УДК 004.272:[519.87:519.248] DOI 10.18522/2311-3103-2022-4-95-103

**В.А. Павский, К.В. Павский**

# ОЦЕНКА ОСУЩЕСТВИМОСТИ РЕШЕНИЯ ЗАДАЧ НА ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМАХ ПРИ ГРУППОВОМ ОБСЛУЖИВАНИИ*

*Рост производительности вычислительных систем (ВС) связан как с масштабируемостью, так и с развитием архитектуры вычислительных элементов системы. Кластерные ВС, которые являются масштабируемыми, составляют 93% суперкомпьютеров списка Top500 и относятся к высокопроизводительным. При этом по – прежнему остается проблема эффективного и полного использования всего имеющегося вычислительного ресурса суперкомпьютера и ВС для решения пользовательских задач. Отказы элементарных машин (узлов, вычислительных модулей) снижают технико-экономическую эффективность вычислительных систем и эффективность решения пользовательских задач. Поэтому при планировании процесса решения задач, уменьшение потерь времени на восстановление ВС от сбоев, отказов является важной задачей. Для количественной оценки потенциальных возможностей вычислительных систем используются показатели осуществимости решения задач. Эти показатели характеризуют качество работы систем с учетом надежности, временных характеристик и параметров обслуживания поступающих задач. В работе предлагается математическая модель функционирования вычислительной системы с накопителем при групповом обслуживании потока задач. Математическая модель использует методы теории массового обслуживания, основанных на теории вероятностей и системах дифференциальных уравнений. Следует заметить, что методика составления систем дифференциальных уравнений достаточна проста, если представлена соответствующая им граф-схема. Однако точное решение систем уравнений и, как правило, в элементарных функциях, не существует, либо формулы труднообозримы. Здесь решение получено в стационарном режиме функционирования системы массового обслуживания. Рассчитаны показатели, позволяющие оценить наполненность накопителя. Полученные аналитические решения просты, могут быть использованы для экспресс-анализа функционирования вычислительных систем.*

*Вычислительные системы; накопитель; поток задач; групповое обслуживание; показатели осуществимости решения задач.*

**V.A. Pavsky, K.V. Pavsky**

# ESTIMATION OF REALIZABILITY OF SOLVING TASKS ON COMPUTER SYSTEMS IN GROUP MAINTENANCE

*The increase in the performance of computer systems (CS) is associated with both scalability and the development of the architecture of the computing elements of the system. Cluster CS, which are scalable, make up 93% of the Top500 supercomputers and are high-performance. At the same time, there is still the problem of efficient and complete use of all available computer resources of the supercomputer and CS for solving user tasks. Failures of elementary machines (nodes, computing modules) reduce the technical and economic efficiency of CS and the efficiency of solving user tasks. Therefore, when planning the process of solving problems, reducing the loss of time to restore CS from failures is an important problem. To quantify the potential capabilities of computer systems, indices of the realizability of solving tasks are used. These indices characterize the quality of the systems, taking into account reliability, time characteristics and service parameters of incoming tasks. The paper proposes a mathematical model of the functioning of a computer system with a buffer memory for group maintenance of a task flow. The mathematical model uses queuing theory methods based on probability theory and systems of differential equations. It should be noted that the method of composing systems of differential equations is simple*

* Работа выполнена в рамках государственного задания ИФП СО РАН (ГЗ 0242-2021-0011).

*enough if the corresponding graph scheme is presented. However, the exact solution of systems of equations and, as a rule, in elementary functions, does not exist, or formulas are difficult to see. Here the solution is obtained in the stationary mode of operation of the queuing system. The indices allowing to estimate the fullness of the buffer memory are calculated. The obtained analytical solutions are simple, can be used for express analysis of the functioning of computer systems.*

***C**omputer systems; buffer memory; task flow; group maintenance; indices of realizability of solving tasks.*

**Введение.** Рост производительности вычислительных систем связан как с развитием архитектуры вычислительных элементов, так и с масштабируемостью [1, 2]. Развитие высокопроизводительных систем наглядно демонстрирует список TOP 500 [3], например, кластерные ВС составляют 93% суперкомпьютеров этого списка. Для таких систем сохраняется крайне сложная проблема эффективного использования всего имеющегося вычислительного ресурса суперкомпьютера для решения пользовательских задач. Данная проблема еще более усложняется тем обстоятельством, что при современном уровне надежности элементной базы время между отказами ЭМ (элементарные машины, узлы, вычислительные модули) вычислительной системы может измеряться часами или даже минутами [4, 5].

