{x})},\qquad (i=1,2,3),$$

на основании которых строим вектор-столбец:

$$A(t,\mathbf{x}(t))=(A_1(t,\mathbf{x}(t)),A_2,(t,\mathbf{x}(t))\,A_3(t,\mathbf{x}(t)))^T. \quad (10)$$

Строим еще один вспомогательный вектор-столбец по формуле $H(t,\mathbf{x})=\left[\frac{\partial b_i(t,\mathbf{x})}{\partial x_j}\right]\cdot B(t,\mathbf{x})$, где $\left[\frac{\partial b_i(t,\mathbf{x})}{\partial x_j}\right]$ – матрица, столбцы которой – частные производные компонент вектора (8) по переменным x_1,x_2,x_3.

Коэффициент $A_0(t,\mathbf{x})$ системы (5), для которой функции $u(t,\mathbf{x})$, $v(t,\mathbf{x})$ являются первыми интегралами, определяется по формуле:

$$A_0(t,\mathbf{x}(t))=A(t,\mathbf{x}(t))+\frac{1}{2}H(t,\mathbf{x}(t)). \quad (11)$$

Система СДУ с начальными условиями $\mathbf{x}(0)=\mathrm{x}_0$ и инвариантами $u\big(t,\mathbf{x}(t,\mathrm{x}_0)\big)=u(0,\mathrm{x}_0)$, $v\big(t,\mathbf{x}(t,\mathrm{x}_0)\big)=v(0,\mathrm{x}_0)$ построена.

Стохастическая модель информационной системы, защищенной от заражения компьютерными вирусами с вероятностью 1. Случайность вносит сильный вклад с поведение модели. Однако можно внести в систему (3) компенсатор (управление), который позволит сохранять с вероятностью 1 заданный показатель защищенности [21], описанный с помощью переменных модели. Поскольку этот показатель должен сохранять постоянное значение (быть инвариантом), то его можно рассматривать как первый интеграл системы СДУ [19].

Определение 2 [21, 22]. Программным управлением с вероятностью 1 (РСР1) будем называть такое управление в стохастической системе, которое с вероятностью, равной 1, сохраняет заданный инвариант, обеспечивая нечувствительность системы к случайным возмущениям.

Нечувствительность к внешнему воздействию будем сопоставлять с некоторыми инвариантами – функциями $u\big(t,S(t),I(t),R(t)\big)$ и $v\big(t,S(t),I(t),R(t)\big)$, аргументами которых являются фазовые координаты и время, и сохраняющие постоянное значение в любой момент времени *t*.

Пусть модель (3) можно записать в матричном виде

$$d\boldsymbol{x}(t)=K(t,\boldsymbol{x}(t))\cdot dt+r(t,\boldsymbol{x}(t))dw(t)\,,\quad \mathbf{x}(0)=\mathrm{x}_0, \quad (12)$$

Для модели (12) обязательным условием является сохранение инварианта $u(t,\mathbf{x}(t))=u(0,\mathrm{x}_0)=x_1\,(t)+\,x_2(t)+x_3(t)-1=0$. Если положить, что еще необходимо сохранение некоторого инварианта $v(t,\mathbf{x}(t))=v(0,\mathrm{x}_0)$, то можно построить систему СДУ

$$d\mathbf{x}(t)=A_0(t,\mathbf{x}(t))\cdot dt+B(t,\mathbf{x}(t))dw(t)$$

с коэффициентами $A_0(t,\mathbf{x}(t))$ и $B(t,\mathbf{x}(t))$, определяемыми по формулам (8) и (11), а затем, используя равенства

$$A_0(t,\mathbf{x}(t))=K(t,\mathbf{x}(t))+U_1(t,\mathbf{x}(t)),\qquad B(t,\mathbf{x}(t))=r(t,\mathbf{x}(t))+U_2(t,\mathbf{x}(t)),$$

определить компенсаторы – функции управления $U_1(t,\mathbf{x}(t))$ и $U_2(t,\mathbf{x}(t))$. Если функции $r(t,\mathbf{x})$ первоначально неизвестны, то полагаем, что $B(t,\mathbf{x}(t))=r(t,\mathbf{x}(t))$.

