Intellectual Technologies on Transport No 4

Интеллектуальные технологии на транспорте № 4

Санкт-Петербург
St. Petersburg
2017

Интеллектуальные технологии на транспорте
№ 4, 2017

Сетевой электронный научный журнал, свободно распространяемый через Интернет.
Публикует статьи на русском и английском языках с результатами исследований и практических достижений в области интеллектуальных технологий и сопутствующих им научных исследований

Журнал основан в 2015 году

Учредитель и издатель

Федеральное государственное бюджетное образовательное учреждение высшего образования «Петербургский государственный университет путей сообщения Императора Александра I» (ФГБОУ ВПО ПГУПС)

Адрес редакции
190031 Санкт-Петербург, Московский пр., 9, ПГУПС
email: itt-pgups@yandex.ru, сайт: http://itt-pgups.ru, редактор сайта Рогальчук В.В.

ISSN 2413-2527

Журнал зарегистрирован Федеральной службой по надзору в сфере связи и массовых коммуникаций, свидетельство ЭЛ № ФС77-61707 от 07 мая 2015 г.

Журнал зарегистрирован в Российском индексе научного цитирования (РИНЦ)

Intellectual Technologies on Transport
Issue № 4, 2017

Network electronic scientific journal, open access. It publishes articles in Russian and English with the results of research and practical achievements in the field of intelligent technologies and associated research

Founded in 2015

Founder and Publisher
Federal State Educational Institution of Higher Education
«Emperor Alexander I Petersburg State Transport University»

Adress
190031, St. Petersburg, Moskovskiy pr., 9, 2–108
email: itt-pgups@yandex.ru, http://itt-pgups.ru, Site Editor: Rogalchuk V.V.

ISSN 2413-2527

The journal is registered by the Federal Service for Supervision of Communications and Mass Media, EL №FS77-61707 testimony from May 7, 2015

The journal is registered in the Russian Science Citation Index (RSCI)

Содержание

Contents

Модели и методы анализа систем массового обслуживания с параметрической неопределенностью

Гончаренко В. А.
Военно-космическая академия имени А. Ф. Можайского
Санкт-Петербург, Россия
vlango@mail.ru

Аннотация. **Обсуждается подход к описанию случайных процессов, используемых в теории очередей, для учета влияния параметрической неопределенности исходных данных. Рассмотрен метод представления распределений вероятностей в виде двухуровневой композиции интегрального ядра и фазовой функции. Предложены методы расчета систем массового обслуживания в условиях интервальной неопределенности параметров распределений времени между входными заявками и времени их обслуживания.**

Ключевые слова: **рандомизация, случайный параметр, параметрическая неопределенность, интегральное ядро, обобщенная функция, распределение фазового типа, аппроксимация, фазовая функция.**

Введение

При исследовании процессов функционирования современных информационно-вычислительных систем (ИВС) активно используются математические модели массового обслуживания [1]. Одной из основных проблем проектирования и модернизации ИВС является трудность их формирования на начальных этапах разработки достоверных исходных данных. Использование простейших случайных потоков без последействия значительно упрощает исследование систем, однако может приводить к существенным искажениям оцениваемых характеристик систем [2]. Для более точного описания моделей обслуживания используются произвольные потоки случайных событий [1, 3].

Точные методы расчета систем массового обслуживания (СМО) весьма ограничены в применении, поэтому развиваются различные приближенные методы. Среди них так называемые аппроксимационные методы, предполагающие аппроксимацию реальных распределений вероятностей распределениями фазового типа [2], описывающие случайные процессы в виде совокупности последовательных и/или параллельных экспоненциальных фаз. Данный подход, предложенный еще А. Эрлангом, был развит Д. Коксом [4], М. Ньютсом [5] и другими учеными [3, 6, 7], найдя широкое применение в теории надежности и теории очередей при расчете немарковских систем.

Однако физическая природа протекающих в ИВС случайных процессов и воздействие на них различных возмущающих факторов приводит к отклонениям параметров распределений. Кроме того, данные параметры могут быть не полностью определены, и по отношению к ним могут использоваться приближенные оценки [8]. Всё это приводит к необходимости использовать более обобщенные модели случайных процессов с неопределенностью [9].

Актуальна задача разработки общих подходов к описанию СМО с возмущениями или с неопределенностью параметров. В статье развиваются методы расчета СМО для общего случая, когда произвольные распределения могут быть аппроксимированы распределениями фазового типа с использованием не дискретных фаз, а непрерывной фазовой функции. При этом аппроксимирующее распределение представляется в виде композиции экспоненциального ядра и фазовой функции, в частном случае выступающей плотностью распределения (ПР) случайного параметра экспоненциального ядра.

Описание случайных процессов обслуживания с параметрической неопределенностью

Информация об исследуемой системе может иметь разные уровни неопределенности [9]:

• *неизвестность* соответствует начальной стадии изучения системы и характеризует состояние практически полного отсутствия информации;

• *недостоверность* соответствует первым этапам сбора информации, когда процесс сбора временно приостановлен или для этого не хватает ресурсов;

• *неоднозначность* соответствует ситуации, когда полностью определённое описание не может быть получено даже при наличии всей требуемой достоверной информации, поскольку неопределенность свойственна самой сущности рассматриваемых процессов.

В процессе изучения системы уменьшается степень недостоверности исходных данных. Воздействия различных возмущающих факторов на параметры случайных потоков приводят к их детерминированным или случайным возмущениям, а также к неоднозначности их описания.

Неопределенность описания случайного процесса из-за недостоверности исходных данных и действия возмущающих факторов часто может быть сведена к параметрической неопределенности, которую необходимо в процессе накопления исходных данных либо устранить, либо описать более точно (в случае, если неоднозначность параметров присуща реальным процессам).

Предположим, что случайные внешние воздействия на систему представимы в виде неопределенности (в частности, случайности) параметров распределений случайных величин, характеризующих систему [9].

Рассмотрим рекуррентный поток, описывающий один из случайных процессов в исследуемой СМО и заданный набором номинальных параметров $\Theta = \{\theta_1, \theta_2, ..., \theta_m\}$ функции распределения (ФР) интервалов между событиями. Параме-

тры распределений подвержены изменениям, определяющимся как логикой и динамикой функционирования самой системы, так и проявлением различных возмущающих факторов, отклоняющих параметры системы от номинальных. Пусть эти изменения оказывают *аддитивное* влияние на номинальные значения параметров, тогда реальные значения последних могут быть представлены в виде

$$\hat{\theta}_i(t) = \theta_i(t) + \Delta\hat{\theta}_i(t);\ \ i = 1 \div m. \qquad (1)$$

Данные параметры при неоднозначности исходных данных могут принимать как детерминированные, так и случайные значения из фиксированного множества или непрерывного диапазона в зависимости от времени или независимо от него.

В то же время аналогично может быть задан поток событий, параметры которого имеют *недостоверное представление* в виде взвешенного множества возможных значений, определенных по результатам статистического или экспертного оценивания. Эта недостоверность выражается в последнем слагаемом.

Таким образом, обобщенное представление случайного потока событий с параметрической неопределенностью (возмущением) позволит учесть как недостоверность исходных данных, так и возмущающие факторы.

Параметры распределения $\hat{\Theta}(t)$ или интенсивность потока $\hat{\lambda}(t)$ могут быть представлены в зависимости от имеющихся исходных данных случайной функцией времени или случайной величиной, не зависящей от времени.

В первом представлении рассматриваемые параметры ($\hat{\Theta}(t)$ или $\hat{\lambda}(t)$) являются случайными процессами, не зависящими от моментов наступления событий случайного потока. В частности, случайный поток, интенсивность которого есть случайный процесс, называют *дважды стохастическим потоком* [10]. Интенсивность такого потока может быть как непрерывной, так и кусочно-постоянной случайной. В последнем случае речь идет о MC (Markov chain)-потоках, в которых $\hat{\lambda}(t)$ сохраняет постоянное значение в течение некоторого времени, после чего скачком принимает новое значение [11].

Во втором представлении моменты изменения случайных параметров $\hat{\Theta}(t)$ распределения времени между событиями или случайной интенсивности потока $\hat{\lambda}$ определяются моментами наступления событий. Следовательно, интервалы между событиями распределены по одному закону, но со стохастически различными параметрами, вероятностный закон распределения которых характеризует ситуацию неопределенности их значений.

Таким образом, ФР времени между наступлением событий при случайности параметров распределений сама становится случайной функцией – $F(x, \hat{\Theta}) = \hat{y}(x)$, полной характеристикой которой является *функционал распределения* $G(y(x)) = P\{\hat{y}(x) < y(x)\}$. Например, для экспоненциальной ФР $F(t, \hat{\lambda}) = 1 - e^{-\hat{\lambda}t}$ с равномерно распределенным параметром $\hat{\lambda}$ в диапазоне $[a, b]$ функционал распределения $G(y(t))$ получим в виде

$$G(y(t)) = \ln[e^{-at} / (1 - y(t))] / (b - a)t.$$

Математическим ожиданием случайной ФР является усредненная по параметрам ФР [9].

Пусть случайный параметр $\hat{\lambda}$ экспоненциальной функции распределения сам имеет *экспоненциальную плотность распределения*:

$$h(\lambda) = \theta e^{-\theta\lambda};\ \ \lambda > 0.$$

В этом случае функция и плотность распределения времени между событиями находятся довольно просто:

$$F(t) = \frac{t}{t + \theta};\quad f(t) = \frac{\theta}{(t + \theta)^2}.$$

Однако $f(t)$ при $t \to 0$ имеет очень длинный «хвост», из-за чего высшие начальные моменты будут бесконечными. Данное распределение является частным случаем распределения Парето. Такие случайные процессы относятся к *самоподобным*, весьма трудны в исследовании, но типичны для потоков в компьютерных сетях, моделях дорожной сети и многих других приложениях [12].

Таким образом, процессы восстановления, используемые для аппроксимации случайных процессов со случайно распределенными параметрами, совпадают с последними на уровне математических ожиданий исследуемых процессов. Качество же такой аппроксимации зависит от величины дисперсии случайного процесса. Кроме того, при рандомизации параметра функции распределения $F(t)$ средняя интенсивность потока $1/\nu_1$ получает смещение влево от первоначального значения для нерандомизированной ФР.

Предложенный подход может быть использован при построении и исследовании *нового класса моделей с неопределенностью параметров* в теории очередей [9, 13].

Формирование аппроксимационных распределений с произвольной фазовой функцией на основе двухуровневой композиции

При моделировании систем массового обслуживания часто используются распределения фазового типа [2]. Используем понятие фазовой функции как обобщение набора фаз (последовательных, параллельных) в методе фаз Эрланга [14]. *Фазовая функция* представляет собой произвольную дифференцируемую функцию, принадлежащую пространству *основных и обобщенных функций* [15], описывающую структуру фазового построения распределения вероятностей фазового типа.

Согласно [16], плотность распределения случайной величины t для $\forall t$ может быть представлена в виде уравнения Фредгольма 1-го рода как композиция интегрального ядра $f(t, \lambda)$ и фазовой функции $h(\lambda)$:

$$f(t) = \int_{-\infty}^{\infty} f(t, \lambda) h(\lambda) d\lambda. \qquad (2)$$

Интегральное ядро $f(t, \lambda)$ может задаваться одной из легко интегрируемых функций, чаще всего экспоненциальной, поскольку именно на базе *экспоненциального интегрального ядра* можно построить большое количество распределений фазового типа. Таким образом, фазовая функция $h(\lambda)$ служит своего рода *оператором преобразования* функции $f(t, \lambda)$ к функции $f(t)$ и в ряде случаев может не иметь физического смысла плотности распределения [14]. В частном случае при интерпретации $h(\lambda)$ как ПР случайного параметра

используются как *обобщенные* (например, гипердельтное распределение [17]), так и *основные* [15] функции (например, равномерное, нормальное, экспоненциальное распределения).

В качестве аппроксимирующей плотности распределения случайного параметра $\hat{\lambda}$ можно применить гипердельтное распределение:

$$h_a(\lambda) = \sum_{i=1}^{n} C_i \delta(\lambda - \lambda_i), \quad (3)$$

где C_i – вероятности, удовлетворяющие условию $\sum_{i=1}^{n} C_i = 1$; $\delta(\lambda)$ – дельта-функция Дирака.

При гипердельтной аппроксимации фазовой функции $h(\lambda)$, подставляя (3) вместо $h(\lambda)$ в (2), получим *гиперпредставление* ПР случайной величины t:

$$f(t) = \sum_{i=1}^{n} C_i f(t, \lambda_i). \quad (4)$$

При экспоненциальном интегральном ядре $f(t, \lambda_i)$ из следующей формулы получим *гиперэкспоненциальную плотность распределения*, часто используемую для аппроксимации реальных распределений в теории очередей:

$$f(t) = \sum_{i=1}^{n} C_i \lambda_i e^{-\lambda_i t}. \quad (5)$$

При аппроксимации произвольного распределения распределением с *произвольной фазовой функцией* используем метод производных [18], при котором аппроксимация производится на основе равенства производных аппроксимирующей и аппроксимируемой функций в нулевой точке. Можно установить взаимосвязь между аппроксимацией *методом производных* произвольной ПР и аппроксимацией *методом моментов* фазовой функции этой плотности [16].

В [16] была доказана лемма, что аппроксимация методом производных произвольной плотности распределения случайной величины, представленной формулой (3), соответствует аппроксимации методом моментов фазовой функции этой плотности.

При экспоненциальности интегрального ядра $f(t, \lambda)$ ПР $f(t)$ согласно (2) определяется фазовой функцией (оператором) $h(\lambda)$:

$$f(t) = \int_0^{\infty} \lambda e^{-\lambda t} h(\lambda) d\lambda. \quad (6)$$

На основе формулы (6) при различных фазовых функциях можно получить выражения для распределений времени между событиями. Для гиперэкспоненциальной плотности распределения (5) фазовая функция представляется гипердельтной функцией (3).

Для плотности распределения Эрланга k-го порядка

$$f(t) = \frac{\lambda_0^{\,k} t^{k-1}}{(k-1)!} e^{-\lambda_0 t}$$

фазовая функция представляется обобщенной функцией:

$$h_a(\lambda) = \frac{\lambda_0^{\,2} \cdot d\delta(\lambda - \lambda_0)}{\lambda d\lambda}.$$

Возможен и обратный переход – от фазовой функции к функции распределения. Так, если фазовая функция является плотностью равномерного распределения

$$h_a(\lambda) = \frac{\mathbf{1}(\lambda - a) \cdot \mathbf{1}(b - \lambda)}{b - a},$$

где $\mathbf{1}(\lambda)$ – единичная ступенчатая функция Хевисайда, то плотность распределения времени между событиями будет задаваться *равномерно-экспоненциальным законом*:

$$f(t) = \frac{(1 + at)e^{-at} - (1 + bt)e^{-bt}}{(b - a)t^2}.$$

Начальные моменты случайного параметра $\hat{\lambda}$ случайного экспоненциального распределения $f(t, \hat{\lambda})$ могут быть определены с помощью производных усредненной по параметру плотности $f(t)$ точки $t = 0$ [7]:

$$\gamma_k = (-1)^{k-1} f^{(k-1)}(0).$$

В отсутствие сведений о характере изменения параметров распределений исходят из принципа «максимума неопределенности», и расчет системы проводят при допущении равномерного распределения случайного параметра $\hat{\lambda}$. При наличии сведений о другом виде распределения случайного параметра $\hat{\lambda}$ (например, нормальном), или о начальных моментах случайных параметров характеристики потока находятся на основе предлагаемого аппроксимационного метода.

Предложенный метод позволяет использовать единое представление для распределений случайных величин в виде композиции интегрального ядра и фазовой функции, даже если последняя по физическому смыслу не является плотностью распределения. При построении фазовых функций используется математический аппарат обобщенных функций, представляющих собой линейные непрерывные функционалы на пространстве основных функций.

Методы расчета систем массового обслуживания с параметрической неопределенностью

Класс моделей обслуживания с параметрической неопределенностью образуется с помощью введения представления исходных распределений в виде уравнений Фредгольма 1-го рода с интегральным ядром в виде фазового распределения и произвольной фазовой функцией (как дискретной, так и непрерывной).

Приведем основные классы систем массового обслуживания с параметрической неопределенностью:

1) модели с экспоненциальным ядром и *дискретной фазовой функцией* – получим стандартные фазовые распределения (типа гиперэкспоненциального и гипоэкспоненциального);

2) модели с экспоненциальным ядром и *фазовой функцией, не являющейся плотностью* (например, в виде производной функции Дирака);

3) модели с *ядром фазового типа* (распределения экспонента, гиперэкспонента, гипоэкспонента, Эрланга, Кокса и т. д.) и *непрерывной фазовой функцией* (равномерной, нормальной, экспоненциальной и т. д.);

4) модели с *ядром нефазового типа* и *произвольной фазовой функцией*.

Рассмотрим модели третьего класса, допускающие возможность учета реальной неопределенности или возмуще-

ний параметров распределений. Предположим наличие интервальной неопределенности информации о параметрах исходных распределений в СМО. При интервальном подходе [13] неопределенные параметры θ_i модели задаются в виде диапазона возможных значений $[\theta_{\min i}, \theta_{\max i}]$. Это могут быть границы случайного изменения параметров, доверительные интервалы, построенные с заданной надежностью для θ_i по результатам наблюдений над реальным узлом, экспертные оценки возможных значений параметров проектируемой системы, допустимые отклонения параметров узла от номинальных значений и т. д., в зависимости от характера рассматриваемой неопределенности.

Пусть СМО имеет экспоненциальные распределения входного потока и потока обслуживания с неопределенными параметрами распределений, бесконечный накопитель очереди и дисциплину обслуживания FIFO. Параметры экспоненциальных распределений λ и μ принимают значения в известных пределах $[a, b]$ и $[c, d]$, соответственно. Необходимо получить вероятностно-временные характеристики СМО с учетом данной неопределенности.

При использовании усредненных детерминированных значений параметров экспоненциальных распределений $\lambda = (a + b)/2$ и $\mu = (c + d)/2$ приходим к известной модели типа $M/M/1$. Однако при этом никак не учитывается реальный уровень неопределенности исходных данных, что приводит к существенным погрешностям и к смещению математических ожиданий оцениваемых характеристик.

Используем прием рандомизации экспоненциальной модели типа $M/M/1$, предложенный в [13]. Будем рассматривать множество моделей, являющихся окрестностью модели $M/M/1$, в которой допускаются отклонения (колебания) параметров распределений в заданных выше пределах, а сами параметры λ и μ будем считать случайными и непрерывно распределенными в этих диапазонах. Обозначим данную систему в символике Кендалла $\hat{M}/\hat{M}/1$. Условные плотности распределений интервалов времени между поступающими в узел заявками $a(t, \lambda|\lambda)$ и времени их обслуживания в узле $b(x, \mu|\mu)$ (при условии, что случайные параметры $\hat{\lambda}$ и $\hat{\mu}$ приняли значения λ и μ) имеют вид

$$a(t,\lambda \mid \lambda) = \lambda e^{-\lambda t};\ t > 0, a < \lambda < b; \tag{7}$$

$$b(x,\mu \mid \mu) = \mu e^{-\mu x};\ x > 0, c < \mu < d. \tag{8}$$

В отсутствие сведений о характере изменения λ и μ будем исходить из принципа максимума энтропии [9], считая возможные значения параметров равновероятными. Плотности равномерных распределений случайных параметров $\hat{\lambda}$ и $\hat{\mu}$, соответствующие максимальной неопределенности информации, имеют вид

$$f_1(\lambda) = \begin{cases} 1/(b-a), \lambda \in [a,b]; \\ 0, \lambda \notin [a,b]; \end{cases} \quad f_2(\mu) = \begin{cases} 1/(d-c), \mu \in [c,d]; \\ 0, \mu \notin [c,d]. \end{cases}$$

Безусловные (усредненные по случайным параметрам) плотности распределений $a(t)$ и $b(x)$ можно получить, используя обобщенную формулу полной вероятности для непрерывного случая:

$$a(t) = \int_a^b \lambda e^{-\lambda t} f_1(\lambda) d\lambda = \frac{(1+at)e^{-at} + (1+bt)e^{-bt}}{(b-a)t^2}; \tag{9}$$

$$b(x) = \int_c^d \mu e^{-\mu x} f_2(\mu) d\mu = \frac{(1+cx)e^{-cx} + (1+dx)e^{-dx}}{(d-c)x^2}. \tag{10}$$

Полученные $a(t)$ и $b(t)$ являются математическими ожиданиями функционалов распределений случайных плотностей распределения, но они имеют также собственные начальные моменты α_k и β_k, соответственно:

$$\alpha_1 = \frac{\ln(b/a)}{b-a};\ \ \alpha_k = \frac{(b^{k-1} - a^{k-1}) \cdot k!}{(k-1)(b-a)(ab)^{k-1}};\ k > 1; \tag{11}$$

$$\beta_1 = \frac{\ln(d/c)}{d-c};\ \ \beta_k = \frac{(d^{k-1} - c^{k-1}) \cdot k!}{(k-1)(d-c)(cd)^{k-1}};\ k > 1. \tag{12}$$

Чтобы найти характеристики СМО $\hat{M}/\hat{M}/1$ со случайными параметрами, используем метод спектрального разложения интегрального уравнения Линдли [8, 13], основное соотношение для которого имеет вид

$$A^*(-s) \cdot B^*(s) - 1 = \Psi_+(s) / \Psi_-(s), \tag{13}$$

где $A^*(s)$ и $B^*(s)$ – преобразования Лапласа – Стилтьеса (ПЛС) исходных плотностей распределений $a(t)$ и $b(x)$; $\Psi_+(s)$ – рациональная аналитическая функция от s без нулей в $\mathrm{Re}(s) > 0$; $\lim\limits_{s \to 0} \Psi_+(s)/s = 1$ для $\mathrm{Re}(s) > 0$; $\Psi_-(s)$ – рациональная аналитическая функция от s без нулей в $\mathrm{Re}(s) < D$; $\lim\limits_{s \to 0} \Psi_-(s)/s = -1$ для $\mathrm{Re}(s) < D$.

ПЛС $A^*(s)$ и $B^*(s)$ для (9) и (10) будут иметь вид

$$A^*(s) = 1 - s\alpha(s);\ B^*(s) = 1 - s\beta(s), \tag{14}$$

где $\alpha(s) = \ln[(b+s)/(a+s)]/(b-a)$ и $\beta(s) = \ln[(d+s)/(c+s)]/(d-c)$.

Тогда после подстановки (14) в (13) и некоторых преобразований получим следующее соотношение:

$$\frac{s(1/\beta(s) - 1/\alpha(s) - s)}{1/\alpha(s)/\beta(s)} = \frac{\Psi_+(s)}{\Psi_-(s)}. \tag{15}$$

Несмотря на то, что левая часть (15) не является рациональной функцией, она удовлетворяет условиям аналитичности. Чтобы найти $\Psi_+(s)$ и $\Psi_-(s)$, используя теорему Руше [13], покажем, что числитель левой части (15) имеет кроме нулевого корня еще только один действительный корень $s_1 < 0$. Уравнение

$$1/\beta(s) - 1/\alpha(-s) - s = 0 \tag{16}$$

является трансцендентным и разрешимо относительно s в частных случаях ($a = b$ или/и $c = d$) – соответственно, узлы типа $M/G/1$, $G/M/1$ или $M/M/1$.

Для решения задачи общего типа ($G/G/1$) используем следующий прием: корень уравнения (16) найдем по аналогии с решением для узла типа $G/M/1$, но выраженный через переменную S:

$$s_1(s) = a - \frac{b-a}{e^{(b-a)/(1/\beta(s) - s)} - 1}. \tag{17}$$

Тогда функции $\Psi_+(s)$ и $\Psi_-(s)$ можно представить в виде следующего спектрального разложения:

$$\Psi_+(s) = s\beta(s) \cdot (s - s_1(s)); \tag{18}$$

$$\Psi_-(s) = \frac{(s - s_1(s))/\alpha(-s)}{1/\beta(s) - 1/\alpha(-s) - s}. \quad (19)$$

В частных случаях данное разложение трансформируется в соответствующие решения для частных типов СМО ($M/G/1$, $G/M/1$ или $M/M/1$). Так, при $\mu = c = d$ корень s_1 из (17) превратится в константу:

$$s_1 = a - \frac{b-a}{e^{(b-a)/\mu} - 1}.$$

Используя данные функции, найдем основные характеристики отдельного узла сети со случайными параметрами.