Отказы ЭМ снижают технико-экономическую эффективность ВС и эффективность решения задач [2, 6]. Поэтому актуальным является организация функционирования ВС и анализ надежности их потенциальных возможностей [7–14].

Для оценки потенциальных возможностей вычислительных систем используют показатели осуществимости решения задач. Эти показатели характеризуют качество работы систем с учетом надежности ВС и параметров поступающих задач [2]. В работе предлагается математическая модель для расчета показателей осуществимости решения задач, в режиме обслуживания потока задач на ВС с накопителем.

Постановка задачи. В накопитель вычислительной системы поступают задачи, из которых формируются пакеты фиксированного размера с последующей их обработкой в ВС. Требуется оценить эффективность работы накопителя (рис. 1). Считается, что накопитель может находиться в двух состояниях, либо переполненное, если число задач в нем больше критического уровня, либо нормальное -- число задач меньше значения заданного уровня.

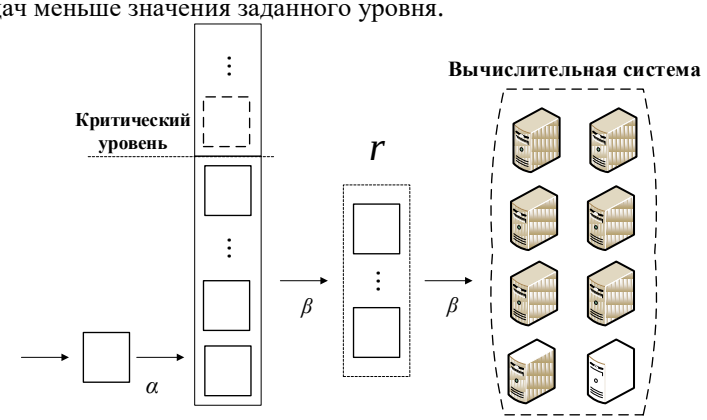


*Рис. 1. Модель системы с накопителем*

Математическая модель выполнена в рамках теории массового обслуживания [15–19], где под потоком требований понимаем: в первом случае -- поток поступающих задач на обслуживание с известной интенсивностью, в другом случае --

поток отказов элементарных машин (ЭМ) с последующим, также известным, восстановлением. Предполагается, что случайные потоки простейшие. Параметр $\alpha$ -- интенсивность поступающих задач, а $\beta$ -- интенсивность решения задач, зависящая от числа исправных ЭМ в масштабируемых ВС [1, 14].

**1. Математическая модель**. На систему массового обслуживания (СМО) поступает пуассоновский поток требований интенсивностью $\alpha$. Требования обслуживаются группами; время обслуживания группы из $r$ требований подчинено экспоненциальному распределению с параметром $\beta$, $\alpha<\beta$ [17]. В каждый момент времени $t \in [0,\infty)$, СМО находится в одном из множества $C_k$ несовместных состояний (см. рис.2), $k$ число требований в системе. Если система находится в состоянии $C_k$, то $l = \begin{cases} r, & \text{если } k \geq r, \\ k, & \text{если } o \leq k < r \end{cases}$ требований покидают систему с интенсивностью $\beta$ и система переходит в состояние $C_{k-l}$. Если в систему приходит требование, то система переходит из состояния $C_k$ в состояние $C_{k+1}$. На рис. 2 представлена граф-схема состояний СМО.