Положим: $\hat{y}(t) := U_1\big(t, S(t), I(t), R(t)\big)$, $\hat{z}(t) := U_2\big(t, S(t), I(t), R(t)\big)$, $r(t) := r\big(t, S(t), I(t), R(t)\big)$. Тогда стохастическая модель защищенной от эпидемии вирусов информационной системы имеет вид:

$$\boldsymbol{d}\begin{pmatrix} S(t) \\ I(t) \\ R(t) \end{pmatrix} = \left[\begin{pmatrix} -\beta I(t)S(t) \\ \beta I(t)S(t) - \delta I(t) \\ \delta I(t) \end{pmatrix} + \begin{pmatrix} \hat{y}_1(t) \\ \hat{y}_2(t) \\ \hat{y}_3(t) \end{pmatrix}\right] dt + \left[\begin{pmatrix} r_1(t) \\ r_2(t) \\ r_3(t) \end{pmatrix} + \begin{pmatrix} \hat{z}_1(t) \\ \hat{z}_2(t) \\ \hat{z}_3(t) \end{pmatrix}\right] dw(t) \quad (13)$$

с начальными условиями

$$\mathrm{S}(0) = \mathrm{S}_0,\ \ \mathrm{I}(0) = \mathrm{I}_0,\ \ \mathrm{R}(0) = \mathrm{R}_0,$$

в которой с вероятностью 1 сохраняются свойства:

$$u\big(t, S(t), I(t), R(t)\big) = S(t) + I(t) + R(t) - 1 \quad (14)$$

и

$$v(t, \mathbf{x}(t)) = v(0, \mathrm{x}_0) = Const \quad (15)$$

Таким образом, в модели (13) – (15), в отличие от модели (3), обязательно сохраняется инвариант (14) и какое-либо дополнительное свойство (15).

Пусть в модели (13) вектор коэффициентов $r(t, \mathbf{x})$ неизвестен. Рассмотрим пример построения стохастической модели SIR для защищенной ИС, в которой, кроме обязательного инварианта (14) будет еще сохраняться значение функции

$$v\big(t, S(t), I(t), R(t)\big) = S(t). \quad (16)$$

Так как для модели (13) располагаем определенным количеством объектов, то условие (14) является естественным ограничением при построении модели. Условие (16) позволит сохранить неизменность доли уязвимых объектов и не допустить их заражения, тем самым ликвидировать распространение эпидемии.

В начальный момент времени t_0 функции (14) и (16) принимают постоянное значение:

$$u\big(t_0, S(t_0), I(t_0), R(t_0)\big) = S(t) + I(t) + R(t) - 1 = C_1 = 0 \quad (17)$$

и

$$v\big(t, S(t), I(t), R(t)\big) = S(t) = C_2. \quad (18)$$

В качестве дополнительной возьмем, например, функцию $h\big(t, S(t), I(t), R(t)\big) = I(t) + e^t$, и, в качестве произвольной, функцию $\mathrm{q}(t, S(t), I(t), R(t)) = S(t)$.

Для сохранения необходимых инвариантов $u\big(t, S(t), I(t), R(t)\big)$ и $v\big(t, S(t), I(t), R(t)\big)$ введем в систему уравнений функцию-компенсатор РСР1:

$$\hat{y}(t) := \hat{y}\big(t, S(t), I(t), R(t)\big).$$

Тогда система (13) примет вид:

$$\begin{cases} dS(t) = (-\beta I(t)S(t) + \hat{y}_1(t))dt + r_1(t)dw(t), \\ dI(t) = \big(\beta I(t)S(t) - \delta I(t) + \hat{y}_2(t)\big)dt + r_2(t)dw(t), \\ dR(t) = (\delta I(t) + \hat{y}_3(t))dt + r_3(t)dw(t). \end{cases} \quad (19)$$

Следуя изложенному выше алгоритму, на основе первых интегралов можно построить систему СДУ с винеровскими возмущениями и РСР1 на основе модели эпидемии компьютерных вирусов, для которой функций (14) и (16) будут первыми интегралами (инвариантами), сохраняющие равенства (17) и (18).

Построенная система СДУ, и, соответственно, стохастическая модель защищенной ИС будет иметь вид:

$$\begin{cases} dS(t) = 0, \\ dI(t) = -e^t dt + S(t)dw(t), \\ dR(t) = e^t dt - S(t)dw(t). \end{cases} \quad (20)$$

Исходя из (19) и (20), определим функцию-компенсатор РСР1 $\hat{y}(t) := \hat{y}(t, S(t), I(t), R(t))$:

$$\begin{cases} \hat{y}_2(t) = -e^t - \beta I(t)S(t) + \delta I(t), \\ \hat{y}_3(t) = e^t - \delta I(t). \end{cases} \quad (21)$$

Таким образом, построенная система СДУ (20) представляет стохастическую модель информационной системы, защищенной от эпидемии компьютерных вирусов, в которой с вероятностью 1 сохраняются инварианты (14) и (16).