Вероятность застать узел незанятым:

$$r_0 = \lim_{s\to\infty} \frac{\Psi_+(s)}{s} = \left(\frac{b-a}{e^{(b-a)\beta_1} - 1} - a \right) \cdot \beta_1. \quad (20)$$

При $\lambda = a = b$ r_0 совпадает с вероятностью простоя p_0:

$$r_0 = p_0 = 1 - \frac{\lambda \ln(d/c)}{d-c}. \quad (21)$$

ПЛС ПР времени ожидания заявки в очереди:

$$W^*(s) = \frac{r_0}{(s - s_1(s))\beta(s)}. \quad (22)$$

ПЛС ПР периода простоя имеет вид

$$V^*(s) = 1 - \frac{s(1 - \alpha(s)/\beta(-s) - s\alpha(s))}{s + s_1(-s)}. \quad (23)$$

Обозначив $W^*(s) = r_0/H(s)$, $V^*(s) = 1 - E(s)/F(s)$, запишем выражения для их начальных моментов ω_k и υ_k, соответственно:

$$\omega_k = \frac{1}{r_0} \sum_{j=1}^{k} \binom{k}{j} (-1)^{j+1} H^{(j)}(0) \omega_{k-j}; \quad (24)$$

$$\upsilon_k = \sum_{j=1}^{k-1} \binom{k}{j} (-1)^{j+1} \frac{F^{(j)}(0)}{F(0)} \upsilon_{k-j} + (-1)^{k+1} \frac{E^{(k)}(0)}{F(0)}, \quad (25)$$

где $E^{(j)}(0)$, $F^{(j)}(0)$ и $H^{(j)}(0)$ – производные j-го порядка по s соответствующего выражения в точке $s = 0$, которые вычисляются с помощью рекуррентного алгоритма [13].

Выведем формулу среднего времени ожидания обслуживания в узле:

$$\omega_1 = \frac{\beta_1}{r_0} \left(1 + \frac{(b-a)^2 \cdot (\beta_2/2 - \beta_1^2) \cdot e^{(b-a)\beta_1}}{(e^{(b-a)\beta_1} - 1)^2} \right) - \frac{\beta_2}{2\beta_1}. \quad (26)$$

Для расчета сетей массового обслуживания представляет интерес время пребывания заявки в узле и выходящий из узла поток заявок. ПЛС плотностей распределения времени пребывания заявки в узле $G^*(s)$ и времени между выходящими заявками $D^*(s)$ имеют вид

$$G^*(s) = W^*(s) \cdot B^*(s) = \frac{r_0(1/\beta(s) - s)}{(s - s_1(s))\beta(s)};$$

$$D^*(s) = (1 - r_0 + r_0 V^*(s)) \cdot B^*(s).$$

С учетом (12), (24) и (25) получим начальные моменты распределения времени пребывания заявки в узле γ_k и распределения времени между выходными заявками δ_k:

$$\gamma_k = \sum_{j=0}^{k} \binom{k}{j} \omega_j \beta_{k-j};$$

$$\delta_k = \beta_k + r_0 \sum_{j=1}^{k} \binom{k}{j} \beta_{k-j} \upsilon_j.$$

Для коэффициента вариации выходящего потока имеем

$$C_\delta = \sqrt{C_\alpha^2 + 2(D_\beta - (\alpha_1 - \beta_1)\omega_1)/\alpha_1^2}.$$

Для оценки влияния неопределенности параметров распределений на характеристики системы удобно использовать коэффициенты неопределенности параметров:

$$\Delta_1 = (b-a)/(b+a); \ \Delta_2 = (d-c)/(d+c),$$

принимающие значения от 0 до 1. Отсутствию неопределенности соответствуют нулевые значения коэффициентов, при увеличении степени неопределенности параметров коэффициенты стремятся к единице.

На рис. 1 изображена криволинейная поверхность, отражающая зависимость относительного времени ожидания ω_1/β_1 от коэффициентов неопределенности Δ_1 и Δ_2 при фиксированном коэффициенте загрузки $\rho = 0{,}5$. Анализ показал, что характеристики модели более чувствительны к неопределенности параметров обслуживания, чем к аналогичной неопределенности параметров входного потока. При увеличении загрузки ρ зависимость ω_1/β_1 монотонно возрастает, но Δ_2 оказывает на нее большее влияние, чем Δ_1. Аналогичные выводы можно сделать и по высшим моментам.

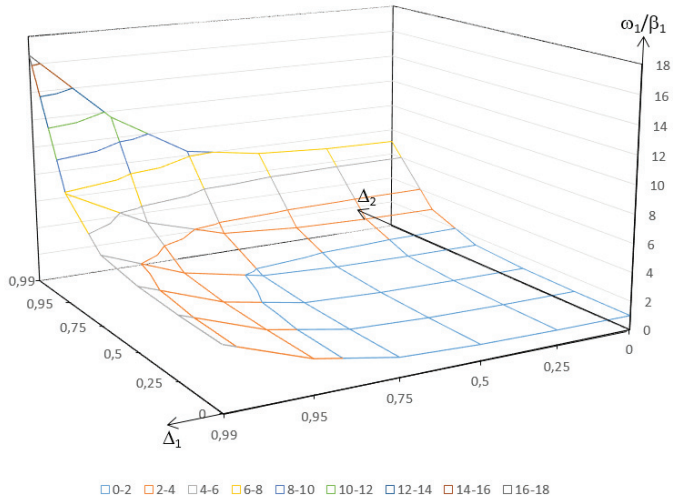


Рис. 1. Зависимость ω_1/β_1 от коэффициентов Δ_1 и Δ_2

На рис. 2 изображена зависимость отношения коэффициентов вариации выходящего и входящего потоков C_δ/C_α от коэффициентов Δ_1 и Δ_2. Из графика видно, что при фиксированном Δ_1 и увеличении Δ_2 данная зависимость возрастает, а при фиксированном Δ_2 и увеличении Δ_1 – наоборот, убывает. Это объясняется тем, что при увеличении Δ_2 увеличивается коэффициент вариации времени обслуживания, что ведет к большему разбросу времени между выходящими заявками по сравнению со входящими. При увеличении же Δ_1 увеличивается коэффициент вариации входного потока C_α, причем более быстро, чем C_δ. Зависимости коэффициента

вариации C_δ от загрузки системы при различных неопределенностях ведут себя по-разному. При $\Delta_1 = 0$ и $\Delta_2 \neq 0$ эта зависимость возрастающая, при $\Delta_1 \neq 0$ и $\Delta_2 = 0$ – убывающая. При $\rho \approx 0{,}7$–$0{,}75$ зависимости пересекаются. Это обусловлено тем, что при малом ρ разброс выходящего потока почти целиком определяется характером входного потока. При увеличении же ρ на выходном потоке начинает все больше сказываться влияние механизма обслуживания.

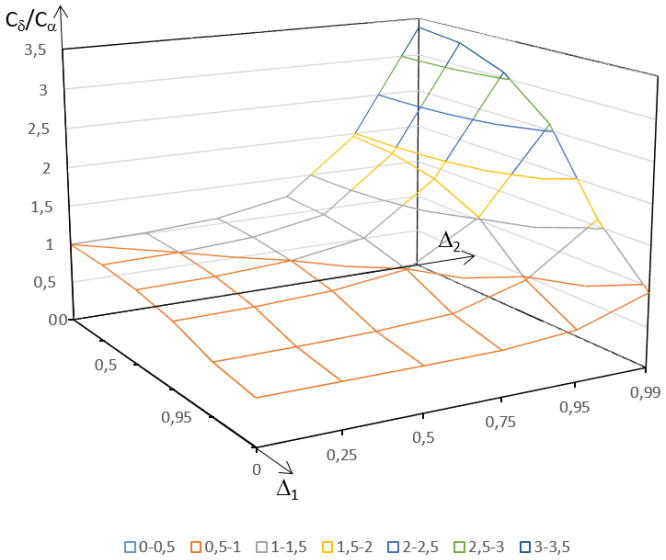


Рис. 2. Зависимость C_δ/C_α от коэффициентов Δ_1 и Δ_2

На основе предложенного подхода так же рассчитаны и другие модели с параметрической неопределенностью – с гиперэкспоненциальными $\hat{H}_n$ и/или эрланговскими $\hat{E}_n$ законами во входном потоке или потоке обслуживания, однако при одновременной немарковости распределений аналитический вывод зависимостей затрудняется трансцендентностью уравнений, и требуются численные решения.

Заключение

Предложенный подход позволяет рассчитывать усредненные вероятностно-временные характеристики СМО в условиях параметрической неопределенности исходных распределений, вызванной как изменчивостью, так и недостоверностью параметров. На основе анализа полученных зависимостей можно сделать вывод, что характеристики анализируемой системы более чувствительны к колебаниям (неопределенности) параметров обслуживания, чем параметров входного потока.

Практическая значимость метода определяется его возможностью использования на различных этапах проектирования и модернизации ИВС в зависимости от имевшегося объема исходных данных, и более обоснованного предъявления требования к производительности ИВС, критичных к нарушению устойчивости функционирования.

Литература

1. Рыжиков Ю. И. Алгоритмический подход к задачам массового обслуживания: моногр. / Ю. И. Рыжиков. – СПб.: ВКА им. А. Ф. Можайского, 2013. 496 с.

2. Buchholz P. Input Modeling with Phase-Type Distributions and Markov Models. Theory and Applications / P. Buchholz, J. Kriege, I. Felko. – Springer, 2014. 127 p.

3. Рыжиков Ю. И. Итерационный метод расчета многоканальных систем с произвольным законом обслуживания / Ю. И. Рыжиков, А. Д. Хомоненко // Проблемы управления и теории информации. 1980. № 3. С. 203-213.

4. Cox D. R. A use of complex probabilities in theory of stochastic processes / D. R. Cox // Proc. Cambr. Phil. Soc., 1955. Vol. 51, № 2. P. 313-319.

5. Neuts M. F. Matrix-Geometric Solutions in Stochastic Models: an Algorithmic Approach, Chapter 2: Probability Distributions of Phase Type / M. F. Neuts. – Baltimore: Johns Hopkins Univ. Press, 1981. 352 p.

6. Смагин В. А. Об одном методе исследования немарковских систем / В. А. Смагин // Изв. АН СССР. Техническая кибернетика. 1983. № 6. С. 31-36.

7. Бочаров П. П. Методы анализа и расчета систем массового обслуживания с распределениями фазового типа / П. П. Бочаров, В. Г. Литвин // Автоматика и телемеханика. 1986. № 5. С. 5-23.

8. Буранова М. А. Анализ времени ожидания для узла сети типа G/D/1 при неточном знании параметров трафика / М. А. Буранова, В. Г. Карташевский // Информационные технологии и телекоммуникации. 2017. Т. 5, № 1. С. 24-33.

9. Гончаренко В. А. Формальный аппарат представления случайных процессов обслуживания с возмущающими воздействиями и неопределенностью параметров / В. А. Гончаренко // Тр. ВКА им. А. Ф. Можайского. 2015. Вып. 648. С. 13-18.

10. Kingman J. F. C. On doubly stochastic Poisson process / J. F. C. Kingman // Proc. Cambridge Philos. Soc., 1964. Vol. 60, № 4. P. 923-930.

11. Горцев А. М. О связи МС-потоков и МАР-потоков событий / А. М. Горцев, Л. А. Нежельская // Вестн. ТомГУ. Управление, вычислительная техника и информатика. 2011. № 1. С. 13-21.

12. Рыжиков Ю. И. Теория очередей и распределение Парето / Ю. И. Рыжиков // Тр. ВКА им. А. Ф. Можайского. 2015. Вып. 648. С. 28-43.

13. Гончаренко В. А. Анализ реактивности узла вычислительной сети в условиях интервальной неопределенности / В. А. Гончаренко // Изв. вузов. Приборостроение. 2008. № 7. С. 34-39.

14. Кочегаров В. А. Проектирование систем распределения информации. Марковские и немарковские модели / В. А. Кочегаров, Г. А. Фролов. – М.: Радио и связь, 1991. 216 с.

15. Гельфанд И. М. Пространства основных и обобщенных функций. Обобщенные функции / И. М. Гельфанд, Г. Е. Шилов. – М.: Физматгиз, 1958. Вып. 2. 307 с.

16. Гончаренко В. А. Композиционный метод формирования аппроксимационных распределений с произвольной фазовой функцией / В. А. Гончаренко // Труды СПИИРАН. 2016. Вып. 3 (46). С. 212-225.

17. Смагин В. А. О моделировании случайных процессов на основе гипердельтного распределения / В. А. Смагин, Г. В. Филимонихин // Автоматика и вычислительная техника. 1990. № 1. С. 25-31.

18. Смагин В. А. К аппроксимации законов распределений методом производных / В. А. Смагин // Изв. вузов. Приборостроение. 1993. № 2. С. 16-21.

Models and Methods of Queueing Systems Analysis with Parametric Uncertainty

Goncharenko V.A.
Mozhaisky Military Space Academy
St. Petersburg, Russia
vlango@mail.ru

Abstract. **The article discusses an approach to the description of the random processes used in queueing theory to account for the influence of parametric uncertainty of the input data. A method of the representation of probability distributions in the form of duplex composition of integral kernels and the phase function is considered. Methods of calculation of queueing systems under interval uncertainty of parameters of distributions of time between input requests and time of their service are offered.**

Keywords: **randomization, random parameter, parametric uncertainty, integral kernel, generalized function, phase-type distribution, approximation, phase function.**

References

1. Ryzhikov Ju. I. Algorithmic Approach to Queuing Problems [Algoritmicheskij podhod k zadacham massovogo obsluzhivaniya], monogr. St. Petersburg, VKA im. A. F. Mozhajskogo, 2013. 496 p.

2. Buchholz P., Kriege J., Felko I. Input Modeling with Phase-Type Distributions and Markov Models. Theory and Applications. Springer, 2014. 127 p.

3. Ryzhikov Ju. I., Khomonenko A. D. Iterative Method of Calculation of Multichannel Systems with Arbitrary Law of Service [Iteratsionnyj metod rascheta mnogokanal'nyh sistem s proizvol'nym zakonom obsluzhivaniya]. *Problems of Control and Inf. Theory [Problemy upravleniya i teorii informatsii]*, 1980, no. 3, pp. 203-213.

4. Cox D. R. A use of Complex Probabilities in Theory of Stochastic Processes. *Proc. Cambr. Phil. Soc.*, 1955. Vol. 51, no. 2, pp. 313-319.

5. Neuts M. F. Matrix-Geometric Solutions in Stochastic Models: an Algorithmic Approach, Chapter 2: Probability Distributions of Phase Type. Baltimore: Johns Hopkins Univ. Press, 1981. 352 p.

6. Smagin V. A. About one Method of Research of Non-Markovian Systems [Ob odnom metode issledovaniya nemarkovskih sistem]. *Proc. Acad. Sci. USSR [Izvestiya AN SSSR. Tehnicheskaja kibernetika]*, 1983, no. 6, pp. 31-36.

7. Bocharov P. P., Litvin V. G. Analysis and Calculation Methods of Queueing Systems with Phase-type Distributions [Metody analiza i rascheta sistem massovogo obsluzhivaniya s raspredeleniyami fazovogo tipa]. *Automation and Telemechanics [Avtomatika i telemehanika],* 1986, no. 5, pp. 5-23.

8. Buranova M. A., Kartashevskiy V. G. The Analysis of the Latency Period for Knot of Network of the G/D/1 Type at Inaccurate Knowledge of Parameters of the Traffic [Analiz vremeni ozhidaniya dlya uzla seti tipa G/D/1 pri netochnom znanii parametrov trafika]. *Inf. Technol. Telecommunications [Informatsionnye tekhnologii i telekommunikatsii],* 2017, T. 5, no. 1, pp. 24-33.

9. Goncharenko V. A. The Formal Apparatus of Representation of Stochastic Processes of Service with the Disturbance and Uncertainty Parameters [Formal'nyj apparat predstavleniya sluchajnyh protsessov obsluzhivaniya s vozmushchayushchimi vozdejstviyami i neopredelennost'yu parametrov]. *Proc. Mozhaisky Military Aerospace Acad. [Trudy Voenno-kosmicheskoj akademii im. A. F. Mozhajskogo],* 2015, vol. 648, pp. 13-18.

10. Kingman J. F. C. On Doubly Stochastic Poisson Process. *Proc. Cambridge Philos. Soc.*, 1964, vol. 60, no. 4, pp. 923-930.

11. Gortsev A. M., Nezhelskaya L. A. On Relationship of MC-flows and MAP-flows of Events [O svyazi MS-potokov i MAP-potokov sobytij]. *Tomsk State Univ. J. Controland Comput. Sci. [Vestnik Tomskogo gosudarstvennogo universiteta. Upravlenie, vychislitel'naya tekhnika i informatika]*, 2011, no. 1, pp. 13-21.

12. Ryzhikov Y. I. Queuing Theory and the Pareto Distribution [Teoriya ocheredej i raspredelenie Pareto]. *Proc. Mozhaisky Military Aerospace Acad. [Trudy Voenno-kosmicheskoj akademii im. A. F. Mozhajskogo]*, 2015, vol. 648, pp. 28-43.

13. Goncharenko V. A. Analysis of a Reactivity of the Computer Network Node in Conditions of Interval Uncertainty [Analiz reaktivnosti uzla vychislitel'noj seti v usloviyah interval'noj neopredelennosti]. *J. Instrum. Eng. [Izvestiya vuzov. Priborostroenie]*, 2008, no.7, pp. 34-39.

14. Kochegarov V. A., Frolov G. A. Designing of Systems of information Distribution. Markovian and Non-Markovian Models [Proektirovanie sistem raspredelenija informacii. Markovskie i nemarkovskie modeli]. Moscow, Radio i svjaz', 1991. 216 p.

15. Gel'fand I. M., Shilov G. E. Spaces of the Test and Generalized Functions. Generalized Functions 2 [Prostranstva osnovnyh i obobshhennyh funkcij. Obobshhennye funkcii, vyp.2]. Moscow, Fizmatgiz, 1958. 307 p.

16. Goncharenko V. A. Composite Formation Method of Approximating Distributions with an Arbitrary Phase Function [Kompozitsionnyj metod formirovaniya approksimatsionnyh raspredelenij s proizvol'noj fazovoj funktsiej]. *SPIIRAS Proc. [Trudy SPIIRAN]*, 2016, Is. 3 (46), pp. 212-225.

17. Smagin V. A., Filimonihin G. V. About Modelling of Stochastic Processes on a Basis of Hyperdelta Distribution [O modelirovanii sluchajnyh protsessov na osnove giperdel'tnogo raspredeleniya]. *Automation and Computer Eng. [Avtomatika i vychislitel'naja tehnika]*, 1990, no. 1, pp. 25-31.

18. Smagin V. A. To the Approximation of the Laws of Distributions by the Method of Derivatives [K approksimatsii zakonov raspredelenij metodom proizvodnyh]. *J Instrum. Eng. [Izvestiya vuzov. Priborostroenie]*, 1993, no. 2, pp. 16-21.

Управление рисками ИТ-проектов на основе компонентной структуры разрабатываемого программного обеспечения

Титов А. И.
Петербургский государственный университет путей сообщения Императора Александра I
Санкт-Петербург, Россия
titovvvv@rambler.ru

Аннотация. **Рассматриваются распространенные риски ИТ-проектов, приводится обзор методов управления рисками, основные этапы идентификации рисков. Для оценки влияния риска используется вербально-числовая шкала Харрингтона. Описывается агрегирование оценки рисков по каждому компоненту в общую оценку. Рассматривается задача управления идентифицированными рисками и предлагается метод управления рисками, основанный на компонентной структуре разрабатываемого программного обеспечения.**

Ключевые слова: **управление проектами, управление рисками, разработка програмного обеспечения.**

Введение

Реализуемые в сфере информационных технологий проекты (ИТ-проекты) включают в себя большое число используемых технологий, аппаратных средств и специалистов. В больших ИТ-проектах значительно возрастает сложность реализации, а следовательно, возникают многочисленные риски, способные негативно повлиять на результат.

На практике руководители проектов часто отказываются от существующих методов управления рисками, так как их внедрение может усложнить процесс управления проектом.

Кроме того, управление рисками может усложниться при разработке больших информационных систем тем, что составляющие ее модули могут значительно различаться по всем ключевым аспектам: объему задач, применяемым технологиям, задействованным специалистам. Управлять рисками в таких проектах эффективнее по каждому разрабатываемому компоненту отдельно.

Таким образом, можно сформулировать актуальную задачу: выявление рисков, различающихся оценкой для разных компонентов, и выбор метода управления рисками, позволяющего оценивать риски раздельно для каждого компонента и подсчитывать общий риск. При этом используемый метод также должен дополнять их и вписываться в выбранную в проекте методологию разработки ПО.

Обзор рисков ИТ-проектов

Управление рисками как одна из составных частей управления проектами описано в руководствах [1–3]. Применительно к сфере информационных технологий управление рисками описывается в работах, посвященных управлению ИТ-проектами [4–6] и в методологиях разработки ПО [7, 8]. Также большое число исследований сфокусировано на описании рисков, их классификации и ранжировании по степени важности применительно к ИТ-проектам.

В работе одного из наиболее известных исследователей управления ИТ-проектами – Б. Боэма – «Software risk management: principles and practices» [9] приведен список рисков (по убыванию важности) (табл. 1).

Таблица 1

Список рисков и методик их управлением Б. Боэма

№	Риск	Методика управления риском
1	Нехватка компетенций сотрудников	Наем высококвалифицированных сотрудников, мероприятия по формированию команды, обучение сотрудников
2	Нереалистичные сроки и бюджет	Детализация оценки затрат и сроков, разработка повторно используемого ПО, уточнение требований
3	Несоответствие разработанной и требуемой функциональности	Анализ организации, анализ целей, опрос пользователей, прототипирование, оценка производительности, проверка качества
4	Несоответствие разработанного и требуемого пользовательского интерфейса	Прототипирование, разработка сценариев использования, участие пользователей
5	Неэффективное управление требованиями и качеством (Gold-plating)	Уточнение требований, прототипирование, анализ стоимости
6	Постоянный поток изменений требований	Установка ограничений для внесения изменений, итеративность разработки (внесение изменений в следующих итерациях)
7	Недостатки используемых внешних компонентов	Сравнительное тестирование, технический аудит, анализ совместимости
8	Проблемы в задачах, выполняемых внешними подрядчиками	Проверка контрагентов, подготовка макетов и прототипирование, мероприятия по формированию команды
9	Недостаточная производительность	Моделирование, проведение сравнительного тестирования, прототипирование
10	Технологическое отставание	Технический анализ, анализ стоимости, прототипирование

В работе Т. Аддисона перечислены наиболее часто встречающиеся риски [10]:

1) неточность и неконкретность целей ИТ-проекта;
2) недооценка требований ИТ-проекта;
3) невовлеченность пользователей;

4) ошибки в процессе реализации ИТ-проекта;
5) невовлеченность руководства;
6) нереалистичные сроки и бюджет;
7) изменения требований в процессе реализации ИТ-проекта;
8) неэффективное использование методологий проектного управления;
9) знания и умения проектной команды не соответствуют требованиям проекта;
10) завышение качества, неэффективное управление требованиями (Gold-plating).

Для крупных ИТ-проектов, срок реализации которых составляет более года, М. Самнер назвал следующие риски [11]:
1) влияние внешних факторов на проект;
2) нехватка опыта участников проектной команды;
3) нехватка компетенций;
4) неточность целей проекта;
5) изменения требований в процессе реализации ИТ-проекта;
6) неэффективное использование методологий проектного управления;
7) отсутствующая или недостаточная коммуникация с пользователем;
8) нереалистичные сроки и бюджет;
9) конфликт между заинтересованными лицами проекта.

Как можно увидеть из этих списков, в каждом присутствуют несколько наиболее часто встречающихся рисков:
1) неточная оценка сроков и бюджета;
2) расхождение между требуемой реализацией и получившимся результатом;
3) нехватка компетенций и опыта участников проектной команды;
4) проблемы коммуникации с руководством, пользователями, подрядчиками.

Для этих рисков характерно то, что их источниками являются ошибки, допущенные на ранних этапах проекта, а в крупных проектах оценка этих рисков может выполняться отдельно для каждого компонента.

Метод управления рисками ИТ-проекта

Прежде чем перейти к описанию компонентно-ориентированного подхода к оценке рисков, необходимо рассмотреть существующие методологии управления рисками. В большинстве методологий управление рисками включает в себя основные этапы (рис. 1):

1. Идентификация риска

Для идентификации риска имеется большое число методов [12]:
- анализ проектной документации;
- применение метода «блок-схема принятия решения»;
- использование опросных листов;
- применение метода «мозгового штурма»;
- интервьюирование экспертов с опытом решения аналогичных задач.