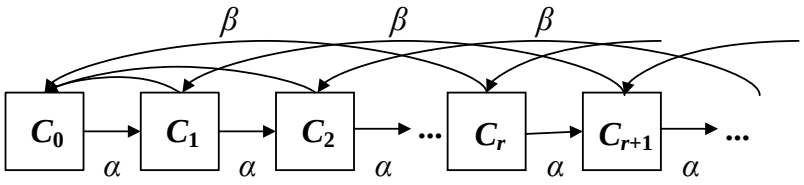


*Рис. 2. Размеченный граф состояний, описывающий процесс с групповым восстановлением*

Граф-схема формализуется системой дифференциальных уравнений как функций времени [15–17] для неизвестных вероятностей $P_k(t)$, того, что СМО находится в состоянии $C_k$. в момент времени $t$. Имеем, систему

$$\begin{cases} \frac{dP_0(t)}{dt} = -\alpha P_0(t) + \beta(P_1(t) + P_2(t) + \ldots + P_r(t)), \\ \frac{dP_k(t)}{dt} = -(\alpha+\beta)P_k(t) + \beta P_{k+r}(t) + \alpha P_{k-1}(t), \quad k \geq 1 \end{cases} \tag{1}$$

с условием нормировки $\sum_{k=1}^{\infty} p_k(t) = 1$, $t \in [0,\infty)$. Рассмотрим стационарный режим функционирования СМО, где $p_k = \lim_{t\to\infty} P_k(t)$, тогда из (1) получаем

$$\begin{cases} \alpha p_0 = \beta(p_1 + p_2 + \ldots + p_r), \\ (\alpha+\beta)p_k = \beta p_{k+r} + \alpha p_{k-1}, \quad k \geq 1. \end{cases} \tag{2}$$

Для решения алгебраической системы уравнений (2) используем метод производящих функций [20], которые при $|z| \leq 1$ обычно имеют вид

$$H(z) = \sum_{k=0}^{\infty} p_k z^k \quad . \tag{3}$$

Каждое уравнение $k$ системы (2) умножаем на $z^k$, где $k$=0,1,.. соответствует номеру уравнения, и суммируем. После стандартных преобразований, получаем алгебраическое уравнение

$$(\alpha+\beta)(H(z) - p_0) = \frac{\beta}{z^r}\left(H(z) - \sum_{k=0}^{r} p_k z^k\right) + \alpha z H(z),$$

из которого, предварительно, приведя к общему знаменателю $z^r$, находим

$$H(z) = (\beta \sum_{k=0}^{r} p_k z^k - (\alpha+\beta)p_0 z^r)/(\alpha(z - (\alpha+\beta))z^r + \beta). \tag{4}$$

Из системы (2) и определения функции $H(z)$ (3) следует, что

$$-(\alpha+\beta)p_0 z^r = -\beta z^r \sum_{k=0}^{r} p_k z^k.$$

Подставляя правую часть в уравнение (4) и объединяя суммы, получим

$$H(z) = \frac{\beta \sum_{k=0}^{r} p_k \, (z^k - z^k)}{\big(\alpha z - (\alpha + \beta)\big) z^r + \beta}.$$

Знаменатель дроби - многочлен степени $r$+1. Один корень $z$=1, другой $z$=0, а оставшиеся $r$-1корней, по теореме Руше, имеют один $|z_0|>1$, а остальные $|z|<1$. Числитель и знаменатель дроби у $H(z)$ должны быть пропорциональны, поскольку производящая функция является многочленом, отсюда

$$\frac{\mathrm{A}\beta \sum_{k=0}^{r} p_k \, (z^k - z^k)}{z - 1} = \frac{\big(\alpha z - (\alpha + \beta)\big) z^r + \beta}{(z - 1)(z - z_0)}$$

где А – коэффициент пропорциональности.