Для анализа построенной модели проведем численное моделирование решений системы СДУ (20) при различных начальных условиях (табл. 1). Будем рассматривать случаи, когда в начальный момент времени доли уязвимых объектов и зараженных одинакова, доля уязвимых значительно превышает долю зараженных и доля зараженных значительно превышает долю уязвимых.

На рис. 1 представлены результаты численного моделирования решений системы СДУ (20), где для любого из вариантов решения сохраняются значения функций $u\big(t,S(t),I(t),R(t)\big)=0$ (т. е. $LX_i=(X_i)_0+(X_i)_1+(X_i)_2-1=0$) и $v\big(t,S(t),I(t),R(t)\big)=S(t)$ (т. е. $VX_i=(X_i)_0=const$).

Таблица 1

Начальные условия для численного моделирования модели (20)

Исследуемый показатель	Обозначения на рис. 1	Начальные условия		
		Вариант 1 (рис. 1,а)	Вариант 2 (рис. 1,б)	Вариант 3 (рис. 1,в)
Доля уязвимых объектов, S_0	$(X_i)_0$	0,5	0.3	0.7
Доля зараженных объектов, I_0	$(X_i)_1$	0,5	0.7	0.3
Доля невосприимчивых или вылеченных объектов, R_0	$(X_i)_2$	0	0	0

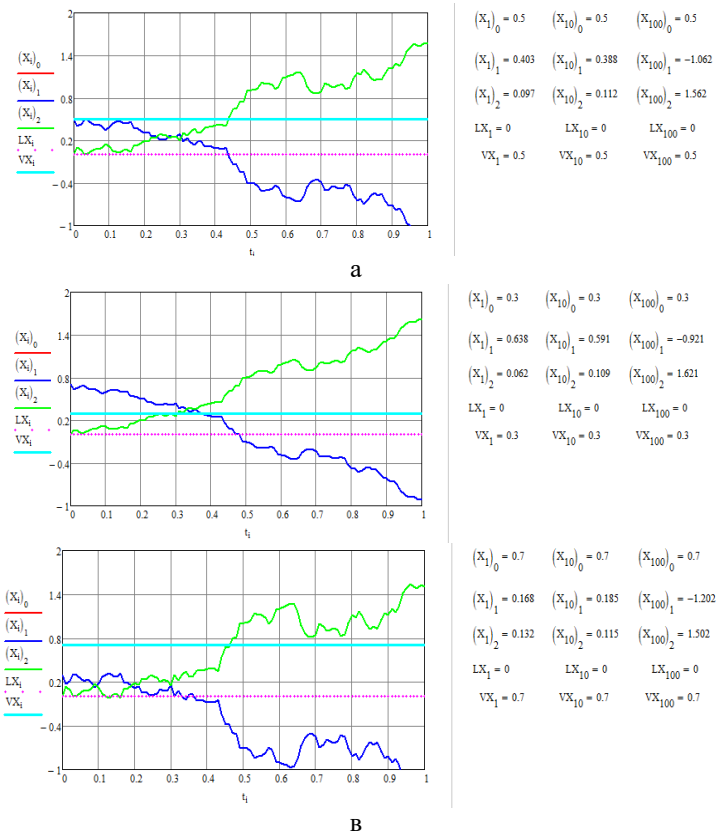

Рис. 1. Численное решение системы СДУ (20) с различными начальными условиями: а – вариант 1, б – вариант 2, в – вариант 3 (LX_i и VX_i – первые интегралы соответственно $u\big(t,S(t),I(t),R(t)\big)$ и $v\big(t,S(t),I(t),R(t)\big)$)

Анализируя результаты моделирования, представленные на рис. 1, можно сделать следующий вывод: при условии сохранения постоянного значения функций $u\big(t,S(t),I(t),R(t)\big)=0$, $v\big(t,S(t),I(t),R(t)\big)=S(t)$ и начальных значений доли зараженных компьютеров их количество практически не увеличиваются и с течением времени уменьшаются.

Таким образом, была построена стохастическая математическая модель информационной системы, защищенная от заражения компьютерными вирусами. Полученная модель позволяет не допустить распространения эпидемии компьютерных вирусов и устранить негативное воздействие на информационную систему.