В рамках решаемой задачи рассматривается управление уже идентифицированными рисками, поэтому подробно методы идентификации в статье не описываются;

2. Анализ риска

Для каждого риска необходимо оценить его вероятность и влияние по 10-балльной шкале. Для увеличения качества

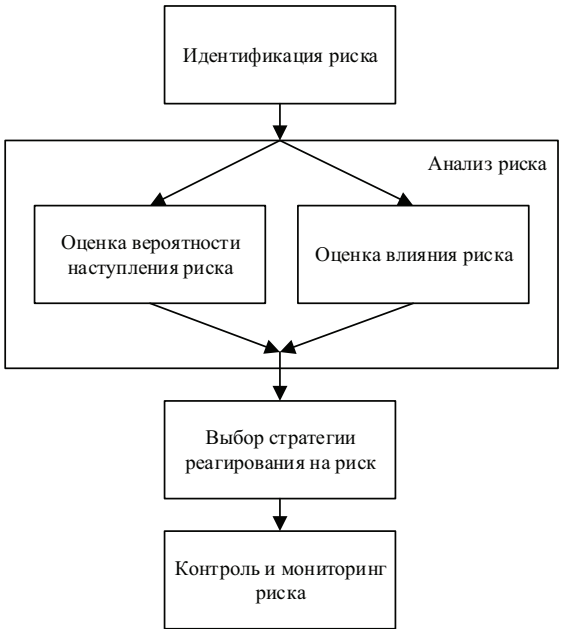


Рис. 1. Основные этапы управления рисками

экспертной оценки можно использовать вербально-числовую шкалу Харрингтона [13] (табл. 2, 3);

Таблица 2

Вербально-числовая шкала Харрингтона для оценки вероятности наступления риска

Степень вероятности наступления риска в проекте	Коэффициент Харрингтона (согласно PMBoK)	Коэффициент Харрингтона	Вероятность
Очень высокая	8–10	5	Риск неизбежен. Гарантированное наступление риска
Высокая	6,4–8	4	Риск вероятен
Средняя	3,7–6,4	3	Нет гарантий, что риск наступит, но все же существует такая возможность
Низкая	2–3,7	2	Есть возможность наступления риска
Очень низкая	0–2	1	Есть потенциальная возможность наступления риска
Нет вероятности	0	0	Риск невозможен

3. Реагирование на риск

Для каждого риска необходимо выбрать способ реагирования, который позволит сократить влияние этого риска на проект. Как правило, в методологиях управления рисками приводятся следующие стратегии работы с рисками:

1) уклонение – полное исключение риска из проекта, которое может вызвать отказ от определенных работ или изменение целей проекта;
2) снижение – вероятности или влияния риска на проект;
3) передача – перенос ответственности за последствия риска на третью сторону (подрядчика, заказчика и т. д.);

4) принятие – формирование плана действий в случае проявления риска либо резерва ресурсов на устранение последствий.

Таблица 3

Вербально-числовая шкала Харрингтона для оценки влияния риска

Степень влияния риска на проект	Коэффициент Харрингтона (согласно PMBoK)	Коэффициент Харрингтона	Влияние
Очень высокая	8–10	5	Остановка работ в проекте
Высокая	6,4–8	4	Выполнение работ в проекте с большим опозданием
Средняя	3,7–6,4	3	Задержки в выполнении работ
Низкая	2–3,7	2	Выполнение работ в проекте с небольшим опозданием
Очень низкая	0–2	1	Незначительные отставания от намеченных планов
Нет влияния	0	0	Выполнение работ согласно плану проекта

После выбора стратегии остается этап контроля и мониторинга, который длится весь проект.

Пример управления рисками на основе компонентной структуры разрабатываемого ПО

В качестве примера рассмотрим проект разработки информационной системы управления проектами (ИСУП) в сфере строительства.

На начальном этапе выполняются приблизительная декомпозиция системы на компоненты, оценка сроков и трудоемкости разработки. Список работ по проекту, выполненный в MS Project, представлен на рис. 2.

На разных этапах проекта оценки риска могут различаться, некоторые риски характеры только для отдельных этапов проекта [14]. Для дальнейшего рассмотрения выберем риск неточной оценки сроков и бюджета, поскольку он относится к наиболее важными рискам и требует мониторинга на протяжении всего проекта.

На основе списка работ составляется оценка рисков для каждого компонента. Для идентифицированных рисков будут использованы обозначения, представленные в табл. 4.

Таблица 4

Выбранные обозначения вероятностей и влияния рисков

Параметр	Обозначение параметра	Риск
Вероятность	x_{limit}	Неточная оценка сроков и бюджета
Влияние	c_{limit}	

Вероятность и влияние риска оцениваются по шкале от 1 до 10 для каждого компонента отдельно. На момент оценки проект находится на ранней стадии, подробное проектирование еще не выполнено, и оценка носит предварительный характер (табл. 5).

Таблица 5

Оценка рисков для каждого компонента на ранних этапах проекта

Компонент	x_{limit}	c_{limit}
Управление содержанием и сроками	2	7
Управление коммуникациями	2	5
Управление ресурсами и стомостью	2	7
Управление закупками	3	4
Обмен план-фактной информацией	4	5
Вывод бизнес-аналитики	5	3

После оценки рисков определяется стратегия реагирования (табл. 6).

По завершении этапа проектирования оценку трудоемкости можно пересчитать на основе полученных данных. Также по окончании этапа проектирования должно быть готово

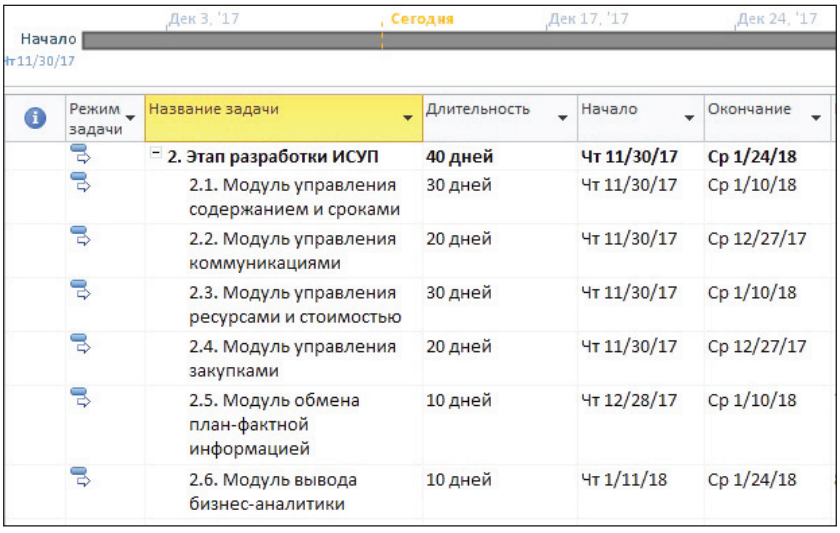


Рис. 2. Список работ по проекту

Таблица 6

Выбор стратегий реагирования на ранних этапах проекта

Компонент	Выбранная стратегия реагирования
Управление содержанием и сроками	Принятие риска
Управление коммуникациями	Принятие риска
Управление ресурсами и стоимостью	Принятие риска
Управление закупками	Снижение риска (увеличение ресурсов для сбора требований)
Обмен план-фактной информацией	Снижение риска (увеличение ресурсов для сбора требований)
Вывод бизнес-аналитики	Снижение риска (увеличение ресурсов для сбора требований)

техническое описание, следовательно, можно скорректировать оценку риска того, что итоговая реализация не будет соответствовать исходным требованиям. На основе полученных данных корректируется оценка рисков (табл. 7).

Таблица 7

Оценка рисков для каждого компонента по завершении проектирования

Компонент	x_{limit}	c_{limit}
Управление содержанием и сроками	4	7
Управление коммуникациями	2	5
Управление ресурсами и стомостью	2	7
Управление закупками	3	4
Обмен план-фактной информацией	4	5
Вывод бизнес-аналитики	8	3

На основе скорректированной оценки рисков можно скорректировать и стратегию управления рисками (табл. 8).

Таблица 8

Выбор стратегий реагирования по завершении проектирования

Компонент	Выбранная стратегия реагирования
Управление содержанием и сроками	Снижение риска. Увеличение ресурсов
Управление коммуникациями	Принятие риска
Управление ресурсами и стоимостью	Принятие риска
Управление закупками	Принятие риска
Обмен план-фактной информацией	Снижение риска. Увеличение ресурсов
Вывод бизнес-аналитики	Передача риска. Привлечение подрядчиков для выполнения работ

В данном примере изменения оценки рисков вызвало изменение стратегии реагирования на риски, но не по всему проекту, а только для тех компонентов, где степень риска возросла.

Оценка рисков для каждого компонента позволяет более гибко управлять разработкой, что крайне важно в больших проектах. Кроме того, такой метод управления рисками имеет низкую трудоемкость и может быть вписан в уже выбранную методологию управления разработкой.

Агрегирование оценки рисков по каждому компоненту в общую оценку

Оценка риска для отдельного компонента позволяет лучше управлять его разработкой, но тогда возникает вопрос, можно ли как-то суммировать риски по отдельным компонентам и получить общую оценку. При незначительном возрастании сроков разработки одного компонента потребуется лишь пропорциональное увеличение ресурсов, что не будет иметь решающего влияния на ход проекта. При более серьезных рисках по одному или нескольким компонентам может нарушиться ход всего проекта. Кроме того, может возникнуть необходимость сравнить важность разных рисков, для чего необходимо иметь численную оценку по каждому риску, поэтому для более целостного похода к управлению рисками необходимо решить задачу агрегирования рисков по каждому компоненту в общую оценку, что требует построения модели.

Среди моделей принятия решений по управлению рисками ИТ-проекта распространены модели на основе нечеткой логики [15–19]. Понятие риска уже включает в себя то, что это некая субъективная оценка, которая может быть выражена не в конкретных числовых значениях, а в определенном множестве значений (например, «низкая», «средняя», «высокая»). Нечеткая логика хорошо подходит для обработки именно таких данных, поскольку позволяет обрабатывать их через лингвистические переменные и функции принадлежности.

Для вычисления общей оценки выбран метод принятия решения на основе алгоритма нечеткого вывода Такаги – Сугено из статьи [20]. В этой статье метод применен для задачи ранжирования и последующего выбора ПО на основе экспертных оценок, но также может быть адаптирован под другие задачи.

Поскольку для оценки рисков определяется такой параметр, как влияние, вместо перебора нечетких правил будет использован предварительно заданный параметр. Дополнительно для каждого компонента вводится параметр значимости, который позволяет управлять весом оценки компонентов относительно друг друга. Таким образом, оценка риска по всем компонентам будет суммироваться по формуле

$$y_i = \sum_{j=1}^{n} x_{ij} \times c_{ij} \times z_j,$$

где n – число компонентов; y_i – суммарная оценка по i-му риску; x_{ij} – оценка вероятности i-го риска в j-м компоненте; c_{ij} – оценка влияния i-го риска в j-м компоненте; z_j – значимость j-го компонента.

Чтобы полученная в результате оценка находилась в диапазоне от 0 до 1, значения параметров x_{ij}, c_{ij}, z_j нормируются

к единице. Для параметра значимости z_j должно выполняться дополнительное условие:

$$\sum_{j=1}^{n} z_j = 1.$$

В табл. 9 приведены значения значимости компонентов, определенные на основе экспертной оценки.

Таблица 9

Оценка значимости компонентов

Компонент	Оценка значимости
Управление содержанием и сроками	0,3
Управление коммуникациями	0,2
Управление ресурсами и стомостью	0,3
Управление закупками	0,1
Обмен план-фактной информацией	0,05
Вывод бизнес-аналитики	0,05

В качестве примера вычисления общей оценки по данному методу будут взяты данные по оценке рисков на раннем этапе проекта и по завершении проектирования. Результат вычислений на раннем этапе (исходные значения параметров x_{ij} и c_{ij} – из табл. 5):

$$y_{\lim it} = \sum_{j=1}^{6} x_{ij} \times c_{ij} \times z_j =$$

$$= 0,2 \times 0,7 \times 0,3 + 0,2 \times 0,5 \times 0,2 + 0,2 \times 0,7 \times 0,3 +$$

$$+ 0,3 \times 0,4 \times 0,1 + 0,4 \times 0,5 \times 0,05 = 0,1335.$$

Результат вычислений по завершении проектирования (исходные значения параметров x_{ij} и c_{ij} – из табл. 7):

$$y_{\lim it} = \sum_{j=1}^{6} x_{ij} \times c_{ij} \times z_j =$$

$$= 0,4 \times 0,7 \times 0,3 + 0,2 \times 0,5 \times 0,2 + 0,2 \times 0,7 \times 0,3 +$$

$$+ \ 0,3 \times 0,4 \times 0,1 + 0,8 \times 0,5 \times 0,05 = 0,18.$$

Из разницы полученных значений оценок можно увидеть, что хотя изменения в оценке риска затронули только два из шести компонентов, результирующая оценка риска возросла, и стратегия реагирования на риск может быть пересмотрена для всего проекта.

Заключение

По результатам исследований предложен подход к управлению рисками ИТ-проекта на основе компонентной структуры разрабатываемого ПО. Этот подход позволяет использовать управление рисками в распространенных методологиях разработки ПО, таких как RUP и MSF, за счет оценивания рисков для проекта, декомпозированного на компоненты. Также предложен вариант объединения оценки риска по компонентам в общую оценку для проекта, что позволяет более гибко выбирать стратегию реагирования на риск, применяя ее для части проекта или для проекта целиком.

Дальнейшие исследования целесообразно продолжить в направлении практического применения предложенного подхода с большим числом реальных проектов и более широким охватом рассматриваемых рисков.

Литература

1. Руководство к своду знаний по управлению проектами (Руководство PMBOK. Russian). 2014. 589 с.
2. Арчибальд Р. Д. Управление высокотехнологичными программами и проектами / Р. Д. Арчибальд. – М.: ДМК-Пресс, 2002. 472 с.
3. Новиков Д. А. Управление проектами: организационные механизмы / Д. А. Новиков. – М.: ПМСОФТ, 2007. 140 с.
4. Архипенков С. Я. Лекции по управлению программными проектами / С. Я. Архипенков. – М., 2009. 127 с.
5. Фатрелл Р. Т. Управление программными проектами. Достижение оптимального качества при минимуме затрат / Р. Т. Фатрелл, Д. Ф. Шафер, Л. И. Шафер; пер. с англ. – М.; СПб.; Киев: Вильямс, 2004. 1136 с.
6. Соммервилл И. Инженерия программного обеспечения / И. Соммервилл. – М.: Вильямс, 2002. 624 с.
7. Крачтен Ф. Введение в Rational Unified Process / Ф. Крачтен. – М.: Вильямс, 2002. 240 с.
8. Тернер М. Основы Microsoft Solution Framework / М. Тернер. – М.: Русская редакция; СПб.: Питер, 2008. 336 с.
9. Boehm B. W. Software risk management: principles and practices / B. W. Boehm // IEEE software. 1991. Т. 8, № 1. С. 32-41.
10. Addison T. Controlling Software Project Risks – An Empirical Study of Methods Used by Experienced Project Managers / T. Addison, S. Vallabh // Proc. SAICSIT. 2002. P. 128-140.
11. Sumner M. Risk Factors in Enterprise-wide/ERP Projects / M. Sumner // J. Inf. Technol. 2000. № 15. P. 317-327.
12. Дайбова К. Е. Разработка инструментария оперативной идентификации рисков в ИТ-проектах / К. Е. Дайбова, В. С. Николаенко // Ресурсоэффективным технологиям – энергию и энтузиазм молодых: сб. науч. тр. VI всерос. конф. – Томск: Изд-во Томск. политех. ун-та, 2015. С. 254-257.
13. Николаенко В. С. Внедрение риск-менеджмента в ИТ-проекты / В. С. Николаенко // Гос. управление. Электрон. вестн. 2016. № 54. С. 63-88.
14. Đurković O. Risks in Information Systems Development Projects / O. Đurković, L. Raković // Management. 2009. Т. 4, № 1. С. 13-19.
15. Булдакова Т. И. Оценка информационных рисков в автоматизированных системах с помощью нейро-нечёткой модели / Т. И. Булдакова, Д. А. Миков // Наука и образование: науч. изд. МГТУ им. Н. Э. Баумана. 2013. № 11. С. 295-310.
16. Ехлаков Ю. П. Нечеткая модель оценки рисков продвижения программных продуктов / Ю. П. Ехлаков, Н. В. Пермякова // Бизнес-информатика. 2014. № 3 (29). С. 69-78.
17. Карпеев Д. О. Идентификация параметров нечетких моделей оценки информационных рисков информационных систем / Д. О. Карпеев и др. // Информация и безопасность. 2010. Т. 13, № 1. С. 37-42.
18. Lee H. M. A new algorithm for applying fuzzy set theory to evaluate the rate of aggregative risk in software development / H. M. Lee et al. // Inf. Sci. 2003. Т. 153. С. 177-197.
19. Chen S. M. Fuzzy group decision making for evaluating the rate of aggregative risk in software development / S. M. Chen // Fuzzy Sets and Systems. 2001. Т. 118, № 1. С. 75-88.
20. Титов А. И. Выбор программного обеспечения с помощью алгоритма Такаги – Сугено на примере систем управления проектами / А. И. Титов, А. Д. Хомоненко // Научно-технические ведомости СПбГПУ. Информатика. Телекоммуникации. Управление. 2016. № 1 (236). С. 41-52.

Risk Management for Software Projects Based on the Component Structure

Titov A. I.
Emperor Alexander I St. Petersburg State Transport University
Saint-Petersburg, Russia
titovvvv@rambler.ru

Abstract. **Widespread risks of IT projects are considered, the review of methods of management of risks is provided. The main stages of identification of risks are given. For an impact assessment of risk the verbal and numerical scale of Harrington is used. Aggregation of assessment of risks on each component in the general assessment is described. The task of control of the identified risks is considered and the method of management of risks based on component structure of the developed software is offered.**

Keywords: **project management, risk management, software development.**

References

1. A Guide to the Project Management Body of Knowledge (RMVOK Guide) [Rukovodstvo k svodu znaniy po upravleniyu proyektami (Rukovodstvo PMBOK. Russian)]. 2014. 589 p.

2. Archibald R. D. Managing High-Technology Programs and Projects [Upravlenie vysokotekhnologichnymi programmami i proektami], Moscow, DMK-Press, 2002. 472 p.

3. Novikov D. A. Project Management: Organizational Mechanisms [Upravlenie proektami: organizacionnye mekhanizmy], Moscow, PMSOFT, 2007. 140 p.

4. Arhipenkov S. Ja. Software Project Management Lectures [Lekcii po upravleniju programmnymi proektami], Moscow, 2009. 127 p.

5. Fatrell R. T., Shafer D. F., Shafer L. I. Quality Software Project Management First Edition [Upravlenie programmnymi proektami. Dostizhenie optimal'nogo kachestva pri minimume zatrat], Moscow, St. Petersburg, Kiev: Vil'jams, 2004. 1136 p.

6. Sommerville I. Software Engineering [Inzheneriya programmnogo obespecheniya], Moscow, Vil'jams. 2002. 624 p.

7. Kruchten Ph. The Rational Unified Process: An Introduction [Vvedenie v Rational Unified Process], Moscow, Vil'jams. 2002. 240 p.

8. Turner M. S. V. Microsoft Solutions Framework Essentials [Osnovy Microsoft Solution Framework], Moscow, Russkaja redakcija; St. Petersburg, Piter, 2008. 336 p.

9. Boehm B. W. Software Risk Management: Principles and Practices, *IEEE Software*, 1991, T. 8, no. 1, pp. 32-41.

10. Addison T., Vallabh S. Controlling Software Project Risks – An Empirical Study of Methods Used by Experienced Project Managers. *Proc. SAICSIT*, 2002. Pp. 128-140.

11. Sumner M. Risk Factors in Enterprise-wide/ERP Projects, *J. Inf. Technol.*, 2000, no. 15, pp. 317-327.

12. Dajbova K. E., Nikolaenko V. S. Development of Tools for Rapid identification of Risks in IT Projects [Razrabotka instrumentariya operativnoj identifikacii riskov v IT-proektah]. *Resource-efficient technologies – energy and enthusiasm of young people: a collection of scientific papers of the VI All-Russian Conf. [Resursoehffektivnym tekhnologiyam – ehnergiyu i ehntuziazm molodyh: sbornik nauchnyh trudov VI vserossijskoj konferencii]*. Tomsk: Izdatelstvo Tomskogo politekhnicheskogo universiteta, 2015. Pp. 254-257.

13. Nikolaenko V. S. Introduction of Risk Management in IT Projects [Vnedrenie risk-menedzhmenta v IT-proekty], *Public administration. Electronic Bul. [Gosudarstvennoe upravlenie. EHlektronnyj Vestnik]*, 2016, no. 54, pp. 53-88.

14. Đurković O., Raković L. Risks in Information Systems Development Projects, *Management*, 2009, T. 4, no. 1, pp. 013-019.

15. Buldakova T. I., Mikov D. A. Assessment of information Risks in Automated Systems with the Help of a Neuro-fuzzy Model [Ocenka informacionnyh riskov v avtomatiziro-vannyh sistemah s pomoshch'yu nejro-nechyotkoj modeli], *Sci. and Educ. [Nauka i obrazovanie]*. Moscow Bauman State Tech. Univ., 2013, no. 11, pp. 295-310.

16. Ekhlakov Yu. P., Permyakova N. V. Fuzzy Model for Assessing the Risks of Promoting Software Products [Nechetkaya model' ocenki riskov prodvizheniya programmnyh produktov], *Business Informatics [Biznes-informatika]*, 2014, no. 3 (29), pp. 69-78.

17. Karpeev D. O. et al. Identification of Parameters of Fuzzy Models for Assessing the Information Risks of Information Systems [Identifikaciya parametrov nechetkih modelej ocenki informacionnyh riskov informacion-nyh sistem], *Information and security [Informaciya i bezopasnost']*, 2010, T. 13, no. 1, pp. 37-42.

18. Lee H. M. et al. A New Algorithm for Applying Fuzzy Set Theory to Evaluate the Rate of Aggregative Risk in Software Development, *Inf. Sci.*, 2003, T. 153, pp. 177-197.

19. Chen S. M. Fuzzy Group Decision Making for Evaluating the Rate of Aggregative Risk in Software Development, *Fuzzy Sets and Systems*, 2001, T. 118, no. 1, pp. 75-88.

20. Titov A. I., Khomonenko A. D. Software Selection by Using Takagi – Sugeno Algorithm on Example Project Management System [Vybor programmnogo obespecheniya s pomoshch'yu algoritma takagi-sugeno na primere sistem upravleniya proektami], *St. Petersburg State Polytechnical Univ. J. Comput. Sci. Telecommunication and Control Systems [Nauchno-tekhnicheskie vedomosti SPbGU. Informatika. Telekommunikacii. Upravlenie]*, 2016, no. 1 (236), pp. 41-52.

Комплекс программ оценивания надежности и планирования разработки программных средств на основе динамических моделей

Данилов А. А.
ООО «Нокиа Солюшенз энд Нетвокс»
Санкт-Петербург, Россия
andrey.danilov.aad@mail.ru

Аннотация. **Разработан комплекс программ для вычисления вероятностных показателей процессов испытаний и состояния программных средств: вероятности пребывания системы в определённых состояниях, функции распределения времени обнаружения и устранения ошибок, математические ожидания случайных величин, количество обнаруженных или устраненных ошибок. Известные модели испытаний программных средств не учитывают вероятностный характер нахождения и исправления ошибок. Комплекс построен на усовершенствованных численных моделях отладки программ и учитывает вероятности обнаружения ошибок для каждого модуля при тестировании, а также состоятельность (мощность) используемых тестов. Использование комплекса при планировании сокращает сроки и затрат на разработку программных средств при обеспечении необходимых показателей качества и надежности. Он позволяет планировать необходимые ресурсы для достижения заданных показателей качества, сравнивать стратегии тестирования и выбирать лучшую из них с учётом особенностей конкретной стадии жизненного цикла программ с учётом вычислительных, экономических, временны́х, квалификационных и других возможностей.**

Ключевые слова: **модель, программные средства, ошибка, вероятность, стратегия испытаний, граф.**

Введение

Информационные технологии в современном мире используются во всех сферах деятельности для повышения производительности и улучшения качества. Требования к надежной и безопасной работе программных средств (ПС) неуклонно повышаются. Отказы ПС могут приводить к большим экономическим потерям, а порой – и к катастрофическим последствиям. Экономические затраты на проекты должны укладываться в заранее определенные рамки. Несоблюдение сроков поставок приводит к штрафным санкциям для организаций, разрабатывающих ПС. Эти важные аспекты нашли отражение во всех современных стандартах разработки ПС – как российских, так и международных.

Сокращение затрат и сроков на разработку ПС и обеспечение их качества (надежности) могут быть достигнуты за счет использования не только более совершенных технологий, среды разработки и средств автоматизации тестирования (отладки), но и грамотного и эффективного планирования работ и разделения ресурсов при создании ПС.

Для решения этих задач могут быть использованы средства математического моделирования надежности ПС и процессов их разработки (отладки). К настоящему времени создано большое количество моделей для оценивания и предсказания надежности ПС на различных этапах их жизненного цикла. Подробный обзор и описание таких моделей дан в [1–3].

Все известные модели в совокупности имеют ряд недостатков, ограничивающих их использование: модели не обладают достаточной общностью (универсальностью); описывают процессы обнаружения, но не устранения ошибок, что делает невозможным их применение собственно для планирования испытаний; моделируют процессы обнаружения и устранения всех прогнозируемых ошибок, хотя не все эти ошибки могут быть допущены (найдены) с единичной вероятностью, т. е. модели не учитывают вероятностный характер обнаружения ошибок и состоятельность (мощность) используемых тестов [4–6].

Цель данной работы – создание комплекса программ, в котором предусматривается возможность учитывать вероятностные параметры обнаружения ошибок при тестировании программ или состоятельность используемых тестов.

Программный комплекс

Программный комплекс оценивания надежности и планирования построен на базе усовершенствованных динамических моделей. Процесс обнаружения ошибок аппроксимируется экспоненциальным законом, а процесс устранения может аппроксимироваться экспоненциальным двухэтапным неоднородным распределением Эрланга или двухфазным обобщенным распределением Кокса. Процесс отладки программ после аппроксимации представляется Марковской системой обслуживания с дискретным множеством состояний и непрерывным временем. Предусмотрена возможность использования вероятностей обнаружения ошибок для каждого модуля при их тестировании.

На базе модифицированных размеченных графов составляются системы дифференциальных уравнений, решение которых позволяет вычислить вероятностные показатели процессов испытаний и состояния программных средств. Задав начальные условия к системе уравнений, можно найти численное решение соответствующей задачи Коши для произвольного значения времени и вычислить вероятностные показатели. Решение уравнений целесообразно выполнять методом Рунге – Кутты. Для построения комплекса использовались подходы, рассмотренные в [7, 8]. При этом обеспечиваются приемлемые характеристики устойчивости и точности решения, обусловленные тем, что при используемом

методе нумерации состояний соответствующие матрицы состояний являются нижними треугольными. Программный комплекс создан с использованием среды MATLAB.

Исходные данные

Для каждой модели определяются исходные данные. Некоторые из них одинаковы для всех моделей, другие являются специфичными для конкретной модели.

Исходные данные для расчета надежности: общее число ошибок, начальные моменты распределений длины временны́х интервалов обнаружения и исправления ошибок (в зависимости от используемой модели задаются от одного до трех начальных моментов), вероятности обнаружения ошибок и граф переходов между состояниями. Используя рассчитанные показатели надежности и данные о структуре ПС, оценивают надежность отдельных модулей и всего ПС, обоснуют стратегии и планирование испытаний многомодульных ПС.

Одинаковые исходные данные для всех моделей:

- предполагаемое количество ошибок;
- средняя длительность интервалов времени тестирования для каждой ошибки;
- значения вероятностей обнаружения ошибок.

При задании исходных данных для таких моделей распространенным подходом является использование собранной статистики уже завершенных проектов. Однако для учета особенностей конкретного проекта широко применяются программные метрики, характеризующие программный продукт (его структуру, сложность, интерфейсы, факторы разработки и др.). Так, с точки зрения современного объектно-ориентированного программирования целесообразно использовать наборы метрик Чайдамбера – Кемерера и Бансия – Дэвиса [9, 10]. Значения метрик собираются из документов проектирования. На основе полученных метрик решается задача классификации модулей. Так, вероятность наличия ошибки в модуле ω_i можно оценить с использованием логистической регрессии и выразить формулой

$$\omega_i = 1/(1+e^{-(\beta_0+\sum\beta_j x_j)}),$$

где β_j – параметры логистической регрессии, которые определяются методом максимального правдоподобия; x_j – значение метрики сложности.

Для моделей с экспоненциальной аппроксимацией процесса устранения необходимо определить длительность интервалов времени исправления ошибок. При использовании распределений Эрланга и Кокса для аппроксимации процесса устранения определяют интенсивности экспоненциальных фаз.

Двухэтапное неоднородное (обобщенное) распределение Эрланга предполагает последовательное прохождение двух экспоненциальных фаз с интенсивностями μ_1 и μ_2. Для корректной аппроксимации случайной произвольной величины двухэтапным распределением Эрланга необходимо, чтобы первые два момента распределений совпадали. Тогда система уравнений принимает вид

$$\begin{cases} \dfrac{1}{\mu_1}+\dfrac{1}{\mu_2}=f_1; \\ \dfrac{1}{\mu_1^{\,2}}+\dfrac{1}{\mu_1\mu_2}+\dfrac{1}{\mu_2^{\,2}}=f_2, \end{cases} \qquad (1)$$

где $f_i = g_i / i!$; $i = 1, 2$; g_i – i-й начальный момент исходного распределения. Решая систему уравнений (1), получим

$$\mu_{1,2} = \frac{f_1 \pm \sqrt{4f_2 - 3f_1^{\,2}}}{2(f_1^{\,2} - f_2)}. \qquad (2)$$

Из (2) следует, что параметры являются вещественными при аппроксимации исходной плотности с коэффициентом вариации $1/\sqrt{2} \le \nu < 1$. При использовании аппроксимации в диапазоне $0 \le \nu < 1/\sqrt{2}$ целесообразно использовать комплексно сопряженные параметры $\mu_1 = \alpha + j\beta$, $\mu_2 = \alpha - j\beta$. Из (2) находим:

$$\alpha = f_1/2(f_1^{\,2} - f_2),\ \ \beta = \sqrt{3f_1^{\,2} - 4f_2}\,/2(f_1^{\,2} - f_2).$$

Параметры аппроксимирующего распределения могут быть вещественными или комплексно сопряжёнными, при этом вероятности состояний исследуемой системы являются вещественными. Таким образом, для распределения Эрланга необходимо определить два первых момента аппроксимируемого распределения.

Дополнительно для распределения Кокса находят вероятность (после прохождения первой фазы) продолжения или завершения процесса. Двухфазное распределение Кокса представляет собой смесь двух экспоненциальных фаз с интенсивностями μ_1 и μ_2. При этом после прохождения первой фазы с некоторыми вероятностями p и $1 - p = p'$ выбираются продолжение (следующая фаза) или завершение процесса. Для получения параметров аппроксимирующего распределения C_2 используется система уравнений

$$\begin{cases} p = \mu_2(f_1\mu_1 - 1)/\mu_1; \\ \mu_1 = (\mu_2 f_1 - 1)/(\mu_2 f_2 - f_1); \\ \mu_2 = (f_1 f_2 - f_3 \pm \sqrt{D})/(2(f_2^2 - f_1 f_3)), \end{cases}$$

где $D = (f_1 f_2 - f_3)^2 - 4(f_2^2 - f_1 f_3)(f_1^2 - f_2)$; $f_i = g_i / i!$; $i = \overline{1,3}$; g_i – i-й начальный момент исходного распределения. Эти параметры тоже могут быть вещественными или комплексно сопряженными, при этом вероятности состояний исследуемой системы являются вещественными. Для распределения Кокса необходимо определить три первых момента исходного распределения.

Матрицы индексации состояний

Для каждой модели формируются матрицы индексации состояний. Для моделей с экспоненциальной аппроксимацией процесса устранения матрицы индексации состояний двумерные, а для аппроксимаций Эрланга и Кокса – трехмерные. Матрицы индексации состояний используются для решения системе уравнений методом Рунге – Кутты.

Моделирование динамических систем. Матрицы индексаци состояний

Для каждой модели формируются матрицы индексации состояний. Для моделей с экспоненциальной аппроксимацией процесса устранения матрицы индексации состояний двумерные, а для аппроксимаций Эрланга и Кокса – трехмерные. Матрицы индексации состояний используются для решения системе уравнений методом Рунге – Кутты.

Для моделирования сложных динамических систем используется функция ode45 среды MATLAB. Эта функция использует формулы Рунге – Кутты 4-го и 5-го порядков. На вход ode45 передаются функции для вычисления правых частей систем дифференциальных уравнений, интервал интегрирования и вектор начальных условий. Вектора начальных условий задаются в виде:

• для моделей с экспоненциальной аппроксимацией процесса устранения –

$$P_{i,j}(0)=\begin{cases}1, \text{ если } i+j=0;\\ 0, \text{ если } i+j\neq 0;\end{cases}$$

• для моделей с аппроксимацией Эрланга и Кокса процесса устранения –

$$P_{i,k,j}(0)=\begin{cases}1, \text{ если } i+k+j=0;\\ 0, \text{ если } i+k+j\neq 0.\end{cases}$$

Основные характеристики моделей находятся по следующим формулам.

Вероятность $Ri(t)$ того, что в процессе испытаний было найдено ровно i ошибок (сумма найденных, но не исправленных и устраненных ошибок):

• для моделей с экспоненциальной аппроксимацией процесса устранения

$$R_i(t)=\sum_{j=0}^{i}P_{i-j,j}(t), i=\overline{0,N};$$

• для моделей с аппроксимацией Эрланга и Кокса процесса устранения

$$R_i(t)=\sum_{j=0}^{i}P_{i-j,0,j}(t)\ +\sum_{j=1}^{i}P_{i-j+1,1,j-1}(t).$$

Вероятность $Pj\ (t)$ того, что в процессе испытаний было устранено (исправлено или отсутствовало) ровно j ошибок:

• для моделей с экспоненциальной аппроксимацией процесса устранения

$$P_j(t)=\sum_{i=0}^{N-j}P_{i,j}(t),\ j=\overline{0,N};$$

• для моделей с аппроксимацией Эрланга и Кокса процесса устранения

$$P_j(t)=\sum_{i=0}^{N-j}P_{i,0,j}(t)+\sum_{i=1}^{N-j}P_{i,1,j}(t).$$

Математическое ожидание числа найденных ошибок

$$N_R(t)=\sum_{i=1}^{N}iR_i(t).$$

Математическое ожидание числа устраненных ошибок

$$N_P(t)=\sum_{j=1}^{N}jP_j(t).$$

Соответственно, среднее число $N_{RL}(t)$ ошибок, не обнаруженных к моменту времени t, и среднее число $N_{PL}(t)$ ошибок, не устраненных к моменту времени t, определяются по формулам

$$N_{RL}=N-N_R(t);$$

$$N_{PL}=N-N_P(t).$$

Функция $Fi\ (t)$ распределения времени устранения не менее i ошибок

$$F_i(t)=\sum_{l=i}^{N}P_l(t), i=\overline{0,N}.$$

Модель позволяет оценить время отладки, которое требуется, чтобы устранить $N_{\text{ТР}}$ ошибок с заданной вероятностью $P_{\text{ТР}}$, как

$$T_{N_{\text{ТР}},P_{\text{ТР}}}=t\,|\,F_{N_{\text{ТР}}}(t)\geq P_{\text{ТР}}.$$

Примеры вычислений

Для всех стратегий расчет выполнен при следующих исходных данных. Предполагается, что изначально в ПС содержится $N = 10$ ошибок со средней длительностью интервалов тестирования, соответственно, 0,3; 0,3; 0,3; 0,7; 0,7; 1; 2; 3; 5; 10 ч. Длительность интервала исправления ошибок равна 3 часам. Значения вероятностей обнаружения ошибок $\omega_i,\ i=\overline{1,N}$ указываются непосредственно на графиках и в таблицах, так как этот параметр для данной работы представляет наибольший интерес. Некоторые результаты расчетов приведены для примера.

Стратегия 0. Обнаруженные ошибки устраняются последовательно по мере их выявления, а тестирование во время исправления найденных ошибок не приостанавливается. Время устранения всех обнаруженных ошибок распределено по экспоненциальному закону [11]. Матрица индексации состояний представлена на рис. 1.

1	2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	21	0
22	23	24	25	26	27	28	29	30	0	0
31	32	33	34	35	36	37	38	0	0	0
39	40	41	42	43	44	45	0	0	0	0
46	47	48	49	50	51	0	0	0	0	0
52	53	54	55	56	0	0	0	0	0	0
57	58	59	60	0	0	0	0	0	0	0
61	62	63	0	0	0	0	0	0	0	0
64	65	0	0	0	0	0	0	0	0	0
66	0	0	0	0	0	0	0	0	0	0

Рис. 1. Матрица индексации для стратегии 0

Стратегия 1. Этап тестирования продолжается, пока не будут определены все отсутствующие и обнаружены имеющиеся ошибки. Затем выявленные ошибки исправляют. Время устранения всех обнаруженных ошибок распределено по экспоненциальному закону с интенсивностью μ. Это подробно рассмотрено в [11]. Матрица индексации состояний эквивалентна матрице для нулевой стратегии. На рис. 2 представлены графики функций распределения времени (ФРВ) устранения не менее i ($i = 5, 10$) ошибок для стратегии 1.

Стратегия 2. Этап тестирования продолжается, пока не будет обнаружена очередная ошибка или не будет определено ее отсутствие. После обнаружения ошибки тестирование приостанавливается, ошибка исправляется. После исправления ошибки или её необнаружения вновь начинается тестирование. Время устранения всех обнаруженных ошибок распределено по экспоненциальному закону [11]. Матрица индексации состояний представлена на рис. 3.

Стратегия 3. Этап тестирования продолжается, пока не будет обнаружено или не будет определено отсутствие N_x первичных ошибок, вместе взятых (ошибок первого, блокирующего пакета). После этого тестирование приостанавливается, обнаруженные первичные ошибки полностью исправляются с интенсивностью μ_1. Затем таким же образом продолжается отладка для вторичных ошибок (второго пакета), а найденные ошибки исправляют с интенсивностью μ_2. Вре-

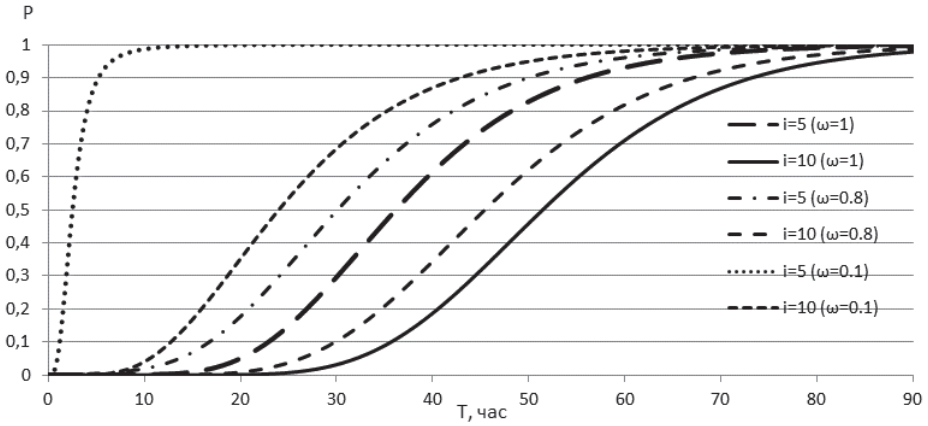


Рис. 2. ФРВ для стратегии 1

1	2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	21	0

Рис. 3. Матрица индексации состояний для стратегии 2

1	2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	0	17	18	19	20	0
21	22	23	24	0	0	25	26	27	0	0
28	29	30	0	0	0	31	32	0	0	0
33	34	0	0	0	0	35	0	0	0	0
36	0	0	0	0	0	37	0	0	0	0

Рис. 4. Матрица индексации для стратегии 3

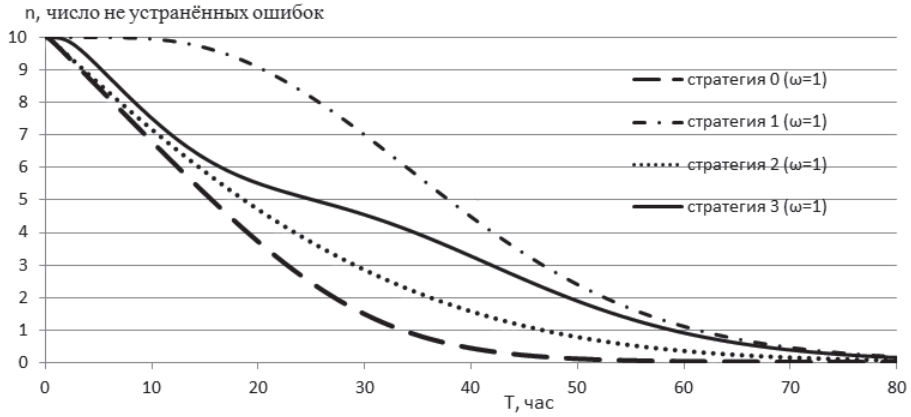


Рис. 5. Сравнение стратегий 0–3 при ω = 1

мя устранения всех обнаруженных ошибок распределено по экспоненциальному закону [11]. Матрица индексации состояний представлена на рис. 4.

Сравнение стратегий 0–3 при ω = 1 представлено на рис. 5.

Стратегия 4. Обнаруженные ошибки устраняются последовательно по мере их выявления, а тестирование во время исправления найденных ошибок не приостанавливается. Произвольное распределение времени устранения всех ошибок аппроксимируется двухэтапным неоднородным распределением Эрланга [12]. Матрица индексации состояний представлена на рис. 6, 7.

Стратегия 5. Этап тестирования продолжается, пока не будет обнаружена очередная ошибка или не будет определено ее отсутствие. После обнаружения ошибки тестирование приостанавливается, ошибка исправляется. После исправления ошибки или её необнаружения вновь начинается тестирование. Произвольное распределение времени устранения всех ошибок аппроксимируется двухэтапным неоднородным распределением Эрланга [12]. Матрица индексации состояний представлена на рис. 8, 9.

Стратегия 6. Этап тестирования продолжается, пока не будут определены все отсутствующие и обнаружены имею-

1	2	3	4	5	6	7	8	9	10	11
22	23	24	25	26	27	28	29	30	31	0
41	42	43	44	45	46	47	48	49	0	0
58	59	60	61	62	63	64	65	0	0	0
73	74	75	76	77	78	79	0	0	0	0
86	87	88	89	90	91	0	0	0	0	0
97	98	99	100	101	0	0	0	0	0	0
106	107	108	109	0	0	0	0	0	0	0
113	114	115	0	0	0	0	0	0	0	0
118	119	0	0	0	0	0	0	0	0	0
121	0	0	0	0	0	0	0	0	0	0

Рис. 6. Первая страница матрицы индексации 4

12	13	14	15	16	17	18	19	20	21	0
32	33	34	35	36	37	38	39	40	0	0
50	51	52	53	54	55	56	57	0	0	0
66	67	68	69	70	71	72	0	0	0	0
80	81	82	83	84	85	0	0	0	0	0
92	93	94	95	96	0	0	0	0	0	0
102	103	104	105	0	0	0	0	0	0	0
110	111	112	0	0	0	0	0	0	0	0
116	117	0	0	0	0	0	0	0	0	0
120	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0

Рис. 7. Вторая страница матрицы индексации 4

1	2	3	4	5	6	7	8	9	10	11
22	23	24	25	26	27	28	29	30	31	0

Рис. 8. Первая страница матрицы индексации 5

12	13	14	15	16	17	18	19	20	21	0
0	0	0	0	0	0	0	0	0	0	0

Рис. 9. Вторая страница матрицы индексации 5

щиеся ошибки. Затем выявленные ошибки исправляют [13]. Произвольное распределение времени устранения ошибок аппроксимируется распределением Кокса.

Стратегия 7. Этап тестирования продолжается, пока не будет обнаружена очередная ошибка или не будет определено ее отсутствие. После обнаружения ошибки тестирование приостанавливается, ошибка исправляется. После исправления ошибки или её необнаружения вновь начинается тестирование. Произвольное распределение времени устранения ошибок аппроксимируется распределением Кокса [13]. Матрица индексации состояний эквивалентна матрице для пятой стратегии.

Для стратегий 6 и 7 получены данные о зависимости вероятности исправления всех $N = 10$ ошибок от разных значений коэффициента вариации v распределения интервалов времени устранения ошибок. Эти данные позволили рассчитать значения требуемого времени отладки по заданной вероятности при $v = 0{,}25; 0{,}5; 0{,}75; 1{,}0$, которые представлены в таблице. Расчеты показывают, что переход от экспоненциальной модели надежности ПС к неэкспоненциальным дает преимущество в точности прогноза.

Расчет времени отладки по вероятности отсутствия ошибок для стратегий 6 и 7

Вероятность отсутствия ошибки	Требуемое время отладки, ч		
	Значения коэффициента вариации		
	$v = 0{,}5$	$v = 0{,}75$	$v = 1{,}0$
Стратегия 6			
0,8	54,8	55,6	56,5
0,9	62,2	63,1	64,5
0,95	69,4	70,4	71,7
0,99	85,6	86,9	88,5
Стратегия 7			
0,8	54,9	55,4	56,4
0,9	62,3	63,2	64,4
0,95	69,2	70,2	71,6
0,99	85,5	86,6	88,4

Стратегия 8. Обнаруженные ошибки устраняются последовательно по мере их выявления, а тестирование во время исправления найденных ошибок не приостанавливается. Произвольное распределение времени устранения ошибок аппроксимируется распределением Кокса [14]. Матрица индексации состояний эквивалентна матрице для четвертой стратегии.

Основные программные модули

Main – основная функция, готовит исходные данные, обращается к функции SystemCalculation для решения системы дифференциальных уравнений и представляет результаты (графики, выходные данные).

StatesIndexMatrix создает матрицы индексации состояний. Параметры – стратегия и количество ошибок.

ErlangFactors, CoxFactors – функции расчета параметров аппроксимации методами Эрланга и Кокса. Параметры – начальные моменты исходного распределения.

IndexToState вычисляет номер состояния системы по индексам состояния модели. Параметры – индексы состояния модели.

DifferentialEquations – система дифференциальных уравнений. Параметры: векторы интенсивностей обнаружения и исправления ошибок, время моделирования, вектор вероятностей состояний системы в текущий момент времени.

ProbabilityProfile – функция расчета вероятностных характеристик и показателей надежности. Параметры – вектор вероятностей пребывания системы в различных состояниях.

SystemCalculation – функция решения системы дифференциальных уравнений (вызов функций ode45 и DifferentialEquations) и расчета показателей надежности (вызов функции ProbabilityProfile).

Обоснование достоверности расчетов

Для проверки достоверности полученных результатов использовали ручную проверку и взаимную проверку моделей.

Ручную проверку проводили путем составления минимальных (рассматривали только две ошибки) систем дифференциальных уравнений и их решения с использованием функции ode45 напрямую. Полученные результаты сравнивали с результатами программного комплекса для соответствующих входных данных.

Взаимная проверка заключалась в сравнении результатов, полученных для более общих моделей, с результатами расчета частных моделей. Схема выполнения взаимной проверки результатов моделирования иллюстрируется на рис. 10.

Рис. 10. Схема взаимной проверки моделей

Подробно схема представлена в [7]. Реализованные модели показаны по степени общности от базовой экспоненциальной до наиболее общей с использованием двухэтапного распределения Кокса. Взаимная проверка моделей показала совпадение полученных результатов.

Заключение

Использование в предложенных моделях оценки надежности для каждого модуля, с одной стороны, повышает точность моделирования процессов отладки ПС, с другой

стороны, модели позволяют учитывать состоятельность тестов, используемых для отладки ПС. Это дает возможность искать пути повышения характеристик надёжности ПС формированием тестов, обнаруживающих ошибки с высокой вероятностью.

Аппроксимация произвольных законов распределения интервалов времени исправления ошибок распределением Кокса обобщает известные Марковские модели, повышает точность моделирования и делает предложенные модели более универсальными. Предложенные модели целесообразно использовать для оценивания текущего уровня надежности ПС и прогнозирования динамики их изменения в процессе испытаний на различных этапах жизненного цикла. Предложенные нестационарные модели позволяют выбрать наилучшую стратегию испытаний ПС исходя из наличия или отсутствия необходимых ресурсов, времени и статистических данных, а также распределить работу групп тестеров и разработчиков.

Разработанный программный комплекс позволяет автоматизировать оценку показателей надежности программ и планирование испытаний для различных стратегий тестирования.

Литература

1. Moranda P. Final Report on Software Reliability Study / P. Moranda, Z. Jelinski. McDonnell Douglas Astronautics Co., MADC Report Number 63921, 1972.

2. Musa J. D. Software Reliability: Measurement, Prediction, Application / J. D. Musa, A. Iannino, K. Okumoto. – NY: McGraw-Hill, 1987.

3. Littlewood B. The Littlewood-Verrall model for software reliability compared with some rivals / B. Littlewood // J. Syst. Softw. 1980. Vol. 1, № 3. P. 251-258. doi: 10.1016/0164-1212 (79)90025-6.

4. Смагин В. А. Основы теории надежности программного обеспечения / В. А. Смагин. – СПб.: ВКА им. А. Ф. Можайского, 2009. 355 с.

5. Бубнов В. П. Разработка динамических моделей нестационарных систем обслуживания / В. П. Бубнов, В. И. Сафонов. – СПб.: Лань, 1999. 64 с.