Детерминированная модель защищенной информационной системы. Аналогичным образом, воспользовавшись алгоритмом, предложенным выше, можно построить детерминированную модель ИС, защищенной от заражения компьютерными вирусами.

Чтобы значения функций $u\big(t,S(t),I(t),R(t)\big)$ и $v\big(t,S(t),I(t),R(t)\big)$ оставались неизменными, в модель (2) внесем управление, подобное программному управлению с вероятностью 1 [23], которое позволит сохранять значение инвариантов: $\hat{y}(t):=\hat{y}\big(t,S(t),I(t),R(t)\big)$.

Тогда SIR-модель защищенной ИС примет вид:

$$\begin{cases} dS(t)=(-\beta I(t)S(t)+\hat{y}_1(t))dt,\\ dI(t)=(\beta I(t)S(t)-\delta I(t)+\hat{y}_2(t))dt,\\ dR(t)=(\delta I(t)+\hat{y}_3(t))dt. \end{cases} \tag{22}$$

При этом выполнены условия (17) и (18).

Для определения вектора функций управления $\hat{y}\big(t,S(t),I(t),R(t)\big)$, сохраняющего заданные инварианты, будем следовать алгоритму, предложенному выше. Отличие будет состоять только в том, что компоненты, соответствующие стохастическому слагаемому, отсутствуют, соответственно, отсутствует и их влияние на коэффициент при dt. Т.е. будем строить такую систему ДУ в матричном виде:

Соответствующая модель защищенной ИС в матричной форме имеет вид:

$$d\mathbf{x}(t)=A(t,\mathbf{x}(t))\cdot dt,$$

где $A(t,\mathbf{x}(t))$ определяется по формуле (10).

Приведем пример построения детерминированной SIR-модели ИС, в которой функции (14) и (16) определяют инварианты, обеспечивающие защищенность ИС от эпидемии вирусов. Построенная система ДУ имеет вид:

$$\begin{cases} \frac{dS(t)}{dt}=0,\\ \frac{dI(t)}{dt}=-e^t,\\ \frac{dR(t)}{dt}=e^t. \end{cases} \tag{23}$$

Исходя из (22) и (23), определим управление, обеспечивающее инварианты: $\hat{y}(t):=\hat{y}\big(t,S(t),I(t),R(t)\big)$:

$$\begin{cases} \hat{y}_2(t)=-e^t-\beta I(t)S(t)+\delta I(t),\\ \hat{y}_3(t)=e^t-\delta I(t), \end{cases} \tag{24}$$

Таким образом, детерминированная модель информационной системы, защищенной от распространения эпидемии компьютерных вирусов, имеет вид (23). Функция управления $\hat{y}\big(t,S(t),I(t),R(t)\big)$, определяемая системой (24), гарантирует сохранение инвариантов $u\big(t,S(t),I(t),R(t)\big)$ и $v\big(t,S(t),I(t),R(t)\big)$. Для анализа построенной модели проведем построение численного решения системы дифференциальных уравнений (23), при различных начальных условиях (табл. 2).

На рис. 2 представлены результаты численного решения системы СДУ (23), где для любого из вариантов решения сохраняются значения функций $u\big(t,S(t),I(t),R(t)\big)=0$ (т. е. $LX_i=(X_i)_0+(X_i)_1+(X_i)_2-1=0$) и $v\big(t,S(t),I(t),R(t)\big)=S(t)$ (т. е. $VX_i=(X_i)_0=const$).

Анализируя результаты численного решения, представленные на рис. 2 можно сделать следующий вывод: что при условии сохранения постоянного значения функций $u\big(t,S(t),I(t),R(t)\big)=0,\ v\big(t,S(t),I(t),R(t)\big)$ и начальных значений доли зараженных компьютеров развитие эпидемии компьютерных вирусов не возникает, т.е. доля зараженных компьютеров с течением времени уменьшается.

Таким образом, построена детерминированная математическая модель информационной системы, защищенная от распространения эпидемии компьютерных вирусов [24].