6. Бубнов В. П. Нестационарная модель надежности программных средств с распределением Кокса длин интервалов времени исправления ошибок / В. П. Бубнов, А. В. Тырва, К. И. Бурцева // Вестн. Всерос. науч.-исслед. и проектно-конструкторского ин-та электровозостроения. 2010. Вып. 1 (59). С. 143-152.

7. Гиндин С. И. Программный комплекс расчета характеристик многоканальных систем массового обслуживания с «разогревом» и подход к его тестированию / С. И. Гиндин, А. Д. Хомоненко, С. В. Матвеев // Соврем. проблемы науки и образования. 2014. № 4. С. 152.

8. Рыжиков Ю. И. Пакет программ для расчета систем с очередями и его тестирование / Ю. И. Рыжиков // Тр. СПИИРАН. 2008. № 7. С. 265–284.

9. Chidamber S. R. A metrics suite for object oriented design / S. R. Chidamber, C. F. Kemerer // IEEE Trans. Software Eng. 1994. Vol. 20, № 6. P. 476-493. doi: 10.1109/32.295895.

10. Emam K. El. The prediction of faulty classes using object-oriented design metrics / K. El Emam, W. Melo, J. C. Machado // J. Syst. Softw. 2001. Vol. 56, № 1. P. 63-75.

11. Хомоненко А. Д. Нестационарные модели стратегий испытаний программных средств при вероятностных параметрах обнаружения ошибок / А. Д. Хомоненко, А. И. Данилов, А. А. Данилов // Информационно-управляющие системы. 2015. Вып. 4. С. 50-58.

12. Хомоненко А. Д. Динамические модели отладки программ с вероятностным обнаружением ошибок и распределением Эрланга длительности их исправления / А. Д. Хомоненко, А. И. Данилов, А. А. Данилов // Науч.-технич. вестн. информ. технологий, механики и оптики. 2016. Т. 16, № 4. С. 655-662. doi: 10.17586/2226-1494-2016-16-4-655-662.

13. Хомоненко А. Д. Нестационарные модели отладки программ с распределением Кокса длительности исправления ошибок / А. Д. Хомоненко, А. И. Данилов, А. А. Данилов, П. В. Герасименко // Междунар. конф. по мягким вычислениям и измерениям. Т. 1. Секции 1–3. – СПб., 2016. С. 163-166.

14. Данилов А. И. Методика численного анализа эффективности отладки программных средств / А. И. Данилов, А. А. Данилов // Науч.-технич. вестн. информ. технологий, механики и оптики. 2017. Т. 17, № 3. С. 543-551. doi: 10.17586/2226-1494-2017-17-3-543-551.

Software Package Based on Dynamic Models for Reliability Estimation and Project Planning

Danilov A.A.
Nokia Solutions and Networks
St. Petersburg, Russia
andrey.danilov.aad@mail.ru

Abstract. **The software package for testing process probabilistic characteristic calculations was created: probability of certain states, time distribution function of errors detection and resolution, mathematical expectation of random variables, number of detected or corrected errors. Available software testing models do not take into account the probabilistic nature of error detection and resolution. The software package is built on advanced numerical models of testing processes and takes into account the error detection probability for each software module as well as tests viability (capacity). The use of the package in planning reduces time and costs for software development and ensures necessary software quality and reliability. The software package allows to plan necessary resources to achieve specified software quality, compare different testing strategies and choose the best one for available resources.**

Keywords: **dynamic process models, software testing, error, probability, software testing stategies, labeled graphs.**

References

1. Moranda P., Jelinski Z. Final Report on Software Reliability Study. McDonnell Douglas Astronautics Company, MADC Report Number 63921, 1972.

2. Musa J.D., Iannino A., Okumoto K. Software Reliability: Measurement, Prediction, Application. NY, McGraw-Hill, 1987.

3. Littlewood B. The Littlewood-Verrall Model for Software Reliability Compared with Some Rivals. *J. Syst. Softw.*, 1980, vol. 1, no. 3, pp. 251-258. doi: 10.1016/0164-1212 (79)90025-6.

4. Smagin V.A. Theory of Software Reliability [Osnovy teorii nadezhnosti programmnogo obespecheniia]. St. Petersburg, VKA im. A.F. Mozhaiskogo Publ., 2009. 355 p.

5. Bubnov V.P., Safonov V.I. Dynamic Modelling of Nonstationary Queueing Systems [Razrabotka dinamicheskikh modelei nestatsionarnykh system obsluzhivaniia]. St. Petersburg, Lan' Publ., 1999. 64 p.

6. Bubnov V.P., Tyrva A.V., Burtseva K.I. Non-stationary Software Reliability Model with Coxian Distribution of Errors Detection Time interval Lengths [Nestatsionarnaya model' nadezhnosti programmnykh sredstv s raspredeleniem Koksa dlin intervalov vremeni ispravleniya oshibok], *Bulletin of All-Russian Scientific Research and Design Institute of Electric Locomotive Engineering [Vestnik Vserossiyskogo nauchno-issledovatel'skogo i proektno-konstruktorskogo instituta elektrovozostroeniya]*, 2010, is. 1, pp. 143-152.

7. Gindin S.I., Khomonenko A.D., Matveev S.V. Software for Calculation the Characteristics of Multichannel Queueing Systems with „Warm-Up" and Approach for its Testing [Programmnyi kompleks rascheta kharakteristik mnogokanal'nykh sistem massovogo obsluzhivaniia s „razogrevom" i podkhod k ego testirovaniiu], *Modern problems of sci. and education [Sovremennye problemy nauki i obrazovaniia]*, 2014, no. 4, pp. 152.

8. Ryzhikov Yu.I. Program Package for Queuing System Computation and its Testing [Paket programm dlya rascheta sistem s ocheredyami i ego testirovanie]. *SPIIRAS Proc. [Trudy SPIIRAN]*, 2008, no. 7, pp. 265-284.

9. Chidamber S.R., Kemerer C.F. A Metrics Suite for Object Oriented Design, *IEEE Trans. Software Eng.*, 1994, vol. 20, no. 6, pp. 476-493. doi: 10.1109/32.295895.

10. Emam K. El, Melo W., Machado J.C. The Prediction of Faulty Classes Using Object-Oriented Design Metrics, *J. Syst. Softw.*, 2001, vol. 56, no. 1, pp. 63-75.

11. Khomonenko A.D., Danilov A.I., Danilov A.A. Nonstationary Models of Software Testing Strategies with Probabilistic Parameters for Fault Detection [Nestatsionarnye modeli strategiy ispytaniy programmnykh sredstv pri veroyatnostnykh parametrakh obnaruzheniya oshibok]. *Inf. Control Syst. [Informacionno-upravljajushhie sistemy]*, 2015, is. 4, pp. 50-58.

12. Khomonenko A.D., Danilov A.I., Danilov A.A. Dynamic Software Testing Models with Probabilistic Parameters for Fault Detection and Erlang Distribution for Fault Resolution Duration [Dinamicheskie modeli otladki programm s veroyatnostnym obnaruzheniem oshibok i raspredeleniem Erlanga dlitel'nosti ikh ispravleniya]. *Sci. Tech.J. Inf. Technol., Mech. Optics [Nauchno-tekhnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki]*, 2016, vol. 16, no. 4, pp. 655-662. doi: 10.17586/2226-1494-2016-16-4-655-662.

13. Khomonenko A.D., Danilov A.I., Danilov A.A., Gerasimenko P.V. Nonstationary Software Testing Models with Cox Distribution for Fault Resolution Duration [Nestatsionarnye modeli otladki programm s raspredeleniem Koksa dlitel'nosti ispravleniya oshibok]. *Proc. 19th Int. Conf. Soft Comput. and Measurements [Mezhdunarodnaya konferentsiya po myagkim vychisleniyam i izmereniyam], SCM 2016*, St. Petersburg, 2016. Pp. 209-212.

14. Danilov A.I., Danilov A.A. Numerical Analysis Methods of Software Test Efficiency [Metodika chislennogo analiza effektivnosti otladki programmnykh sredstv], *Sci. Tech.J. Inf. Technol., Mech. Optics [Nauchno-tekhnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki]*, 2017, vol. 17, no. 3, pp. 543-551. doi: 10.17586/2226-1494-2017-17-3-543-551.

Исследование устойчивости стеганографической системы защиты информации на основе прямого расширения спектра к активным атакам

Балтаев Р. Х., Лунегов И. В.
Пермский государственный национальный исследовательский университет
Пермь, Россия
rodion-baltaev@yandex.ru, lunegov@psu.ru

Аннотация. **Цель работы – исследовать устойчивость стеганографической системы защиты информации (ССЗИ) на основе метода прямого расширения спектра с перекрытием блоков изображения к активным атакам, направленным на удаление скрытой информации. Определены ограничения использования предложенной автором ССЗИ при воздействии на статические изображения активных атак – сжатие JPEG, шумы типа «соль и перец», Гауссов шум, а также низкочастотной фильтрации.**

Ключевые слова: **стеганография, стегоаналитические атаки, метод расширения спектра, перекрытие блоков изображения.**

Введение

Важным направлением развития современных средств защиты информации являются стеганографические системы защиты информации (ССЗИ), которые обеспечивают сокрытие не только информационного содержания передаваемых данных, но и самого факта их передачи. ССЗИ – это совокупность средств и методов, используемых для создания скрытого канала передачи информации [1].

В стеганографии есть два типа атак на стегообъекты: пассивные и активные [2–4]. Пассивные атаки направлены на обнаружение встраивания или извлечения сообщения без изменения стегообъекта. Вид пассивной атаки на ССЗИ, направленной на обнаружение встроенного сообщения, называется пассивным стегоанализом. Вид пассивной атаки на ССЗИ, направленный на извлечение встроенной информации, называется активным стегоанализом.

Активные атаки направлены на удаление или искажение встроенного сообщения путем изменения стегообъекта. Различают две формы активных атак [2]: устраняющие и маскирующие. Устраняющая атака направлена на полное удаление встроенного сообщения из стегообъекта. Удаление встроенного сообщения не означает восстановления оригинального изображения. Маскировка встроенного сообщения означает, что атакуемый стегообъект может содержать встроенное сообщение, и это сообщение не обнаруживается существующими детекторами, но применение более чувствительного детектора позволяет его обнаружить [5].

В данной работе исследуется устойчивость ССЗИ к наиболее распространенным активным атакам: сжатию JPEG, шумам типа «соль и перец», Гауссову шуму, а также к низкочастотной фильтрации. Под устойчивостью понимается возможность безошибочно извлечь встроенную информацию после преобразования изображения.

ССЗИ на основе расширения спектра

Рассмотрим ССЗИ на основе прямого расширения спектра, модель которой предложена в [6] (рис. 1).

На рис. 1 пунктирной линией выделены блоки модели ССЗИ, добавленные автором, остальные блоки являются классическими. На стороне отправителя сообщение кодируется с помощью LDPC-кода, параллельно на основе ключа отправителя формируется псевдослучайная последовательность (ПСП). Сообщение встраивается с помощью метода с перекрытием блока изображения, предложенного автором в [7, 8]:

• берем i-й блок $\mathbf{B}_i$ изображения заданного размера, смещаясь на определенное количество пикселей по строкам и столбцам:

$$\mathbf{B}_i(k,l) = \mathbf{L}(k + i_1, l + j_1),$$

где $k = 1,2,\ldots,M_1$; $l = 1,2,\ldots,N_1$; $\mathbf{L}$ – цветовой канал изображения размера $M \times N$; $\mathbf{B}_i$ – i-й номер блока изображения; $i = 1,2,\ldots,d$; d – количество блоков пикселей изображения; i_1, j_1 – смещение по строкам и столбцам, соответственно.

$$d = \left[floor\left(\frac{M - M_1}{M_1 - s_M} \right) + 1 \right] \left[floor\left(\frac{N - N_1}{N_1 - s_N} \right) + 1 \right],$$

где M_1, N_1 – размер блока по высоте и по горизонтали, соответственно; s_M, s_N – количество перекрытых пикселей блока по строкам и столбцам, соответственно; $floor(a)$ – округление до ближайшего целого $\le a$.

$$i_1 = \frac{i - 1 - \mathrm{mod}(i-1, k_n)}{k_n}(M_1 - s_M);$$

$$j_1 = \mathrm{mod}(i-1, k_n)(N_1 - s_N),$$

где $k_n = floor\left(\frac{N - N_1}{N_1 - s_N} \right) + 1$; $\mathrm{mod}(a,b)$ – остаток от деления a на b;

• развертываем i-й блок $\mathbf{B}_i$ изображения по строкам:

$$\mathbf{x}_i = Vec(\mathbf{B}_i),$$

где $Vec(\cdot)$ – функция преобразования матрицы в вектор.

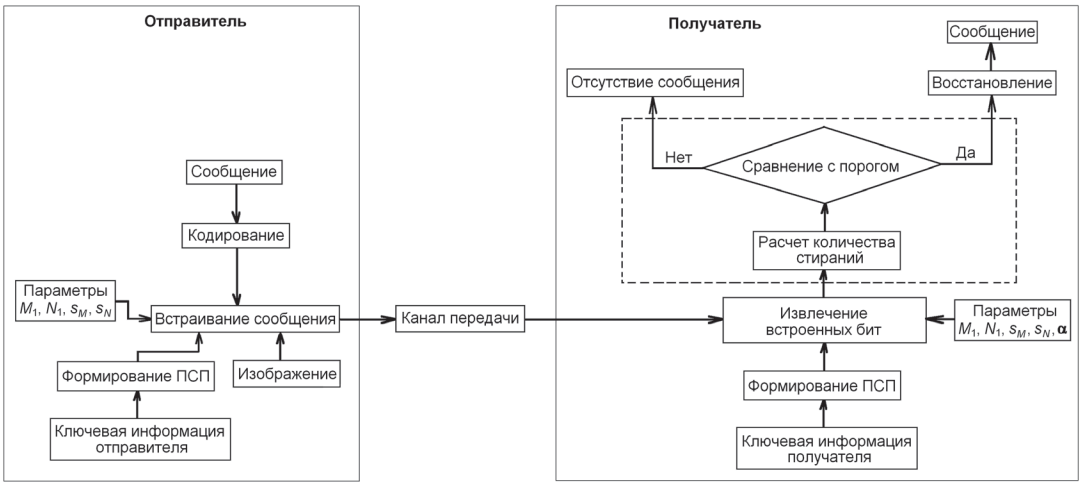


Рис. 1. Модель ССЗИ

$$Vec\begin{pmatrix} b_{1,1} & b_{1,2} & \dots & b_{1,N_1} \\ b_{2,1} & b_{2,2} & \dots & b_{2,N_1} \\ \vdots & \vdots & \ddots & \vdots \\ b_{M_1,1} & b_{M_1,2} & \dots & b_{M_1,N_1} \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_q \\ \vdots \\ x_L \end{pmatrix};$$

$$x_{(l-1)M_1+k} = b_{k,l};\quad q = 1\dots L;\quad L = M_1 N_1;$$

• встраиваем сообщение:

$$\mathbf{y}_i = m_i \mathbf{w} + \mathbf{x}_i,$$

где $m_i \in \{+1, -1\}$ – бит сообщения; $\mathbf{w}$ – вектор шумоподобной последовательности, $w_q \in \{+1, -1\}$; $\mathbf{y}_i$ – модифицированный вектор i-го блока.

На приемной стороне модели ССЗИ (рис. 1) формируется ПСП на основе ключа получателя и извлекается бит сообщения с помощью алгоритма, предложенного в [9]. Предложенная ССЗИ позволяет увеличивать скрытность передаваемого сообщения, передавать сообщение с низкой вероятностью ошибок извлечения, использовать перекрытие блоков изображения для увеличения количества передаваемых данных.

В [6] исследовалась устойчивость предложенной ССЗИ к пассивному стегоанализу. Было определено, что предложенная модель обладает устойчивостью к пассивному стегоанализу при перекрытии блоков изображения вплоть до $s_M = 24$ и $s_N = 24$ пикселя по строкам и столбцам.

Устойчивость ССЗИ к сжатию JPEG

Для исследования устойчивости ССЗИ к сжатию JPEG использовалась база данных из 1000 изображений, описанных в [10]. Встраивали во все цветовые каналы цветовые модели RGB и YCbCr с перекрытием блоков пикселей изображения по строкам и столбцам $s_M = 24$ и $s_N = 24$.

На рис. 2, 3 представлены зависимости коэффициента битовых ошибок BER (Bit Error Ratio) от коэффициента качества Q сжатия JPEG для цветовых каналов модели RGB и YCbCr рассматриваемой модели ССЗИ, где под BER (Bit Error Ratio) понимается отношение количества ошибочных битов к их общему переданному числу.

Встроенная информация считается удаленной, если коэффициент битовых ошибок BER принимает значение 0,5, поскольку после удаления сообщения и при попытке извлечь ее получаем некоторую случайную двоичную последовательность нулей и единиц, вероятность совпадения которых со встроенной последовательностью есть 0,5.

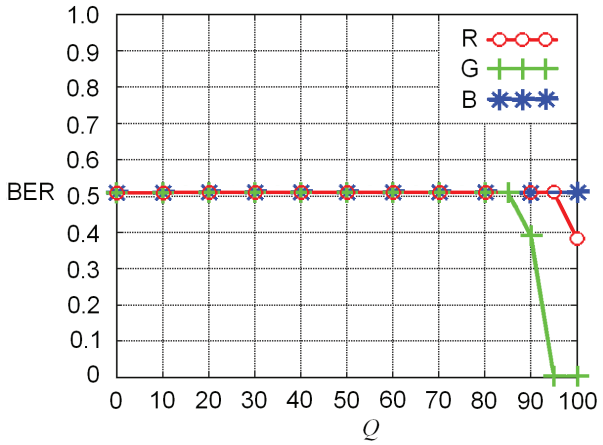


Рис. 2. Зависимости BER от коэффициента качества Q сжатия JPEG для цветовых каналов модели RGB

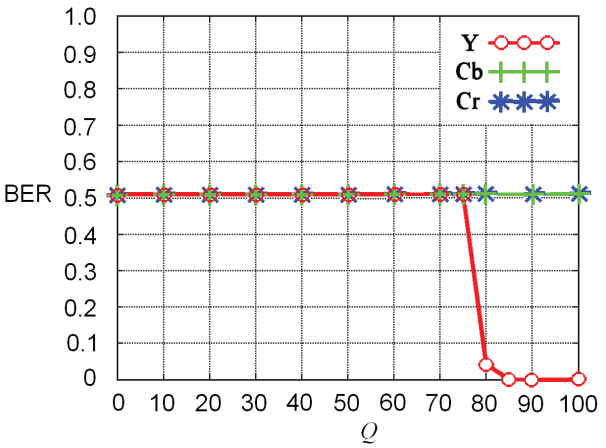


Рис. 3. Зависимости BER от коэффициента качества Q сжатия JPEG для цветовых каналов модели YCbCr

Известно [11], что алгоритм сжатия с потерями JPEG менее всего искажает яркостную компоненту Y цветовой модели YCbCr, поскольку человеческий глаз более чувствителен к яркости, чем к цвету, поэтому цветоразностные каналы Cb и Cr искажаются сильнее. Это подтверждается графиками на рис. 3, из которых следует, что информация, встроенная в цветоразностные каналы Cb и Cr, удаляется при любом значении коэффициента качества Q, в отличие от яркостной компоненты Y, где встроенная информация удаляется при коэффициенте качества Q меньше 80.

Из рис. 2 видно, что коэффициент битовых ошибок BER меньше всего у зеленой компоненты G и больше всего – у синей компоненты B.

Рассмотрим формулы преобразования из цветовой модели RGB в цветовую модель YCbCr [12]:

$$\begin{aligned} Y &= 0,299R + 0,587G + 0,114B; \\ Cb &= -0,169R - 0,331G + 0,5B + 128; \\ Cr &= 0,5R - 0,419G - 0,081B + 128. \end{aligned} \qquad (1)$$

Лучшие показатели устойчивости к сжатию JPEG в зеленой компоненте G объясняются из (1) тем, что зеленая компонента G подвергается меньшим искажениям сжатия JPEG, поскольку является основной частью яркостной компоненты Y.

Предложенная модель ССЗИ (рис. 1) позволяет ограниченно применять изображения, сжатые по алгоритму JPEG. Встроенная информация может быть извлечена из яркостной компоненты Y изображения, сжатого по алгоритму JPEG, с небольшой вероятностью ошибки при коэффициенте качества, большем 80.

Устойчивость ССЗИ к шумам типа «соль и перец» и Гауссову шуму

Процесс добавления шума «соль и перец» заключается в замене с некоторой вероятностью значения яркости пикселя изображения на черные или белые значения, т. е. замена на 0 или 255 для 8-битового изображения. Шум «соль и перец» характеризуется плотностью d (доля пикселей изображения, подверженному этому шуму).

На рис. 4 и 5 представлены зависимости коэффициента битовых ошибок BER от плотности d шума «соль и перец» для цветовых каналов модели RGB и YCbCr, соответственно.

Из рис. 4 и 5 видно, что предложенная ССЗИ имеет низкую устойчивость к шуму «соль и перец». При встраивании в каналы цветовой модели RGB имеется устойчивость к шуму «соль и перец» с плотностью d не более 0,01. Результаты лучше при встраивании информации в яркостную компоненту Y цветовой модели YCbCr, в котором встроенное сообщение сохраняется до значения плотности шума «соль и перец» $d = 0,03$. По сравнению с яркостной компонентой Y коэффициент битовых ошибок BER меньше при встраивании информации в цветоразностные компоненты Cb и Cr, в которых встроенное сообщение сохраняется до значения плотности шума «соль и перец» $d = 0,06$.

Низкая устойчивость к шуму «соль и перец» объясняется применением перекрытия блоков пикселей изображения для встраивания информации. Поскольку элементы ПСП, используемой для встраивания информации, принимают значения +1 и –1, при перекрытии часть этих элементов взаимоуничтожается в результате их сложения. Шум «соль и перец» дополнительно уничтожает элементы ПСП, что приводит к невозможности извлечения встроенной информации.

Рассмотрим применение Гауссова шума к предложенной ССЗИ (все исследования проводились в программном пакете MATLAB). Для добавления шума к изображению использовалась функция *imnoise*. Особенностью наложения шума к изображению с помощью функции *imnoise* является то, что данная функция сначала преобразует изображение в класс *double* в диапазоне [0; 1], добавляет шум, а затем преобразует изображение обратно в исходный тип в диапазоне [0; 255] для 8-битного изображения, поэтому перед заданием параметров шума в функции *imnoise* необходимо уменьшить параметры. При задании среднего шума необходимо среднее значение шума поделить на 256. При задании дисперсии шума необходимо значение дисперсии шума поделить на 256^2 [13].

На рис. 6 и 7 представлены зависимости коэффициента битовых ошибок BER от дисперсии σ^2 Гауссова шума для цветовых каналов модели RGB и YCbCr, соответственно.

Графики на рис. 6 и 7 показывают, что при встраивании в каналы цветовой модели RGB предложенная ССЗИ облада-

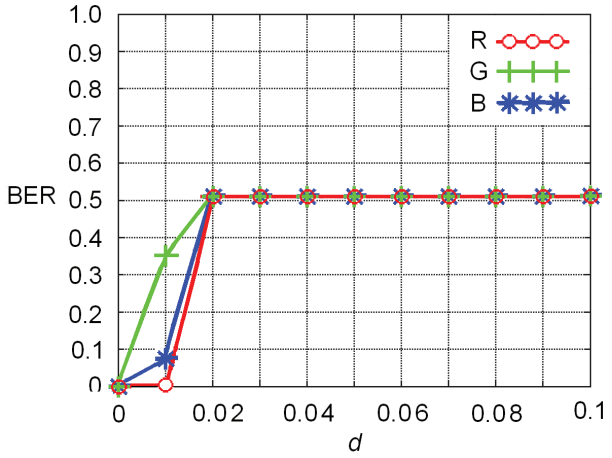


Рис. 4. Зависимости BER от плотности d шума «соль и перец» для цветовых каналов модели RGB

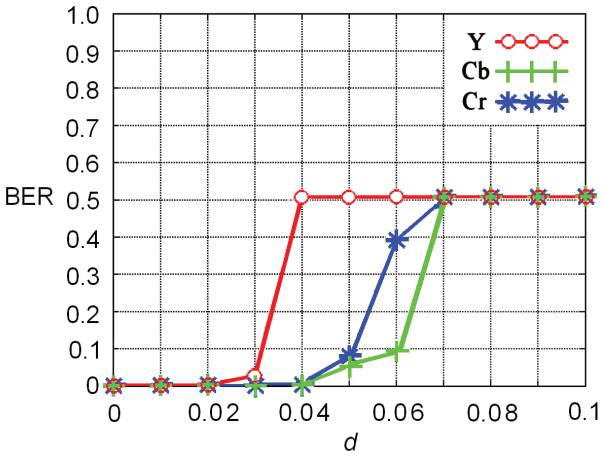


Рис. 5. Зависимости BER от плотности d шума «соль и перец» для цветовых каналов модели YCbCr

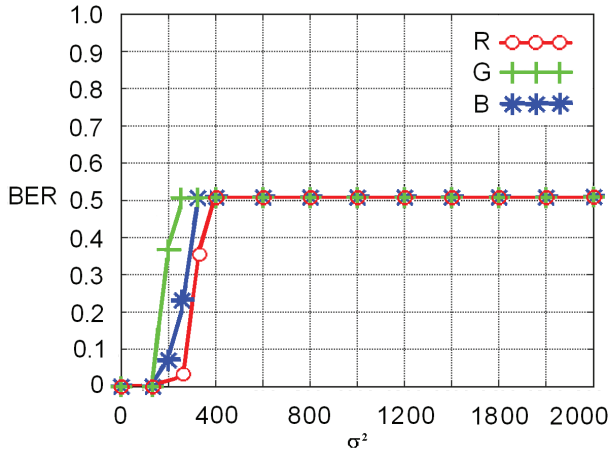


Рис. 6. Зависимости BER от дисперсии σ^2 Гауссова шума для цветовых каналов модели RGB

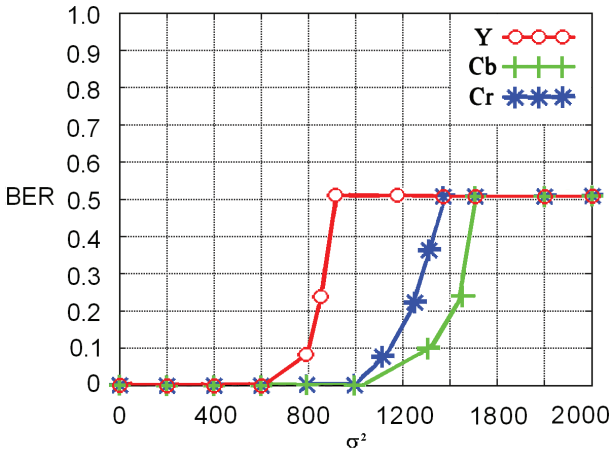


Рис. 7. Зависимости BER от дисперсии σ^2 Гауссова шума для цветовых каналов модели YCbCr

ет устойчивостью к Гауссову шуму при дисперсии σ^2 до значения 200. Так же, как для шума «соль и перец», предложенная ССЗИ обладает большей устойчивостью к Гауссову шуму при встраивании информации в цветоразностные каналы Cb и Cr, при этом дисперсии шума составляют 1500 и 1400, при которых информацию еще можно извлечь.

Высокая устойчивость к искажениям изображения Гауссовым шумом объясняется тем, что используемая ПСП также является распределенной по Гауссу.

Устойчивость ССЗИ к низкочастотной фильтрации

Применим фильтрацию цифровых изображений в качестве метода удаления встроенной информации в изображении. Для встраивания дополнительной информации используется ПСП, которая складывается с пикселями изображения. Используемая ПСП является белым шумом, поэтому ее составляющие пространственно декоррелированы. В данном случае пространственные частоты в спектре псевдослучайной последовательности располагаются выше частот спектра изображений, следовательно, низкочастотная фильтрация изображения служит хорошим методом удаления встроенной информации.

При обработке изображений широко используются семейства низкочастотных фильтров на основе вещественной функции Гаусса [14]. Будем использовать низкочастотный Гауссов фильтр, ядро которого быстро спадает до нуля при удалении центральной точки маски фильтрации, поэтому размер маски фильтрации выбирают малого размера в пределах 2–3 стандартного отклонения Гаусса σ, при этом минимально содержательным размером маски фильтрации считается размер 3×3 пикселя.

На рис. 8 и 9 представлены зависимости коэффициента битовых ошибок BER от стандартного отклонения Гаусса σ фильтра для цветовых каналов модели RGB и YCbCr, соответственно.

Как и предполагалось, ССЗИ из рис. 1 обладает низкой устойчивостью к низкочастотному Гауссову фильтру (рис. 8 и 9). Из рис. 8 и 9 видно, что при встраивании информации в цветоразностные каналы Cb и Cr устойчивость ССЗИ к низкочастотному фильтру Гаусса лучше, что соответствует представленным выше результатам.

Заключение

Исследована устойчивость предложенной ССЗИ к активным атакам (сжатию JPEG, наложению шума типа «соль

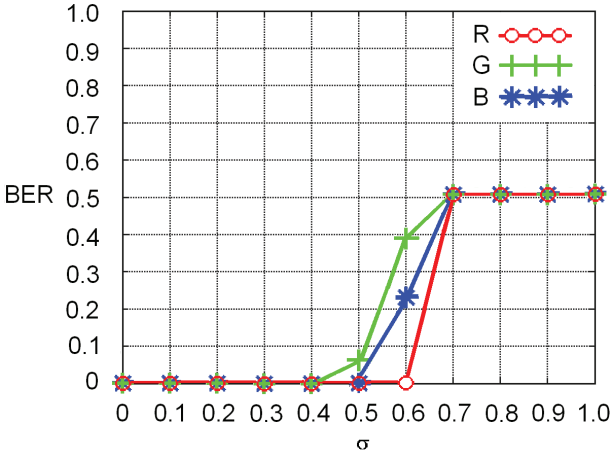


Рис. 8. Зависимости BER от стандартного отклонения Гаусса σ фильтра для цветовых каналов модели RGB

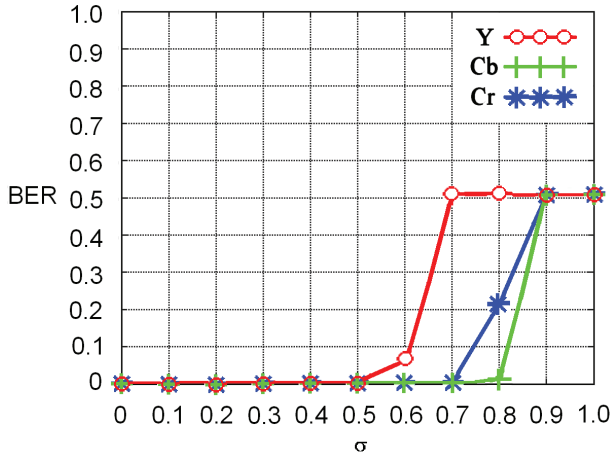


Рис. 9. Зависимости BER от стандартного отклонения Гаусса σ фильтра для цветовых каналов модели YCbCr

и перец», Гауссова шума и низкочастотной Гауссовой фильтрации).

Установлено, что предложенная ССЗИ устойчива к JPEG-сжатию при встраивании в яркостной канал Y цветовой модели YCbCr, так как он при JPEG-сжатии подвергается наименьшим искажениям. Встроенные данные обнаруживаются при коэффициенте качества Q больше 80.

Высокая устойчивость ССЗИ наблюдается при зашумлении изображения Гауссовым шумом, поскольку используемая ПСП для встраивания информации сама является распределенной по Гауссу. Определено, что ССЗИ обладает низкой устойчивостью к шуму «соль и перец» из-за использования перекрытия ПСП для встраивания информации и к фильтрации изображения низкочастотным Гауссовым фильтром, поскольку используемая ПСП является шумоподобным сигналом.

Литература

1. Небаева К. А. Разработка необнаруживаемых стегосистем для каналов с шумом: дис. … канд. техн. наук: 05.12.13 / К. А. Небаева. – СПб., 2014. 176 с.

2. Cox I. J. Digital watermarking and steganography / I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich. – San Francisco: Morgan Kaufmann publ., 2008. 624 p.

3. Ming L. Active spread-spectrum steganalysis for hidden data extraction / L. Ming, M. Kulhandjian, D. A. Pados, S. N. Batalama, M. J. Medley // 13th ACM Workshop on Multimedia and Security. 2011. P. 1-10.

4. Sharp A. A Novel active warden steganographic attack for next-generation steganography / A. Sharp, Q. Qi, Y. Yang // 9th Int. Wireless Communications and Mobile Comput. Conf. 2013. P. 1138-1143.

5. Ming L. Secure spread-spectrum data embedding with PN-sequence masking / L. Ming, G. Yanqing, W. Bo, K. Xiangwei // Signal Proc.: Image Communication. 2015. Vol. 39. P. 17-25.

6. Балтаев Р. Х. Устойчивость стеганографического метода на основе прямого расширения спектра к пассивному стегоанализу / Р. Х. Балтаев // Актуальные проблемы информационной безопасности в Приволжском федеральном округе: сб. ст. 2016. С. 9-13.

7. Балтаев Р. Х. Увеличение количества передаваемой информации в стеганографической системе на основе метода прямого расширения спектра / Р. Х. Балтаев, И. В. Лунегов // Изв. вузов. Приборостроение. 2016. Т. 59, № 9. С. 717-722.

8. Балтаев Р. Х. Метод увеличения скрытности передаваемой информации за счет минимально возможного изменения пикселей изображения при его максимальном заполнении информацией / Р. Х. Балтаев., И. В. Лунегов // Вопр. безопасности. 2016. № 6. С. 52-59.

9. Балтаев Р. Х. Уменьшение ошибок извлечения встроенной информации в стеганографической системе защиты информации со слепым декодером с минимальным изменением пикселей изображения и его максимальном заполнении / Р. Х. Балтаев, И. В. Лунегов // Кибернетика и программирование. 2016. № 6. С. 47-55.

10. Schaefer G. UCID – An uncompressed colour image database / G. Schaefer, M. Stich // Proc. SPIE, Storage and Retrieval Methods and Appl. for Multimedia. 2004. P. 472-480.

11. Кулешов С. В. Идентификация факта компрессии с потерями в процессе обработки изображений / С. В. Кулешов, А. Ю. Аксенов, А. А. Зайцева // Тр. СПИИРАН. 2007. Вып. 5. С. 60-65.

12. Hamilton E. JPEG File Interchange Format, Version 1.02 / E. Hamilton. – 1992.

13. Гонсалес Р. Цифровая обработка изображений в среде MATLAB / Р. Гонсалес, Р. Вудс, С. Эддинс. – М.: Техносфера, 2006. 616 с.

14. Визильтер Ю. В. Обработка и анализ цифровых изображений с примерами на LabVIEW IMAQ Vision / Ю. В. Визильтер, С. Ю. Желтов, В. А. Князь, А. В. Моржин, А. Н. Ходарев. – М.: ДМК-Пресс, 2007. 464 с.

Research of the Robustness of the Steganographic System Based on Direct Sequence Spread Spectrum to Active Attacks

Baltaev R. Kh., Lunegov I. V.
Perm State University
Perm, Russia
rodion-baltaev@yandex.ru, lunegov@psu.ru

Abstract. **The subject of the paper is the study of the robustness of the steganographic system based on direct sequence spread spectrum with overlapping of image blocks to active attacks directed at removing hidden information. Restrictions on the use of the steganographic system proposed by the author in response to static images of active attacks – JPEG compression, "Salt and Pepper" noises, Gaussian noise and low-frequency filtering – are determined.**

Keywords: **steganography, stegoanalytical attacks, direct sequence spread spectrum, overlapping of image blocks.**

References

1. Nebaeva K.A. Development of Undetectable Stegosystems for Channels with Noise [Razrabotka neobnaruzhivaemyh stegosistem dlya kanalov s shumom]: diss. … candidate of technical sciences: 05.12.13. St. Peterburg, 2014. 176 p.

2. Cox I.J., Miller M.L., Bloom, J.A., Fridrich. J. Digital Watermarking and Steganography. San Francisco, Morgan Kaufmann publ., 2008. 624 p.

3. Ming L., Kulhandjian M., Pados D.A., Batalama S.N., Medley M.J. Active Spread-Spectrum Steganalysis for Hidden Data Extraction, *13th ACM Workshop on Multimedia and Security*, 2011, pp. 1-10.

4. Sharp A., Qi Q., Yang Y. A Novel Active Warden Steganographic Attack for Next-Generation Steganography, *9th Int. Wireless Communications and Mobile Comput. Conf.*, 2013, pp. 1138-1143.

5. Ming L., Yanqing G., Bo W., Xiangwei K. Secure Spread-Spectrum Data Embedding with PN-Sequence Masking, *Signal Proc.: Image Communication*, 2015, Vol. 39, pp. 17-25.

6. Baltaev R.Kh. Robust Steganographic Method Based on Direct Spread to Passive Steganalysis [Ustojchivost steganograficheskogo metoda na osnove pryamogo rasshireniya spektra k passivnomu stegoanalizu], *Actual Problems of Information Security in the Volga Federal District [Aktualnye problemy informacionnoj bezopasnosti v Privolzhskom federal'nom okruge]*, 2016, pp. 9-13.

7. Baltaev R.Kh., Lunegov I.V. Increase in Number of the Transmitted Information Steganographic System Based on the Method Direct Spread Spectrum [Uvelichenie kolichestva peredavaemoj informacii v ste-ganograficheskoj sisteme na osnove metoda pryamogo rasshireniya spektra], *J. Instrument Eng. [Izvestiya vysshih uchebnyh zavedenij. Priborostroenie]*, 2016, vol. 59, no. 9, pp. 717-722.

8. Baltaev R.Kh., Lunegov I.V. The Method of Increasing the Information Hidden Due to the Minimum Possible Change of Pixels the Image at Its Maximum Filling Information [Metod uvelicheniya skrytnosti peredavaemoj informacii za schet minimal'no vozmozhnogo izmeneniya pikselej izobrazheniya pri ego maksimal'nom zapolnenii informaciej], *Security Questions [Voprosy bezopasnosti]*, 2016, no. 6, pp. 52-59.

9. Baltaev R.Kh., Lunegov I.V. Reduction of Extraction Errors of Information in the Steganographic System with a Blind Decoder with Minimal Change of the Image Pixels and Its Maximum Filling [Umenshenie oshibok izvlecheniya vstroennoj informacii v steganograficheskoj sisteme zashchity informacii so slepym dekoderom s minimal'nym izmeneniem pikselej izobrazheniya i ego maksimalnom zapolnenii], *Cybernetics and Programming [Kibernetika i programmirovanie]*, 2016, no. 6, pp. 47-55.

10. Schaefer G., Stich M. UCID – An Uncompressed Colour Image Database, *Proc. SPIE, Storage and Retrieval Methods and Applications for Multimedia,* 2004, pp. 472-480.

11. Kuleshov S.V., Aksenov A.Yu., Zajceva A.A. Detection of Lossy Compression Usage in Image Processing [Identifikaciya fakta kompressii s poteryami v processe obrabotki izobrazhenij], *SPIIRAS Proc. [Trudy SPIIRAN]*, 2007, no. 5, pp. 60-65.

12. Hamilton E. JPEG File Interchange Format, Version 1.02. 1992.

13. Gonsales R., Vuds R., Ehddins S. Digital Image Processing Using MATLAB [Cifrovaya obrabotka izobrazhenij v srede MATLAB], Moscow, Technosphera, 2006. 616 p.

14. Vizilter Yu.V., ZHeltov S.Yu., Knyaz V.A., Morzhin A.V., Hodarev A.N. Digital Image Processing and Analysis with Examples on LabVIEW IMAQ Vision [Obrabotka i analiz cifrovyh izobrazhenij s primerami na LabVIEW IMAQ Vision], Moscow, DMK-Press, 2007. 464 p.

Генерация псевдослучайных последовательностей на основе линейного конгруэнтного метода и полиномиального счётчика

Власенко А. В., Дзьобан П. И.
Кубанский государственный технологический университет
Краснодар, Россия
alex_vlasenko@list.ru, antiemoboy@mail.ru

Аннотация. **Специалисты в области информационной безопасности и защиты информации часто сталкиваются с необходимостью генерации случайных последовательностей и чисел. Чаще всего случайные числа требуются в задачах моделирования, численного анализа и тестирования, но есть и множество других весьма специфических задач. Известно, что во всех современных языках программирования есть функция random или её аналоги. Эти функции чаще всего дают действительно хорошие псевдослучайные числа. В статье рассмотрены особенности реализации линейного конгруэнтного метода, который чаще всего используется в функции random, и метод получения случайных чисел с помощью полиномиального счётчика, который применяется для тестирования аппаратуры.**

Ключевые слова: **случайная последовательность, псведослучаная последовательность, энтропия, генератор псевдослучайной последовательности, криптостойкость, линейный конгруэнтный метод, полиномиальный счетчик.**

Введение

Есть смысл генерировать псевдослучайные числа только с равномерным законом распределения, так как все остальные распределения можно получить из равномерного путём преобразований, известных из теории вероятности. В 1927 г. Типпетт опубликовал первую таблицу случайных чисел [1, 2]. Чуть позже были попытки автоматизировать процесс. Стали появляться машины, генерирующие случайные числа. Сейчас такие устройства тоже используются и называются источниками (генераторами) энтропии. Стоит заметить, что только такие устройства могут давать по-настоящему случайные числа. Очевидно, генераторы энтропии довольно до́роги, и их повсеместное использование невозможно. Именно поэтому возникла необходимость в алгоритмах получения псевдослучайных чисел [3].

Некоторые специалисты склонны считать, что генерация случайных и псевдослучайных последовательностей – это простая задача. Мнение обывателей заключается в постулате производить случайные сложные математические действия над исходным числом. Однако данные преобразования последовательны, имеют исходное значение и результат, а значит, заведомо скомпрометированы и подлежат дешифрованию в результате вычислений как в одну, так и в другую стороны [4].

Качественный генератор псевдослучайной последовательности, ориентированный на использование в средствах защиты программных систем, должен удовлетворять следующим требованиям:

- непредсказуемости (криптографической стойкости);
- хороших статистических свойств: псевдослучайная последовательность по своим статистическим свойствам не должна отличаться от истинно случайной последовательности;
- большого периода формируемой последовательности, учитывая, что при преобразовании больших массивов данных каждому элементу входной последовательности необходимо ставить в соответствие свой элемент псевдослучайной последовательности;
- эффективной программной и аппаратной реализации [4, 5].

При использовании непредсказуемого генератора псевдослучайной последовательности три следующие задачи для злоумышленника или аналитика, не знающих ключевой информации, вычислительно неразрешимы:

- определение предыдущего $(i - 1)$-го элемента у последовательности на основе известного фрагмента последовательности $y_{i+1}y_{i+2}\ldots y_{i+1-b}$ конечной длины b (непредсказуемость влево);
- определение последующего $(i + b)$-го элемента элемента y_{i+b}-последовательности на основе известного фрагмента гаммы $y_{i+1}y_{i+2}\ldots y_{i+1-b}$ конечной длины b (непредсказуемость вправо);
- определение ключевой информации по известному фрагменту последовательности конечной длины.

Обращаясь ко второму тому Кнута, можно сделать вывод, что в 1959 г. были попытки построить генератор, основанный на такой последовательности преобразований [6]:

К1. [Выбрать число итераций.] Присвоить Y наибольшую значащую цифру X. (Шаги К2–К13 будут выполнены точно Y+1 раз, т. е. применены псевдослучайные преобразования случайное число раз.)

К2. [Выбрать случайный шаг.] Присвоить следующую наибольшую значащую цифру X. Перейти к шагу K (3 + Z), т. е. к случайно выбранному шагу в программе.

К3. [Обеспечить > 5 x 109.] Если X < 5 000 000 000, присвоить X значение X + 5 000 000 000.

К4. [Средина квадрата.] Заменить X серединой квадрата X.

К5. [Умножить.] Заменить X числом (1001001001 X) mod 1010.

К6. [Псевдодополнение.] Если X < 100 000 000, то присвоить X значение X + 9 814 055 677; иначе присвоить X значение 1010 – X.

К7. [Переставить половины.] Поменять местами пять младших по порядку знаков со старшими.

К8. [Умножить.] Выполнить шаг К5.

К9. [Уменьшить цифры.] Уменьшить каждую не равную нулю цифру десятичного представления числа X на единицу.

К10. [Модифицировать на 99 999.] Если A' < 105, присвоить X значение X 2 + 99 999; иначе присвоить X значение X – 99 999.

К11. [Нормировать.] (На этом шаге A' не может быть равным нулю.) Если X < 109, то умножить X на 10.

К12. [Модификация метода средин квадратов.] Заменить X на средние 10 цифр числа X (X – 1).

К13. [Повторить?] Если Y > 0, уменьшить У на 1 и возвратиться к шагу К2. Если Y = 0, алгоритм завершен. Значение числа X, полученное на предыдущем шаге, и будет желаемым «случайным» значением [7, 8].

Несмотря на кажущуюся сложность, этот алгоритм быстро сошёлся к числу 6 065 038 420, которое через небольшое число шагов преобразовалось в исходное значение [5].

В большинстве языков программирования именно линейный конгруэнтный метод используется в стандартной функции получения случайных чисел. Впервые этот метод был предложен Лехмером в 1949 г. [3]. Выбираются 4 числа:

- модуль m ($m > 0$);
- множитель a ($0 <= a < m$);
- приращение c ($0 <= c < m$);
- начальное значение X0 ($0 <= X0 < m$).

Последовательность получается с использование следующей рекуррентной формулы:

$$X_{n+1} = (a * X_n + c) \bmod m. \qquad (1)$$

Этот метод даёт действительно хорошие псевдослучайные числа, но если взять числа m, a, c произвольно, т. е. определить исходные значения случайно, то результат, скорее всего, разочарует. Например, при исходных значениях $m = 7$, $X_0 = 1$, $a = 2$, $c = 4$ получится следующая последовательность: 1, 6, 2, 1, 6, 2, 1, ... Очевидно, что эта последовательность не совсем подходит под определение случайной или псевдослучайной, не выполняются описанные требования [6]. Тем не менее, полученные результаты позволили сделать следующие выводы:

- исходные значения m, a, c, X_0 не должны быть случайными;
- результат реализации линейного конгруэнтного метода – это повторяющиеся последовательности.

На самом деле любая функция, отображающая конечное множество X в X, будет давать циклически повторяемые значения. Таким образом, задача сводится к тому, чтобы максимально увеличить энтропию – удлинить уникальную часть последовательности. Очевидно, что длина уникальной части не может быть больше m. Период последовательности будет равен m только при выполнении следующих условий:

- значения c и m взаимно простые;
- $a - 1$ кратно p для каждого простого p, являющегося делителем m;
- если m кратно 4, то и $a - 1$ должно быть кратно 4.

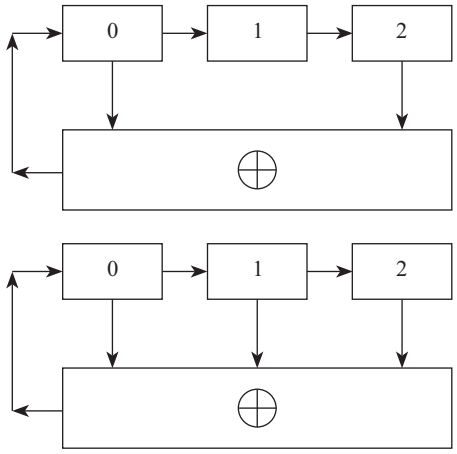
Последовательности, получаемые с помощью линейного конгруэнтного метода, не являются криптографически стойкими, так как, зная четыре подряд идущих числа, криптоаналитик может составить систему уравнений, из которых можно найти a, c, m.

Криптографически стойкий генератор псевдослучайных чисел (КСГПСЧ) – генератор псевдослучайных чисел, обладающий определенными свойствами, позволяющими использовать полученные числа в криптографии [9]. Требования к КСГПСЧ гораздо выше, чем к другим генераторам. В частности, КСГПСЧ должен обладать следующими свойствами:

- криптографической стойкостью;
- хорошими статистическими свойствами, делающими псевдослучайную последовательность неотличимой от истинно случайной;
- большим периодом псевдослучайной последовательности;
- эффективным использованием аппаратного ресурса [4, 5].

В основе полиномиального счетчика (сдвигового регистра) лежит операция исключающего ИЛИ (сумма по модулю два).

Схемы, представленные на рисунке, являются простейшими полиномиальными счётчиками.



Пример простейших схем полиномиальных счетчиков

Нулевой бит в таких схемах вычисляется на основе функции исключающего ИЛИ, а все остальные биты получаются простым сдвигом. Разряды, с которых сигнал идёт на исключающее ИЛИ, называются отводами [3, 5]. В таблице показано, как будут изменяться значения в рассмотренных регистрах при начальном значении 001.