Таблица 2

Начальные условия для построения численного решения системы (23)

Исследуемый показатель	Обозначения (рис. 5)	Начальные условия		
		Вариант 1 (рис. 5,а)	Вариант 2 (рис. 5,б)	Вариант 3 (рис. 5,в)
Доля уязвимых объектов, S_0	$(X_i)_0$	0,5	0.3	0.7
Доля зараженных объектов, I_0	$(X_i)_1$	0,5	0.7	0.3
Доля невосприимчивых или вылеченных объектов, R_0	$(X_i)_2$	0	0	0

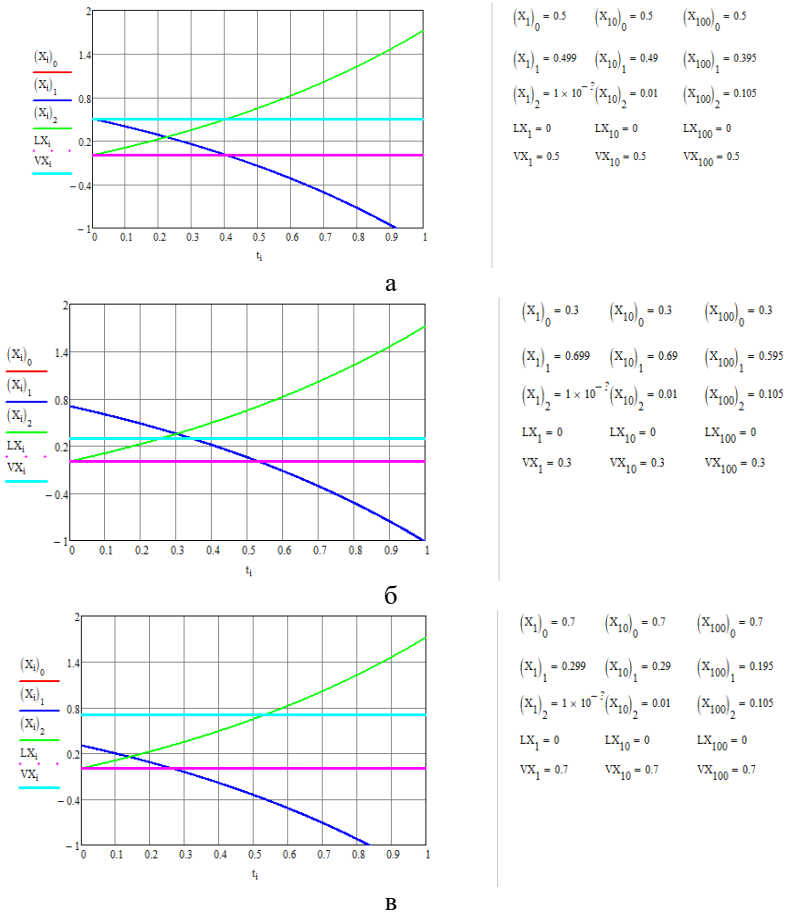

Рис. 2. Численное решение системы (23) с различными начальными условиями: а – вариант 1, б – вариант 2, в – вариант 3 (LX_i и VX_i – первые интегралы соответственно $u\big(t,S(t),I(t),R(t)\big)$ и $v\big(t,S(t),I(t),R(t)\big)$)

Заключение. Внесение в классическую модель SIR стохастического слагаемого позволяет математически описать случайное влияние, вызывающее заражение информационной системы компьютерными вирусами. Показана возможность построения стохастической модели информационной системы, защищенной от распространения эпидемии компьютерных вирусов. Построены две модели: стохастическая инфицирование вирусами которой происходит непрерывно, и детерминированная, в которой вирус находится в системе.

Особенность предлагаемых моделей состоит в том, что в системе сохраняются инварианты, связанные со свойствами, которые обеспечивают защищенность информационной системы. Анализ полученных моделей показал возможность их применения для защиты ИС от распространения эпидемии компьютерных вирусов.

Отметим, что предложенный метод может быть применен к построения стохастической модели, защищенной от эпидемии компьютерных вирусов, и на основе других моделей распространения эпидемии.

Таким образом, предложены методы построения стохастической и детерминированной моделей ИС, защищенной от распространения эпидемии компьютерных вирусов на основе модели SIR, позволяющие информационной системе оставаться в защищенном состоянии.

Финансирование. *Министерство цифрового развития, связи и массовых коммуникаций РФ (проект № 22/23-К), МТУСИ (ФУМО ИБ) от 30.05.2023.*