Пример вычисления значений двух регистров
Счетчик 1 и Счетчик 2

Шаг	Счетчик 1			Счетчик 2		
	Биты			Биты		
	0	1	2	0	1	2
0	0	0	1	0	0	1
1	1	0	0	1	0	0
2	1	1	0	0	1	0
3	1	1	1	1	0	1
4	0	1	1	1	1	0
5	1	0	1	1	1	1
6	0	1	0	0	1	1
7	0	0	1	0	0	1

Стоит отметить, что регистры начинают работу с одного и того же значения, но потом значения, генерируемые регистрами, начинают быстро расходиться. Однако через шесть шагов оба регистра возвращаются в исходное состояние. Не составляет особого труда доказать, что оба этих регистра сгенерировали максимально длинную последовательность, которая содержит все комбинации, кроме нулевой. То есть при разрядности регистра *m* можно получить последовательность длинной $2^m - 1$ [10].

Полиномиальный счётчик любой разрядности имеет ряд комбинаций отводов, которые обеспечат последовательность максимальной длины. Использование неверных комбинаций приведёт к генерации коротких последовательностей. Отдельная и довольно сложная задача – поиск этих комбинаций отводов. Заметим, что эти комбинации не всегда уникальны. К примеру, для 10-битного счётчика их существует две: [6; 11] и [2; 11], для шестиразрядного счётчика таких комбинаций 28. Чтобы найти эти комбинации, необходимо представить счётчик в виде полинома [3, 7]. Счётчики, рассмотренные на рисунке, будут иметь вид $X^2 XOR1$ и $X^2 XOR * XOR1$.

Из теории известно, что необходимым и достаточным условием генерации полной последовательности является примитивность характеристического полинома. Это значит, что:

- характеристический полином нельзя представить в виде произведения полиномов более низкой степени;
- характеристический полином является делителем полинома $z^{\delta} XOR1$ при $\delta = 2^m - 1$ и не является делителем при любых других значениях $\delta < 2^m - 1$.

Преимуществами полиномиального счётчика является простота как программной, так и аппаратной реализации, скорость работы и криптографическая стойкость [9, 11].

Численные характеристики стойкости и трудоемкости реализации рассмотренных алгоритмов генерации, их модернизация защитными преобразованиями будут рассмотрены в следующих работах.

Литература

1. Kendall M. G. The advanced theory of statistics. Vol. II / M. G. Kendall. – L.: C. Griffin & Co. Ltd, 1946. 521 p.

2. Press W. H. Numerical Recipes in C: The Art of Scientific Computing / W. H. Press, S. A. Teukolsky, W. T. Vetterling, B. P. Flannery. 2nd ed. – Cambridge Univ. Press, 1992. P. 277.

3. Bassham L. A Statistical test suite for random and pseudorandom number generators for cryptographic applications april 2010 / L. Bassham, A. Rukhin, J. Soto et al. // Comput. Security Division Inf. Technol. Laboratory Nat. Inst. of Standards and Technol. Gaithersburg, MD 20899-8930. – URL: http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf (дата обращения 28.11.2017).

4. Власенко А. В. Разработка алгоритмов, инструментов и методов авторизации пользователей в Web-приложениях с использованием хеш-функций / А. В. Власенко, П. И. Дзьобан, М. В. Тимченко // Вестн. Адыгейского гос. ун-та. Сер. 4: Естественно-математические и технические науки. 2015. № 4 (171). С. 144-150.

5. Власенко А. В. Защита конфиденциальной информации, передаваемой по открытым каналам связи / А. В. Власенко, В. Г. Смирнов // Изв. ЮФУ. Технические науки. 2003. № 4. С. 230-232.

6. Knuth E. D. The art of computer programming. Vol. 2. Polycycline algorithms / E. D. Knuth. – 2001. 788 p.

7. Козачок А. В. Обоснование возможности применения верификации программ для обнаружения вредоносного кода / А. В. Козачок, Е. В. Кочетков // Вопр. кибербезопасности. 2016. № 3 (16). С. 25-32.

8. Гнидко К. О. Моделирование индивидуального и группового поведения субъектов массовой коммуникации в p-адических системах координат для индикации уровня контаминации сознания / К. О. Гнидко, А. Г. Ломако // Вопр. кибербезопасности. 2016. № 2 (15). С. 54-68.

9. Жуков И. Ю. Принципы построения криптостойких генераторов псевдослучайных кодов / И. Ю. Жуков, М. А. Иванов, С. А. Осмоловский // Проблемы информационной безопасности. Компьютерные системы. 2001. № 1. С. 55-65.

10. Гончарук В. С. Методы генерации случайных чисел / В. С. Гончарук, Ю. С. Атаманов, С. Н. Гордеев // Молодой ученый. 2017. № 8. С. 20-23.

11. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях: учеб. пособие / М. А. Иванов, И. В. Чугунков; под ред. М. А. Иванова. – М.: НИЯУ МИФИ, 2012. 400 с.

Generation of the Pseudorandom Sequences on the Basis of the Linear Congruent Method and the Polynomial Counter

Vlasenko A. V., Dzyoban P. I.
Kuban State Technological University
Krasnodar, Russia
alex_vlasenko@list.ru, antiemoboy@mail.ru

Abstract. **Experts in information security field and information security often face need of generation of random series and numbers. Most often random numbers are required in tasks of simulation, the numerical analysis and testing, but there is also a set of other very specific tasks. It is known that in all modern languages of programming there is a random function or its analogs. These functions most often give really good pseudorandom numbers. In article features of implementation of the linear congruent method which is most often used as random, and a method of receiving random numbers by means of the polynomial counter which is often used for testing of an equipment are considered.**

Keywords: **random series, pseudo stochastic sequence, entropy, generator of the pseudorandom sequence, crypto security, the linear congruent method, polynomial counter.**

References

1. Kendall M. G. The Advanced Theory of Statistics. Vol. II. L., C. Griffin & Co. Ltd, 1946. 521 p.

2. Press W. H., Teukolsky S. A., Vetterling W. T., Flannery B. P. Numerical Recipes in C: The Art of Scientific Computing. 2nd ed. Cambridge Univ. Press, 1992. P. 277.

3. Bassham L., Rukhin A., Soto J., Nechvatal J., Smid M., Barker E., Leigh S., Levenson M., Vangel M., Banks D., Heckert N., Dray J. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications April 2010, *Comput. Security Division Inf. Technol. Laboratory Nat. Inst. of Standards and Technol. Gaithersburg*, MD 20899-8930. Available at: http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf (accessed 28.11.2017).

4. Vlasenko A. V., Dzoban P. I., Timchenko, M. V. Development of Algorithms, Tools and Methods of User Authorization in Web Applications Using Hash Functions [Razrabotka algoritmov, instrumentov i metodov avtorizatsii pol'zovateley v Web-prilozheniyakh s ispol'zovaniem khesh-funktsiy], *Bull. of Adyghe state Univ.*, *Series 4: Natural-mathematical and Technical Sci. [Vestnik Adygeyskogo gosudarstvennogo universiteta. Seriya 4: Estestvenno-matematicheskie i tekhnicheskie nauki]*, 2015, no. 4 (171), pp. 144-150.

5. Vlasenko A. V., Smirnov V. G. Protection of Confidential information Transmitted Over Open Channels of Communication [Zashchita konfidentsial'noy informatsii, peredavaemoy po otkrytym kanalam svyazi], *Izvestiya YuFU. Technical Sci. [Izvestiya YuFU. Tekhnicheskie nauki]*, 2003, no. 4, pp. 230-232.

6. Knuth E. D. The Art of Computer Programming. Vol. 2. Polycycline algorithms. 2001. – 788 p.

7. Kozachok A. V., Kochetkov E. V. Substantiation of Possibility of Application of Program verification to Detect Malicious Code [Obosnovanie vozmozhnosti primeneniya verifikatsii programm dlya obnaruzheniya vredonosnogo koda], *Cybersecurity [Voprosy kiberbezopasnosti]*, 2016, no. 3 (16), pp. 25-32.

8. Gnidko K. A., Lomako A. G. Modeling Individual and Group Behavior of Subjects of Mass Communication in the R-adic Coordinate Systems to Indicate the Level of Contamination of Consciousness [Modelirovanie individual'nogo i gruppovogo povedeniya sub''ektov massovoy kommunikatsii v r-adicheskikh sistemakh koordinat dlya indikatsii urovnya kontaminatsii soznaniya], *Cybersecurity [Voprosy kiberbezopasnosti]*, 2016, no. 2 (15), pp. 54-68.

9. Zhukov I. Yu., Ivanov M. A., Osmolovskii S. A. Principles of Construction of Cryptographically Strong Pseudorandom Codes [Printsipy postroeniya kriptostoykikh generatorov psevdosluchaynykh kodov], *Prob. Inf. Secur. Of the computer system [Problemy informatsionnoy bezopasnosti. Komp'yuternye sistemy]*, 2001, no. 1, pp. 55-65.

10. Goncharuk S. V., Atamanov Yu. S., Gordeev S. N. Methods of Random Number Generation [Metody generatsii sluchaynykh chisel], *The Young scientist [Molodoy uchenyy]*, 2017, no. 8, pp. 20-23.

11. Ivanov M. A., Chugunkov I. V. Cryptographic Methods of Information Protection in Computer Systems and Networks [Kriptograficheskie metody zashchity informatsii v komp'yuternykh sistemakh i setyakh]: textbook; ed. M. A. Ivanov. Moscow, Nat. Res. Nuclear Univ. MEPhI, 2012. 400 p.

Анализ веб-сервисов на наличие уязвимостей на примере сайта «XI Санкт-Петербургский конгресс „Профессиональное образование, наука и инновации в XXI веке“»

Кузьменкова Е. Ю., Саркисян А. Р., Кузнецов Д. А., Диасамидзе С. В.
Петербургский государственный университет
путей сообщения Императора Александра I
Санкт-Петербург, Россия
nessysar1995@gmail.com, sv.diass99@ya.ru

Аннотация. **Статья посвящена вопросам обеспечения безопасности веб-сайтов в интернете. Рассматриваются основные угрозы безопасности сайтов и методы защиты от них. В качестве объекта исследования информационной защищенности рассмотрен сайт «XI Санкт-Петербургский конгресс „Профессиональное образование, наука и инновации в XXI веке“», работающий под управлением системы WordPress – управления содержимым сайта. Описываются анализ сайта, его исходного кода и базы данных, включая проверку правильности настройки индексирования сайта, тестирование на проникновение. Для установления защищенного соединения между сервером и браузером пользователя получен SSL-сертификат сайта. Рассмотрен наиболее распространенный вид атаки на базу данных – SQL-инъекция (внедрение в запрос произвольного SQL-кода).**

Ключевые слова: **защита информации, безопасность данных, база данных, разработка сайта, конфиденциальность, WordPress, SQL.**

Введение

Проблема безопасности вебсайтов ещё никогда не стояла так остро, как в XXI веке. Конечно, это связано со всеобъемлющим распространением сети Интернет практически во всех отраслях и сферах деятельности человека. Каждый день хакеры и специалисты по безопасности находят по нескольку новых уязвимостей сайтов. Многие сайты тут же закрываются либо дорабатываются владельцами и разработчиками, а некоторые остаются незащищенными, чем и пользуются злоумышленники. А ведь с помощью взломанного сайта можно нанести большой вред как его пользователям, администраторам, так и серверам, на которых он размещён.

Исследования показывают, что, например, в 2013 г. в среднем на каждое веб-приложение приходилось 15,6 случаев уязвимости, а в 2014 г. данный показатель возрос до 29,9. Таким образом, среднее количество увеличилось за год почти в два раза. При этом для уязвимостей высокой степени риска данный показатель возрос более чем в два раза (с 2,8 до 7,5). Несмотря на наличие множества уязвимостей, которые могли быть обнаружены и их использование пресечено средствами защиты, механизмы безопасности по-прежнему используются очень мало. Из сказанного можно сделать вывод, что внимание к проблемам безопасности веб-приложений все еще остается на низком уровне.

Предметом исследования статьи является анализ информационной защищенности сайта «XI Санкт-Петербургский конгресс „Профессиональное образование, наука и инновации в XXI веке“» (http://congress-2017.ru). Сайт работает под управлением WordPress – одной из самых популярных систем управления содержимым сайта. В системе WordPress помимо основных блоков управления сайтом (управления контентом, дизайном, работы с медиафайлами) встроен модуль работы с базами данных и сервером баз данных MySQL, к которому предъявляются более высокие требования по защите информации.

Необходимым этапом разработки любого сайта как программного компонента информационных систем, взаимодействующих с критичными ресурсами (базой данных), является исследование разработанных программных решений в контексте информационной безопасности [1–4].

Для создания максимально эффективной подсистемы защиты сайта «XI Санкт-Петербургский конгресс „Профессиональное образование, наука и инновации в XXI веке“» проведен анализ основных угроз информационной безопасности вебсайтов и методов защиты от атак различного рода. Можно выделить следующие основные типы угроз:

- конфиденциальности – несанкционированный доступ к данным;
- целостности – несанкционированное искажение или уничтожение данных;
- доступности – ограничение или блокировка доступа к данным.

Для выявления типовых уязвимостей, через которые могут быть реализованы перечисленные угрозы, проведен аудит сайта. Процедуру аудита веб-сервиса с привязанной базой данных можно разделить на два этапа: анализ непосредственно самого сайта и его исходного кода и анализ базы данных.

Анализ сайта и его исходного кода

Сегодня WordPress [5] является самым популярным среди систем управления контентом. Его доля составляет 60,4 % общего числа сайтов, использующих CMS-движки. За 12 лет существования веб-движка в нем было обнаружено 242 уязвимости.

На первом этапе аудита выполнена проверка правильности настройки индексирования сайта с помощью запроса Google Dorks **site: congress-2017.ru inurl:/wp-content/**. Такие запросы из Google Dork или Google Dork Queries (GDQ) помогают выявить скрытые данные, являющиеся при этом общедоступными.

Указанный запрос позволил проверить, какие права доступа к различным веб-страницам сайта определены. В результате обнаружено, что у неавторизованных пользователей нет доступа к конфиденциальной информации на данном сайте, например, к информации об установленных плагинах и темах, к конфиденциальным данным или резервным копиям баз данных.

На следующем шаге аудита проводилось тестирование на проникновение. Чтобы подобрать нужный для взлома сайта эксплойт (компьютерную программу, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для атаки на вычислительную систему), злоумышленнику необходимо знать используемую при разработке версию WordPress. Такая информация содержится в исходном коде главной веб-страницы в метатеге **generator** (рис. 1).

```
<link rel="EditURI" type="application/rsd+xml" title="RSD"
<link rel="wlwmanifest" type="application/wlwmanifest+xml"
<meta name="generator" content="WordPress 4.8.2"/>
<style type="text/css" media="print">#wpadminbar{display:nc
<style type="text/css" media="screen">html{margin-top:32px!
body{margin-top:46px!important}}</style>
    </head>
    <body class="container">
        <header class="main-header">
            <div class="container clearfix">
```

Рис. 1. Выявление использованной версии WordPress через исходный код страницы сайта

Злоумышленник может подобрать данные учетной записи легального пользователя с помощью подачи запроса **congress-2017.ru/?author=1** и перебора всех возможных значений идентификатора пользователя.

Зная имя пользователя, можно попробовать подобрать пароль к панели администратора. Проблема подбора пароля решается путем либо использования стойких паролей, состоящих из 12 и более символов и включающих буквы верхнего и нижнего регистра, числа и спецсимволы, либо, например, встраивания плагина Login LockDown, который ограничивает количество неудачных попыток авторизации.

В целях безопасности в текст сайта были дополнительно установлены следующие плагины:

- **Revisium WordPress Theme Checker** – позволяет выявлять типичные вредоносные фрагменты в темах WordPress;
- **Sucuri Security** – позволяет проводить мониторинг и обнаруживать вредоносный код;
- **iThemes Security** – многофункциональный плагин для организации защиты платформы WordPress.

Для запрета доступа к критичной информации был изменен файл конфигурации **htaccess.** В этот файл добавлены опции запрета доступа к директориям и файлам, блокировки SQL-инъекций и вредоносных скриптов [2–4]. Это реализуется с помощью добавления в файл следующих правил:

1) закрытие списка файлов и папок: **Options+FollowSym Links–Indexes**;

2) противодействие скриптам, пытающимся установить глобальные переменные или изменить переменную _REQUEST через URL: **RewriteCond %{QUERY_STRING}GLOBALS (=|\[|\% [0–9A-Z]{0,2}) [OR]RewriteCond %{QUERY_ STRING}_REQUEST (=|\[|\% [0–9A-Z]{0,2})**;

3) ограничение доступа к критичным по отношению к безопасности файлам с помощью правил **Order Allow**, **Deny** и **Deny from all**.

К таким файлам можно отнести:

- wp-config.php – содержит имя БД, имя пользователя, пароль и префикс таблиц;
- .htaccess – файл конфигурации веб-серверов;
- readme.html и ru_RU.po – содержат версию WordPress;
- install.php – для работы с php.

Для установления защищенного соединения между сервером и браузером пользователя был получен SSL-сертификат сайта. SSL-сертификат [1] – цифровая подпись сайта, подтверждающая его подлинность. Он даёт возможность владельцу применить к своему сайту технологию SSL-шифрования. Информация передаётся в зашифрованном виде, и расшифровать её можно только с помощью специального ключа, являющегося частью сертификата. Тем самым гарантируется сохранность данных. Схема действия SSL представлена на схеме (рис. 2).

Рис. 2. Схема действия SSL

Когда пользователь заходит на защищённый сайт, выполняются проверка DNS и определение IP-адреса хоста веб-сайта. Затем, если запись веб-сайта найдена, происходит переход на веб-сервер хоста, а затем посылается запрос безопасного SSL-соединения с хоста веб-сайта. Хост отвечает валидным SSL-сертификатом. Таким образом устанавливается защищённое соединение и передаваемые данные шифруются.

Анализ базы данных

Наиболее распространенным видом атаки на базу данных является SQL-инъекция. Эта атака основана на внедрении в запрос произвольного SQL-кода. Это может дать возможность атакующему выполнить произвольный запрос к базе данных, например, прочитать содержимое любых таблиц, удалить, изменить или добавить данные, получить возможность чтения и/или записи локальных файлов и выполнения произвольных команд на атакуемом сервере.

Для работы с базами данных в WordPress предусмотрен класс **$wpdb**, включающий в себя метод **prepare ()** для обеспечения защиты от SQL-инъекций. Запросы к базе данных выглядят следующим образом:

$sql = $wpdb->prepare (‘query’ [, value_parameter, value_parameter …]).

Также необходимо заблокировать запросы к URL, содержащие определенные ключевые слова. Сделать это можно, добавив в файл **.htaccess** следующие строки:

RewriteCond%{query_string} concat.*\([NC, OR]
RewriteCond%{query_string} union.*select.*\([NC, OR]
RewriteCond%{query_string} union.*all.*select [NC]
RewriteRule ^ (.*)$ index.php [F, L]

Еще одним способом обеспечения защиты информации в базе данных является резервное копирование данных на случай их потери или удаления. Для этого используется соответствующая утилита **BackUpWordPress**.

Заключение

WordPress – довольно крупный и сложный продукт, который обладает своими достоинствами и недостатками. Среди последних имеется большое количество уязвимостей. В нашей статье рассмотрены и устранены наиболее типичные из них. Тем самым были сведены к минимуму шансы злоумышленника на компрометацию ресурса. В числе зарубежных публикаций по вопросу обеспечения информационной безопасности сайтов, на наш взгляд, можно рекомендовать статьи [6–10].

Литература

1. Корниенко А. А. Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч. / А. А. Корниенко, М. А. Еремеев, В. Н. Кустов и др.; под ред. А. А. Корниенко. – Ч. 2: Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте. – М.: УМЦ ЖДТ, 2014. 447 с.

2. Глухарев М. Л. Современные модели, методы и средства обеспечения безопасности семантических баз данных / М. Л. Глухарев, М. Ф. Исаева // Интеллектуальные системы на транспорте: материалы V междунар. науч.-практич. конф. «ИнтеллектТранс-2015». – СПб.: ПГУПС, 2015. С. 323-327.

3. Глухарев М. Л. Применение криптографических средств защиты информации в СУБД SQL Server: метод. указания / М. Л. Глухарев. – СПб.: ПГУПС, 2015. 16 с.

4. Vieira M. Using web security scanners to detect vulnerabilities in web services / M. Vieira, N. Antunes, H. Madeira // Dependable Systems & Networks 2009. DSN’09. IEEE/IFIP Int. Conf. 2009. P. 566-571.

5. WordPress. – URL: https://en.wordpress.com.

6. Wang H. Detecting syn flooding attacks / H Wang, D. Zhang, K. G. Shin // INFOCOM-2002. 21 Annual Joint Conf. IEEE Comput. and Communications Soc. Proc. IEEE, vol. 3. 2002. P. 1530-1539.

7. Ertaul L. Implementation of a Web Application for Evaluation of Web Application Security Scanners / L. Ertaul, Y. Martirosyan // Proc. Int. Conf. on Security and Management. – 2012. P. 82-89.

8. Rafique S. Systematic Review of Web Application Security Vulnerabilities Detection Methods / S. Rafique, M. Humayun, Z. Gul et al. // J. Comput. Commun. 2015. Vol. 3. P. 28-40.

9. Karumba M. C. A Hy-brid Algorithm for Detecting Web Based Applications Vulnerabilities / M. C. Karumba, S. Ruhiu, C. A. Moturi // Am. J. Comput. Res. Repository. 2016. Vol. 4 (1). P. 15-20.

10. Singh U. K. Information security assessment by quantifying risk level of network vulnerabilities / U. K. Singh, J. Chanchala, G. Neha // Int. J. Comput. Appl. 2016. Vol. 156.2. P. 37-44.

Настоящая статья опубликована при поддержке Федеральным государственным бюджетным образовательным учреждением высшего профессионального образования «Петербургский государственный университет путей сообщения Императора Александра I» инициативных научных работ, выполняемых студенческими научными коллективами.

Analysis of Web Services for Vulnerabilities on the Example of Site „XI St. Petersburg Congress 'Professional Education, Science and Innovations in the 21st Century'"

Kuzmenkova E. Yu., Sarkisyan A. R., Kuznetsov D. A., Diasamidze S. V.
Emperor Alexander I St. Petersburg State Transport University
St. Petersburg, Russia
nessysar1995@gmail.com, sv.diass99@ya.ru

Abstract. **Article is devoted to questions of safety of web sites on the Internet. The main security risks of the websites and methods of protection against them are considered. As an object of a research of information security the website „The XI St. Petersburg congress 'Professional Education, Science and Innovations in the 21st Century'" working under control of the WordPress system – website content management is considered. The analysis of the website and its source code and the analysis of the database is described, including: validation of setup of index of the website, testing for penetration. For establishment of the protected connection between the server and the user's browser, the SSL certificate of the website is received. The most widespread type of the attack to the database – a SQL injection is considered (implementation in a request of arbitrary SQL code).**

Keywords: **information protection, information security, database, website development, privacy, WordPress, SQL.**

References

1. Kornienko A. A., Eremeev M. A., Kustov V. N., Yakovlev V. V., Borodulin M. E., Glukharyov M. L., Diasamidze S. V. Information Security and Protection of Information on the Railway Transport [Informatsionnaya bezopasnost' i zashchita informatsii na zheleznodorozhnom transporte]: at 2 pm; ed. A. A. Kornienko. Part 2: Software and Hardware for information Security in Railway Transport [Programmno-apparatnye sredstva obespecheniya informatsionnoy bezopasnosti na zheleznodorozhnom transporte]. Moscow, Training Center for Railway Education, 2014. 447 p.

2. Glukharev M. L., Isaeva M. F. Modern Models, Methods and Tools for Ensuring the Safety of Semantic Databases [Sovremennye modeli, metody i sredstva obespecheniya bezopasnosti semanticheskikh baz dannykh]. *Intelligent systems in transport: Proc. 5th Int. Sci. Practical Conf. "IntellektTrans-2015" [Intellektual'nye sistemy na transporte: materialy V mezhdunarodnoy nauchno-prakticheskoy. konferenzii "IntellektTrans-2015"]*. St. Petersburg, PGUPS, 2015. Pp. 323-327.

3. Glukharev M. L. Application of Cryptographic information Security Tools in SQL Server. Methodical instructions [Primenenie kriptograficheskikh sredstv zashchity informatsii v SUBD SQL Server: metod. Ukazaniya]. St. Petersburg, PGUPS, 2015. 16 p.

4. Vieira M., Antunes N., Madeira H. Using Web Security Scanners to Detect vulnerabilities in Web Services. *Dependable Systems & Networks, DSN'09*, IEEE/IFIP Int. Conf., 2009, pp. 566-571.

5. WordPress. Available et: https://en.wordpress.com.

6. Wang H., Zhang D., Shin K. G. Detecting syn Flooding Attacks, *INFOCOM-2002. 21 Annual Joint Conf. IEEE Comput. and Communications Soc. Proc. IEEE*, vol. 3, 2002, pp. 1530-1539.

7. Ertaul L., Martirosyan Y. Implementation of a Web Application for Evaluation of Web Application Security Scanners, *Proc. Int. Conf. Security and Management*, 2012, pp. 82-89.