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Kermack W.O., McKendrick A.* Contributions to the Mathematical Theory of Epidemics // Proc. Royal Society. – 1927. – A 115. – P. 700-721.
2. *Романюха А.А.* Математические модели в иммунологии и эпидемиологии инфекционных заболеваний. – М.: БИНОМ. Лаборатория знаний, 2015. – 256 с.
3. *Захарченко А.* Черводинамика: причины и следствия // Защита информации. Конфидент. – 2004. – № 2. – С. 50-55.
4. *Котенко И.В., Воронцов В.В.* Аналитические модели распространения сетевых червей // Тр. СПИИРАН. – СПб.: Наука, 2007. – № 4.
5. *Минаев В.А., Сычев М.П., Вайц Е.В., Киракосян А.Э.* Имитационное моделирование эпидемии компьютерных вирусов // Вестник Российского нового университета. – 2019. – № 3. – С. 3-12.
6. *Давыдов В.В., Семенов С.Г.* Математическая модель распространения компьютерных вирусов в гетерогенных компьютерных сетях автоматизированных систем управления технологическим процессом // Вестник НТУ ХПИ. – 2012. – № 38. – С. 163-171.
7. *Качалин А.И.* Моделирование процесса распространения сетевых червей для оптимизации защиты корпоративной сети // Искусственный интеллект. – 2006. – № 2. – С. 84-87.
8. *Еремеева Н.И.* Построение модели распространения вируса в компьютерной сети на основе сравнения результатов моделирования с эмпирическими данными // Вестник ТвГУ. Серия: Прикладная математика. – 2022. – № 4. – С. 39-52.
9. *Лесько С.А., Алешкин А.С., Филатов В.В.* Стохастические и перколяционные модели динамики блокировки вычислительных сетей при распространении эпидемий эволюционирующих компьютерных вирусов // Российский технологический журнал. – 2019. – Т. 7, № 3. – С. 7-27.
10. *Борисенко А.Б., Немтинов В.А., Борисенко А.А.* Применение стохастической SIR-модели для моделирования эпидемического процесса // Вестник Тамбовского ГТУ. – 2023. – Т. 29, № 1. – С. 41-51.
11. *Almbrok Hussin Alsonosi Omar, Yahya Abu Hasan,* Numerical simulations of an SIR epidemic model with random initial states // ScienceAsia. – 2013. – 39S. – P. 42-47.
12. *Germán Riaño.* Epidemic Models with Random Infectious Period // medRxiv. – 2020.05.15.20103465.
13. *Caraballo T., Colucci R.* A comparison between random and stochastic modeling for a SIR model // Commun. Pure Appl. – 2017. – A 16. – P. 151-162.
14. *Qingshan Yang, Xuerong Mao*. Stochastic dynamics of SIRS epidemic models with random perturbation // Mathematical Biosciences and Engineering. – 2014. – Vol. 11, Issue 4. – P. 1003-1025.
15. *Swishchuk A., Svishchuk M.* Endemic SIR model in random media with applications // Biom Biostat Int J. – 2018. – Vol. 7, Issue 2. – P. 115-121.
16. *Xue X.* Phase transition for SIR model with random transition rates on complete graphs // Frontiers of Mathematics in China. – 2018. – A 13. – P. 667-690.
17. *Bartoszek K., Bartoszek W., Krzemiński M.* Simple SIR models with Markovian control // Jpn J Stat Data Sci. – 2021. – A 4. – P. 731-762.

18. *Yoon-Gu Hwang, Hee-Dae Kwon, Jeehyun Lee.* Optimal Control Problem of an SIR Model with Random Inputs Based on a Generalized Polynomial Chaos Approach // International Journal of Numerical Analysis and Modeling. – 2022. – Vol. 19. Issue 2-3. – P. 255-274.
19. *Дубко В.А.* Первый интеграл системы стохастических дифференциальных уравнений. – Киев: Институт математики АН УССР, 1978. – 21 с.
20. *Гихман И.И., Скороход А.В.* Стохастические дифференциальные уравнения. – Киев: Наук. Думка, 1968. – 354 с.
21. *Карачанска Е.В.* Интегральные инварианты стохастических систем и программное управление с вероятностью 1. – Хабаровск: Изд-во Тихокеан. гос. ун-та, 2015. – 149 с.
22. *Чалых Е.В.* Построение множества программных управлений с вероятностью 1 для одного класса стохастических систем // Автоматика и телемеханика. – 2009. – Т. 70, № 8. – С. 110-122.
23. *Карачанская Е.В.* Моделирование систем дифференциальных уравнений с динамическими инвариантами // Математическое моделирование и численные методы. – 2019. – № 1. – С. 98-117.
24. *Рыбкина О.В.* Построение детерминированной и стохастической математических моделей защиты информационной системы // Проблемы информационной безопасности. Компьютерные системы. – 2024. – № 3. – С. 30-39.