8. Rafique S., Humayun M., Gul Z., Abbas A., Javed H. Systematic Review of Web Application Security Vulnerabilities Detection Methods, *J. Comput. Communications*, 2015, vol. 3, pp. 28-40.

9. Karumba M. C., Ruhiu S., Moturi C. A. A Hybrid Algorithm for Detecting Web Based Applications Vulnerabilities, *Am. J. Comput. Res. Repository*, 2016, vol. 4 (1), pp. 15-20.

10. Singh U. K., Chanchala J., Neha G. Information security assessment by quantifying risk level of network vulnerabilities, *Int. J. Comput. Appl.*, 2016, vol. 156.2, pp. 37-44.

Исследование изменения фрактальности хаотических процессов на рынках капитала

Загайнов А. И.
Военно-космическая академия имени А. Ф. Можайского
Санкт-Петербург, Россия
zagainov239@gmail.com

Аннотация. **Описана методика выявления изменений фрактальных компонент временны́х рядов биржевых индексов валютных котировок, реализованная автором в математическом пакете MATLAB. Цель этой обработки хаотических данных состояла в выявлении участков детерминированности для установления вида динамического хаоса. Приведен пример детерминированного хаоса, установленного с помощью методики в одном из исследуемых временных рядов экономических показателей. Указаны индикаторы, способные разделять процессы на детерминированные и недетерминированные. Такая классификация является новой мерой численного понятия случайности.**

Ключевые слова: **хаотические временные ряды, биржевые индексы рынков капитала, корреляционная размерность, аппроксимированная энтропия.**

Введение

Наша статья посвящена раскрытию возможностей численного фрактального анализа при обработке временны́х рядов, сгенерированных рынками капитала [1–5]. Принципиальными вопросами анализа временны́х последовательностей наблюдений за рынками являются их нестационарность и наличие признаков хаотической динамики. Интерпретация указанных наблюдений как реализаций процессов динамического хаоса позволяет, с одной стороны, объяснить низкую эффективность диагностических схем, основанных на статистической обработке информации, а с другой стороны, дает потенциальную возможность для построения нового класса прогностических индикаторов, базирующихся на концепции фрактальной математики.

Фрактальные индикаторы состояния временного ряда и их изменение в режиме скользящего окна

Построение фрактала из исходного одномерного конечного сигнала связано с восстановлением его аттрактора. Это положение происходит из теории динамических систем, с которым на начальном этапе своего развития была неразрывно связана теория детерминированного хаоса. Данный факт отчетливо прослеживается в известной теореме Такенса [4, 6], в которой предложен способ построения восстановленного аттрактора, принадлежащего гладкому многообразию, в качестве координат вектора состояния положен тот же ряд, смещенный относительно себя на некоторое постоянное значение:

$$\vec{x}(i) = (x(i), x(i+\tau), ..., x(i+\tau(n-1))) = (x_1, x_2, ..., x_n), \quad (1)$$

где $x(i)$ – исходный временной ряд; n – размерность пространства вложения; τ – временная задержка; полученный вектор – координата одной точки на восстановленном аттракторе. При этом n удовлетворяет условиям теоремы Такенса:

$$n \geq 2[d_A] + 1, \quad (2)$$

где d_A – размерность восстановленного аттрактора.

Наиболее известными характеристиками аттрактора динамической системы являются вероятностные (фрактальные) размерности. Под вероятностью здесь понимается вероятность нахождения точки в определенной области самого аттрактора в фазовом пространстве. Их общим выражением является так называемая размерность Реньи (см. например [7]):

$$D_q = \frac{1}{1-q} \lim_{\varepsilon \to 0} \frac{\ln \sum_{i=1}^{M(\varepsilon)} p_i^q}{\ln(1/\varepsilon)}, \quad (3)$$

где $M(\varepsilon)$ – минимальное количество кубиков со стороной ε, полностью покрывающие аттрактор; p_i – вероятность посещения i-го кубика фазовой траекторией динамической системы.

В настоящее время этот параметр принят равным двум (корреляционная размерность является оценкой информационной размерности, для ее вычисления разработан универсальный численный алгоритм, из полученного алгоритма автоматически следует оценка соответствующей аппроксимированной энтропии). Из (3) следует, что корреляционная размерность есть

$$D_C = \frac{1}{1-2} \lim_{\varepsilon \to 0} \frac{\ln \sum_{i=1}^{M(\varepsilon)} p_i^2}{\ln(1/\varepsilon)} = \lim_{\varepsilon \to 0} \frac{\ln \sum_{i=1}^{M(\varepsilon)} p_i^2}{\ln(\varepsilon)}. \quad (4)$$

Последнее выражение удобно представить в следующей форме:

$$D_c = \lim_{\varepsilon \to 0} \frac{\ln(C(\varepsilon))}{\ln(\varepsilon)}, \quad (5)$$

где $C(r) = \lim_{m \to \infty} \frac{1}{m^2} \sum_{i,j=1}^{m} \theta(r - \rho(x_i, x_j))$ – корреляционный интеграл; $\theta(\alpha) = \begin{cases} 1, \alpha \geq 0; \\ 0, \alpha < 0 \end{cases}$ – функция Хевисайда; $\rho(x_i, x_j)$ – функция расстояния в n-мерном пространстве. Для аттрак-

торов, состоящих из конечного числа точек, корреляционный интеграл заменяется соответствующей оценкой:

$$C(r) = \sum_{i=1}^{M} \sum_{j=i+1}^{M} \frac{\theta(r - \rho(x_i, x_j))}{M(M-1)/2}, \quad (6)$$

где M – количество точек на восстановленном аттракторе.

Фрактальность исследуемого объекта предполагает

$$C(r) \sim r^{D_C}, \quad (7)$$

откуда следует, что

$$\ln C(r) \sim D_C \ln r, \quad (8)$$

и корреляционную размерность можно оценить, получив наклон прямой логарифма корреляционного интеграла.

Аппроксимированная энтропия отражает вероятность возникновения новых режимов при возрастании размерности пространства вложения. Чем она больше, тем больше неопределенностей в исходном сигнале. Для ее вычисления генерируются два аттрактора в последовательных пространствах вложения. Обычно (n + 1)-мерное пространство является следующим по отношению к условиям теоремы Такенса. Для оценки их схожести вычисляют корреляционный интеграл в каждом пространстве. При этом аппроксимированная энтропия находится из условия

$$ApEn(n, r) = -\ln\left(\frac{C^{n+1}(r)}{C^{n}(r)}\right). \quad (9)$$

Таким образом, находят аттрактор и вычисляют его корреляционную размерность и аппроксимированную энтропию по следующему алгоритму:

1) оценивают размерность пространства вложения;
2) оценивают параметр задержки;
3) нормируют расстояния между точками на аттракторе;
4) восстанавливают аттрактор и делают его возможную визуализацию, вычисляют корреляционный интеграл;
5) определяют скейлинговый диапазон;
6) оценивают корреляционную размерность в скейлинговом диапазоне (в двойном логарифмическом масштабе);
7) находят конкретное расстояние r при вычислении аппроксимированной энтропии и определяют ее для этого r.

При модификации рассматриваемых методов для учета их изменения в режиме реального времени (или изменения в режиме «скользящего окна», схематично изображенных на рис. 1) необходимо произвести перерасчет всех указанных параметров. Решение такой задачи даже на современных средствах вычислительной техники невозможно. При этом существует уже показанный ряд упрощений, связанный с видом предварительно рассчитанных значений корреляционной размерности и их аппроксимации в режиме «скользящего окна». Сказанное позволяет сформулировать следующий алгоритм вычисления фрактальных показателей:

1) задать постоянную размерность пространства вложения (на начальном этапе равную 3 и 4);
2) предварительно оценить параметр задержки с помощью предыдущего алгоритма. Запомнить полученный результат, а также вид построенных функций (автокорреляционной и функции средней взаимной информации);
3) выполнить нормирование расстояний между точками на аттракторе;
4) восстановить аттрактор и визуализировать его (в пространстве размерности 3), вычислить корреляционный интеграл;
5) определить скейлинговый диапазон;
6) предварительно оценить корреляционную размерность в скейлинговом диапазоне (в двойном логарифмическом масштабе);
7) определить конкретное расстояние r при вычислении аппроксимированной энтропии и вычислить ее для этого r;
8) проверить найденные значения (в пространствах вложения размерности 3 и 4). При необходимости увеличить размерность пространства вложения и повторить пункты 2–7;
9) сдвинуть временной ряд (перемещение окна выбирается апостериорно);
10) оценить параметр п. 2, изменив лишь значения отсчетов, относительно которых переместилось скользящее окно;
11) изменить аттрактор и корреляционный интеграл относительно отсчетов сместившегося окна;
12) найти оценку скейлингового диапазона относительно переместившегося окна;
13) дать оценку корреляционной размерности относительно нового местонахождения «скользящего окна»;
14) уточнить расстояние r и дать оценку аппроксимированной энтропии относительно нового местонахождения «скользящего окна»;
15) аппроксимировать полученные результаты трендами.

Разработанный MATLAB-скрипт

В пакете прикладных программ MATLAB разработан скрипт, позволяющий:

- строить графики двух- и трехмерного аттрактора (рис. 2, 3) для произвольной задержки τ;
- «проигрывать» исходный временной ряд в режиме «скользящего окна»;
- вычислять и «проигрывать» корреляционную размерность в режиме «скользящего окна»;
- вычислять и «проигрывать» аппроксимированную размерность в режиме «скользящего окна»;
- выводить результаты на совместном графике задержки.

Рис. 1. Способ перемещения «скользящего окна» с шириной 31 (длина окна) на 4 отсчета (перемещение окна)

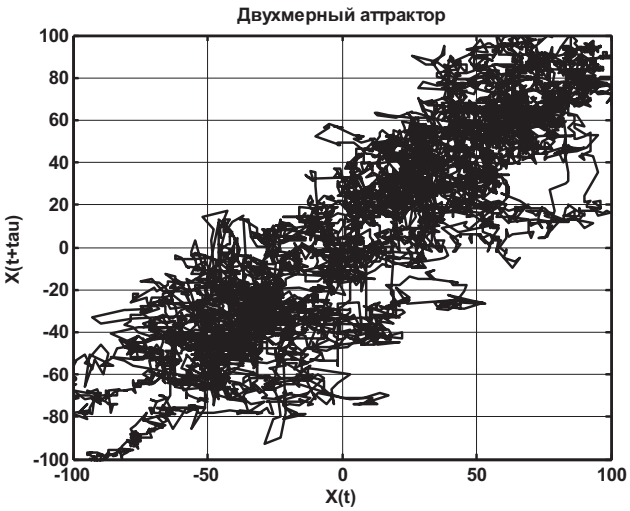


Рис. 2. Фрактал (двухмерный аттрактор) временно́го ряда отношения котировок валют с количеством игры на бирже 10 дней (14 400 отсчетов)

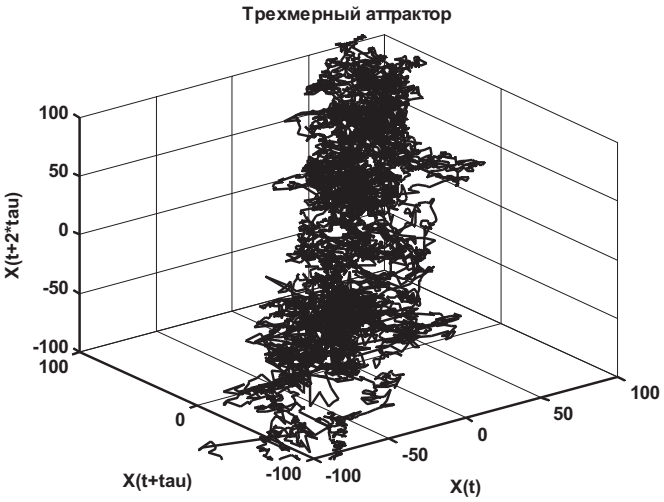


Рис. 3. Фрактал (трехмерный аттрактор) временно́го ряда отношения котировок валют с количеством игры на бирже 10 дней (14 400 отсчетов)

Результаты и их обсуждение

В исследовании были обработаны 16 временных рядов отношения различных котировок валют с количеством игры на бирже 10 дней (14 400 отсчетов). Для каждого временно́го ряда реконструированы аттракторы, произведена их визуализация для двух- и трехмерного случаев (например, рис. 2, 3), найдены необходимые параметры для вычислений. В работе построены тренды корреляционной размерности и аппроксимированной энтропии для всего времени исследования временно́го ряда, для удобного наблюдения и сравнения которых включена возможность отслеживания их изменений на совместном графике.

На рис. 4 приведен график временного ряда отношения котировок USD/CHF. Разработанная методика, к сожалению, не всегда обладает прогностическими способностями. Рассмотренный пример наглядно демонстрирует, что отсутствует явная видимая корреляция между рассмотренным типом фрактальной размерности и исходного временного ряда. Тот же результат был получен нами для аппроксимированной энтропии. Тем не менее, на рис. 5 рассмотрен график отношения других котировок (EUR/USD). В этом случае нами установлена постоянная корреляционная размерность (рис. 5б) и нулевая аппроксимированная энтропия (рис. 6б). Таким образом, мы можем заключить, что нами обнаружен случай детерминированного хаоса, который может быть восстановлен (хотя бы в теории) в виде динамической системы.

Последний результат является наиболее важным, поскольку показывает совершенство рассматриваемой методологии и указывает на индикаторы, способные разделять процессы на детерминированные и недетерминированные.

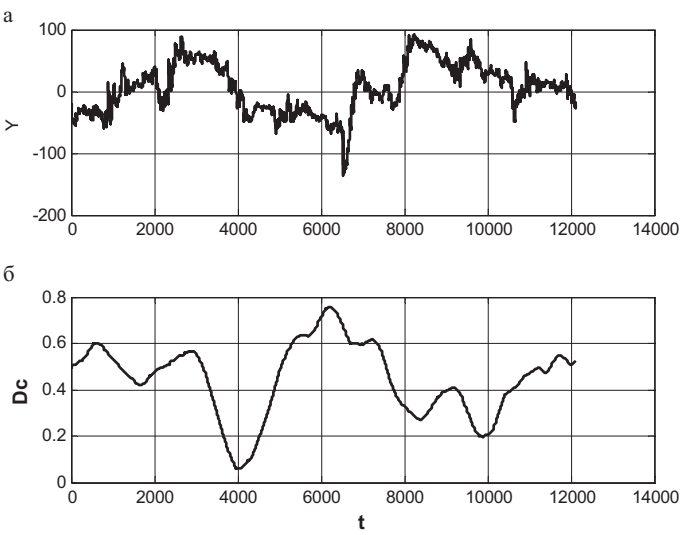


Рис. 4. Исходный временной ряд с количеством 10 дней обучения (14 400 отсчетов) (а)
и корреляционная размерность в режиме «скользящего окна» (б)
в зависимости от времени

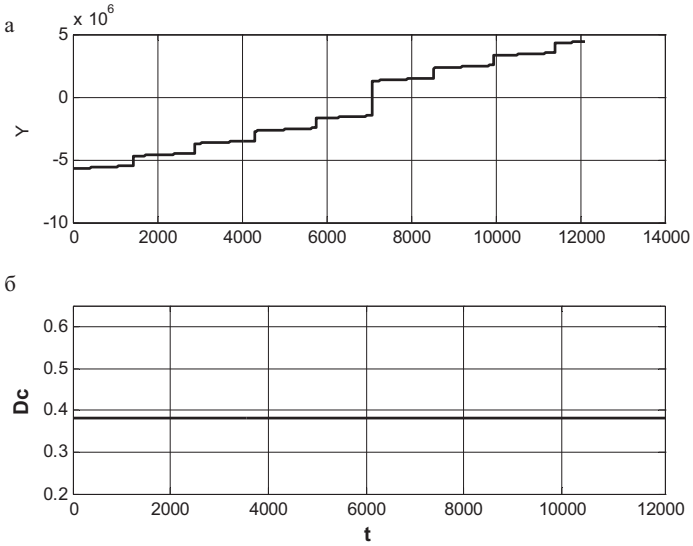


Рис. 5. Пример детерминированного временного ряда отношения биржевых индексов (а) и соответствующая постоянная корреляционная размерность (б) за все время наблюдения

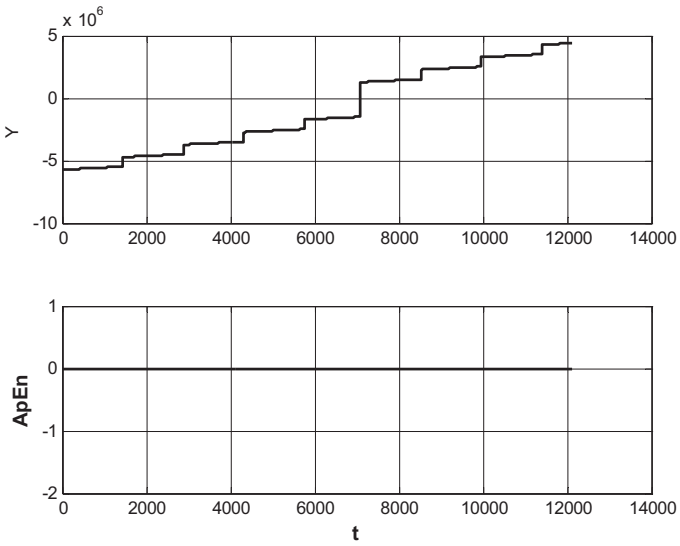


Рис. 6. Пример детерминированного временного ряда отношения биржевых индексов (а) и соответствующая нулевая аппроксимированная энтропия (б) за все время наблюдения

Такая классификация является новой мерой численного понятия случайности и будет предложена в дальнейшем.

Заключение

Данная статья посвящена раскрытию возможностей численного фрактального моделирования экономических временных рядов. В работе приведены основы указанной методологии, описаны возможности созданной программной реализации в математическом пакете прикладных программ MATLAB. Разработанные скрипты позволяют строить двух- и трехмерные аттракторы, в том числе в режиме реального времени, совместно рассматривать изменение исходного временного ряда и построенных корреляционной размерности и энтропии. В результатах работы приведены полученные графики изменения фрактальных показателей. Найден детерминированный случай (с постоянной корреляционной размерностью и нулевой аппроксимированной энтропией), что делает актуальной задачу нелинейной классификации рассматриваемых временных рядов относительно возможности детерминированного описания конечномерной нелинейной динамической системой. Приводятся рекомендации по использованию полученных результатов.

В заключение отметим, что систематическое изложение рассмотренного направления исследований дано в [8]. В числе заслуживающих внимания современных работ по рассмотренной тематике можно выделить статьи [9–11].

Литература

1. Петерс Э. Хаос и порядок на рынке капитала. Новый аналитический взгляд на циклы, цены и изменчивость рынка / Э. Петерс; пер. с англ.; под ред. А. Н. Романова. – М.: Мир, 2000. 334 с.

2. Мусаев А. А. Quod est veritas. Трансформация взглядов на системную составляющую наблюдаемого процесса / А. А. Мусаев // Тр. СПИИРАН. 2010. Вып. 15. С. 53-74.

3. Мусаев А. А. Статистический анализ инерционности хаотических процессов / А. А. Мусаев // Тр. СПИИРАН. 2014. Вып. 2 (33). С. 48-59.

4. Захаров А. И. Мультифрактальное математическое моделирование процессов хаотического происхождения / А. И. Захаров, А. И. Загайнов // Тр. ВКА им. А. Ф. Можайского. 2015. Вып. 648. С. 19-27.

5. Меклер А. А. Применение аппарата нелинейного анализа динамических систем для обработки сигналов ЭЭГ / А. А. Меклер // Актуальные проблемы современной математики: ученые записки. 2004. Т. 13 (2). С. 112-140.

6. Takens F. Detecting strange attractors in turbulence, in dynamical systems and turbulence / F. Takens // Lecture Notes in Mathematics / eds. D. A. Rand, L. S. Young. – Heidelberg, Springer-Verlag, 1981. P. 366-381.

7. Перерва Л. М. Фрактальное моделирование: учеб. пособие / Л. М. Перерва, В. В. Юдин // под общ. ред. В. Н. Грязника. – Владивосток: Изд-во ВГУЭС, 2007. 186 с.

8. Tsonis A. Chaos: from Theory to Applications / A. Tsonis. – NY: Plenum Press, 1992. 274 p.

9. Головко В. А. Нейросетевые методы обработки хаотических процессов / В. А. Головко // Научная сессия МИФИ-2005. VII всерос. науч.-технич. конф. «Нейроинформатика-2005»: Лекции по нейроинформатике. – М.: МИФИ, 2005. С. 43-91.

10. Czarnecki L. Comparison study of global and local approaches describing critical phenomena on the polish stock exchange market / L. Czarnecki, D. Grech, G. Pamula. – Physica A 387. 2008. P. 6801-6811.

11. Matteo Di T. Multi-scaling in finance / T. Di Matteo // Quantitatice Finance. 2007. № 7 (1). P. 21-36.

Investigation of the Change in the Fractality of Chaotic Pocesses in the Capital Markets

Zagaynov A. I.
Mozhaisky Military Space Academy named
St. Petersburg, Russia
zagainov239@gmail.com

Abstract. **The technique of detection of changes of fractal components of time series of market indexes of currency quotations realized by the author in a mathematical packet of MatLab is described. The purpose of similar processing of chaotic data consisted in detection of their sections of determinancy for establishment of a type of dynamic chaos. The example of the determined chaos set by means of a technique in one of the researched time series of economic indices is given. The indicators capable to separate processes on determined and nondeterministic are specified. Similar classification is a new measure of a numerical concept of randomness.**

Keywords: **chaotic time series, stock market indices of capital markets, correlation dimension, approximated entropy.**

References

1. Peters E. Chaos and Order in the Capital Market. A New Analytical Look at Cycles, Prices, and Market volatility [Khaos i poryadok na rynke kapitala. Novyi analiticheskiy vzglyad na tsykly, tseny, i izmenchivost rynka], ed. A. N. Romanov. Moscow, Mir, 2000. 334 p.

2. Musaev A. A. Quod est veritas. Transformation of Views on the System Component of the Observed Process [Transformatsiya vzglyadov na sistemnuyu sostavlyayushchuy nablyudaemogo processa], *Proc. SPIIRAS [Trudy SPIIRAN]*, 2010, is. 15, pp. 53-74.

3. Musaev A. A. Statistical Analysis of the Inertia of Chaotic Processes [Statichesky analiz inerzionnosti khaoticheskich pocessov], *Proc SPIIRAS [Trudy SPIIRAN]*, 2014, is. 2 (33), pp. 48-59.

4. Zakharov A. I., Zagaynov A. I. Multifractal Mathematical Modeling of Processes of Chaotic Origin [Multifraktalnoe matematicheskoe modelirovanie processov khaoticheskogo proishozhdeniya], *Proc. A. F. Mozhaysky Military Space Academy [Trudy voenno-kosmicheskoy akademii imeni A. F. Mozhaiskogo]*, 2015, is. 648, pp. 19-27.

5. Mekler A. A. Application of the Apparatus of Dynamic Non-linear Analysis Systems for the EEG Signal Processing [Primenenie apparata nelineynogo analisa dinamicheskikh system dlya obrabotki signalov EEG], *Actual problems of modern mathematics: scientists notes [Aktualnye problemy sovremennoy matematuki: uchenye zapiski]*, 2004, vol. 13 (2), pp. 112-140.

6. Takens F. Detecting Strange Attractors in Turbulence, in Dynamical Systems and Turbulence, *Lecture Notes in Mathematics*, eds. D. A. Rand, L. S. Young. Heidelberg, Springer-Verlag, 1981. Pp. 366-381.

7. Pererva L. M., Yudin V.V Fractal Modeling: study guide. [Fraktalnoe modelirovanie: uchebnoe posobie], Vladivostok, Publ. house VGUES, 2007. 186 p.

8. Tsonis A. Chaos: from Theory to Applications. NY, Plenum Press, 1992. 274 p.

9. Golovko V. A. Neural Network Methods of Processing Chaotic Processes [Neyrosetevye metody obrabotki khaoticheskikh processov]. *Proc. Scientific session of the MiFi 2005. VII All-Russia scientific-technical conference "Neuroinformatics 2005" Lectures on neuroinformatics [Trudy Nauchnay sessiya MIFI-2005. VII Vserossiyskaya nauchno-tehnicheskaya konferentciya „Neyroinformatika-2005": Lektcii po neyroinformatike].* Moscow, 2005, pp. 43-91.

10. Czarnecki L., Grech D., Pamula G. Comparison Study of Global and Local Approaches Describing Critical Phenomena on the Polish Stock Exchange Market. Physica A 387, 2008, pp. 6801-6811.

11. Matteo T. Di. Multi-scaling in Finance, *Quantitatice Finance*, 2007, no. 7 (1), pp. 21-36.