REFERENCES

1. *Kermack W.O., McKendrick A.* Contributions to the Mathematical Theory of Epidemics, *Proc. Royal Society,* 1927, A 115, pp. 700-721.
2. *Romanyukha A.A.* Matematicheskie modeli v immunologii i epidemiologii infektsionnykh zabolevaniy [Mathematical models in immunology and epidemiology of infectious diseases]. Moscow: BINOM. Laboratoriya znaniy, 2015, 256 p.
3. *Zakharchenko A.* Chervodinamika: prichiny i sledstviya [Chervodynamics: causes and consequences], *Zashchita informatsii. Konfident* [Information Security. Konfident], 2004, No. 2, pp. 50-55.
4. *Kotenko I.V., Vorontsov V.V.* Analiticheskie modeli rasprostraneniya setevykh chervey [Analytical Models of Network Worm Propagation], *Tr. SPIIRAN* [SPIIRAS Proceedings]. Saint Petersburg: Nauka, 2007, No. 4.
5. *Minaev V.A., Sychev M.P., Vayts E.V., Kirakosyan A.E.* Imitatsionnoe modelirovanie epidemii komp'yuternykh virusov [Simulation modeling of computer virus epidemics], *Vestnik Rossiyskogo novogo universiteta* [Bulletin of the Russian New University], 2019, No. 3, pp. 3-12.
6. *Davydov V.V., Semenov S.G.* Matematicheskaya model' rasprostraneniya komp'yuternykh virusov v geterogennykh komp'yuternykh setyakh avtomatizirovannykh sistem upravleniya tekhnologicheskim protsessom [Mathematical model of computer virus propagation in heterogeneous computer networks of automated process control systems], *Vestnik NTU KhPI* [Bulletin of NTU "KhPI"], 2012, No. 38, pp. 163-171.
7. *Kachalin A.I.* Modelirovanie protsessa rasprostraneniya setevykh chervey dlya optimizatsii zashchity korporativnoy seti [Modeling the process of network worm propagation for optimizing corporate network protection], *Iskusstvennyy intellect* [Artificial Intelligence], 2006, No. 2, pp. 84-87.
8. *Eremeeva N.I.* Postroenie modeli rasprostraneniya virusa v komp'yuternoy seti na osnove sravneniya rezul'tatov modelirovaniya s empiricheskimi dannymi [Building a virus spread model in a computer network based on comparing simulation results with empirical data], *Vestnik TvGU. Seriya: Prikladnaya matematika* [Bulletin of Tver State University. Series: Applied Mathematics], 2022, No. 4, pp. 39-52.
9. *Les'ko S.A., Aleshkin A.S., Filatov V.V.* Stokhasticheskie i perkolyatsionnye modeli dinamiki blokirovki vychislitel'nykh setey pri rasprostranenii epidemiy evolyutsioniruyushchikh komp'yuternykh virusov [Stochastic and Percolation Models of Computational Network Lockdown Dynamics During the Spread of Evolving Computer Virus Epidemics], *Rossiyskiy tekhnologicheskiy zhurnal* [Russian Technological Journal], 2019, Vol. 7, No. 3, pp. 7-27.
10. *Borisenko A.B., Nemtinov V.A., Borisenko A.A.* Primenenie stokhasticheskoy SIR-modeli dlya modelirovaniya epidemicheskogo protsessa [Application of the Stochastic SIR Model for Epidemic Process Modeling], *Vestnik Tambovskogo GTU* [Transactions TSTU], 2023, Vol. 29, No. 1, pp. 41-51.
11. *Almbrok Hussin Alsonosi Omar, Yahya Abu Hasan,* Numerical simulations of an SIR epidemic model with random initial states, *ScienceAsia,* 2013, 39S, pp. 42-47.
12. *Germán Riaño.* Epidemic Models with Random Infectious Period, *medRxiv*. 2020.05.15.20103465.
13. *Caraballo T., Colucci R.* A comparison between random and stochastic modeling for a SIR model, *Commun. Pure Appl*., 2017, A 16, pp. 151-162.
14. *Qingshan Yang, Xuerong Mao*. Stochastic dynamics of SIRS epidemic models with random perturbation, *Mathematical Biosciences and Engineering,* 2014, Vol. 11, Issue 4, pp. 1003-1025.
15. *Swishchuk A., Svishchuk M.* Endemic SIR model in random media with applications, *Biom Biostat Int J.*, 2018, Vol. 7, Issue 2, pp. 115-121.

16. *Xue X.* Phase transition for SIR model with random transition rates on complete graphs, *Frontiers of Mathematics in China,* 2018, A 13, pp. 667-690.
17. *Bartoszek K., Bartoszek W., Krzemiński M.* Simple SIR models with Markovian control, *Jpn J Stat Data Sci*., 2021, A 4, pp. 731-762.
18. *Yoon-Gu Hwang, Hee-Dae Kwon, Jeehyun Lee.* Optimal Control Problem of an SIR Model with Random Inputs Based on a Generalized Polynomial Chaos Approach, *International Journal of Numerical Analysis and Modeling,* 2022, Vol. 19. Issue 2-3, pp. 255-274.
19. *Dubko V.A.* Pervyy integral sistemy stokhasticheskikh differentsial'nykh uravneniy [The first integral of the system of stochastic differential equations]. Kiev: Institut matematiki AN USSR, 1978, 21 p.
20. *Gikhman I.I., Skorokhod A.V.* Stokhasticheskie differentsial'nye uravneniya [Stochastic differential equations]. Kiev: Nauk. Dumka, 1968, 354 p.
21. *Karachanska E.V.* Integral'nye invarianty stokhasticheskikh sistem i programmnoe upravlenie s veroyatnost'yu 1 [Integral invariants of stochastic systems and program control with probability 1]. Khabarovsk: Izd-vo Tikhokean. gos. un-ta, 2015, 149 p.
22. *Chalykh E.V.* Postroenie mnozhestva programmnykh upravleniy s veroyatnost'yu 1 dlya odnogo klassa stokhasticheskikh sistem [Constructing the set of program controls with probability 1 for one class of stochastic systems], *Avtomatika i telemekhanika* [Automation and Remote Control], 2009, Vol. 70, No. 8, pp. 110-122.
23. *Karachanskaya E.V.* Modelirovanie sistem differentsial'nykh uravneniy s dinamicheskimi invariantami [Modeling of systems of differential equations with dynamic invariants], *Matematicheskoe modelirovanie i chislennye metody* [Mathematical modeling and numerical methods], 2019, No. 1, pp. 98-117.
24. *Rybkina O.V.* Postroenie determinirovannoy i stokhasticheskoy matematicheskikh modeley zashchity informatsionnoy sistemy [Construction of deterministic and stochastic mathematical models of information system protection], *Problemy informatsionnoy bezopasnosti. Komp'yuternye sistemy* [Problems of information security. Computer systems], 2024, No. 3, pp. 30-39.

Карачанская Елена Викторовна – Дальневосточный государственный университет путей сообщения; e-mail: elena_chal@mail.ru; г. Хабаровск, Россия; д.ф.-м.н., профессор кафедры «Информационные технологии и системы».

Рыбкина Олеся Викторовна – Дальневосточный государственный университет путей сообщения; e-mail: ribkina_ol@mail.ru; г. Хабаровск, Россия; старший преподаватель кафедры «Информационные технологии и системы».

Karachanskaya Elena Viktorovna – Far Eastern State Transport University; e-mail: elena_chal@mail.ru; Khabarovsk, Russia; dr. of phys.-math. sc.; professor of the Department «Information Technologies and Systems».

Rybkina Olesya Viktorovna – Far Eastern State Transport University; e-mail: ribkina_ol@mail.ru; Khabarovsk, Russia; senior lecturer of the Department of «Information Technologies and Systems».

УДК 303.732.4 DOI 10.18522/2311-3103-2025-6-157-178

А.И. Гусева, Р.М. Романов

МЕТОД ПРОГНОЗИРОВАНИЯ ВРЕМЕННЫХ РЯДОВ, ОСНОВАННЫЙ НА КОГНИТИВНОМ НЕЧЕТКОМ МОДЕЛИРОВАНИИ И РЕГРЕССИОННОМ АНАЛИЗЕ

Актуальность исследования определяется низкой эффективностью традиционных методов прогнозирования временных рядов в условиях высокой неопределённости и ограниченного объёма данных, характерных для слабо формализованных систем. Цель работы заключается в разработке и обосновании метода прогнозирования временных рядов на основе гибридного подхода, объединяющего когнитивное нечеткое моделирование, регрессионный анализ и метод аналитических сетей. В рамках исследования проведён системный обзор и сравнительный анализ существующих методов прогнозирования, включая подходы на основе нечеткой логики, нейросетевого и когнитивного моделирования, ансамблевых и гибридных методов, и выявлены их ограничения при работе с малыми выборками, нелинейными зависимостями и неопределённостью. Разработанный ме-