Перепишем последнее выражение в виде

$$\frac{\mathrm{K}\beta \sum_{k=0}^{r} p_k (z^k - z^k)}{1 - z} = \frac{(\alpha z - (\alpha + \beta)) z^r + \beta}{(1 - z)(1 - z/z_0)},$$

где K=A$z_0$, отсюда $H(z)=\frac{1}{K(1-z/z_0)}$. При $z$=1 , $H(1) = 1$, следовательно, $\mathrm{K} = 1/(1 - 1/z_0)$. Таким образом

$$H(z) = \frac{1 - 1/z_0}{1 - z/z_0}. \qquad (5)$$

Из (3) имеем, что $H(0)= p_0$, тогда из (5)

$$p_0 = 1 - 1/z_0. \qquad (6)$$

Последовательно дифференцируя производящую функцию (5) и полагая z=0, находим

$$p_k = (1 - 1/z_0)(1/z_0)^k, \quad k = 0,\ 1,\ 2,\ \ldots,\ z_0>1.$$

Следовательно,

$$p_k = p_0(1 - p_0)^k, \quad k = 0,\ 1,\ 2,\ \ldots \qquad (7)$$

Воспользуемся первым уравнением из (2).

$\alpha p_0 = \beta(p_1 + p_2 + \ldots + p_r)$.

Рассмотрим два крайних случая этого уравнения при r=1 и $r \to \infty$,

$$\beta p_1 \le \alpha p_0 \le \beta \sum_{k=1}^{\infty} p_k,$$

$$\beta p_0(1 - p_0) \le \alpha p_0 \le \beta(1 - p_0). \qquad (8)$$

Из левой части неравенства (8) (сравнение со случаем при $r$=1

$$\beta(1 - p_0) \le \alpha,$$

Следовательно,

$$\frac{\beta - \alpha}{\beta} \le p_0.$$

Из правой части неравенства (8) (т.е. имеем сравнение со случаем $r \to \infty$) следует, что

$$p_0 \le \frac{\beta}{\alpha + \beta}.$$

Тогда, можем сформулировать следующее утверждение.

***Утверждение.*** Для математической модели с групповым обслуживанием, представленной системой уравнений (2), оценкой для вероятности $p_0$ является двойное неравенство

$$\frac{\beta - \alpha}{\beta} \le p_0 \le \frac{\beta}{\alpha + \beta}. \qquad (9)$$

Используя (2), (7) и (9) получаем, что
при $r$=1

$$p_0 = \frac{\beta-\alpha}{\beta}; \quad (10)$$

при $r$=2

$$p_0 = \frac{1}{2}(3 - \sqrt{1+4\frac{\alpha}{\beta}}); \quad (11)$$

при $r \to \infty$

$$p_0 = \frac{\beta}{\alpha+\beta}. \quad (12)$$

**2. Расчет моментов случайных величин.** Производящая функция (3), на основании (6), может быть записана в следующем виде

$$H(z) = \frac{p_0}{1-z(1-p_0)} \quad (13)$$

На основании свойства производящих функций [20] для первого и второго центрального момента для случайной величины $X$ -- числа требований в системе

$$M(X) = H'(1),$$

$$D(X) = H''(1) + H'(1) - H'^2(1),$$

получаем, что производная $n$-го порядка для (13) равна

$$H(z)^{(n)}\Big|_{z=1} = \frac{n!p_0(1-p_0)^n}{(1-z(1-p_0))^{n+1}}\Big|_{z=1} = \frac{n!(1-p_0)^n}{{p_0}^n}.$$

Откуда математическое ожидание и дисперсия равны

$$M(X) = \frac{p_0(1-p_0)}{(1-z(1-p_0))^2}\Big|_{z=1} = \frac{1-p_0}{p_0}, \quad (14)$$

$$D(X) = \frac{2(1-p_0)^2}{{p_0}^2} + \frac{1-p_0}{p_0} - (\frac{1-p_0}{p_0})^2 = \frac{1-p_0}{{p_0}^2}. \quad (15)$$

Используя (9)-(10), легко найти значения $M(X)$ и $D(X)$ (см (14) и (15)), при $r$=1, 2 и $r \to \infty$.

***Пример.*** Пусть интенсивности входящего потока задач $\alpha$=15 1/ч, исходящего потока $\beta$=20 1/ч, тогда на основании (10)-(12) и (14), (15):

при $r$=1 получаем, что средняя наполняемость накопителя равна $M(X)$=3 с соответствующей дисперсией $D(X)$=12;

при $r$=2 средняя наполняемость накопителя равна $M(X)$= 1 с дисперсией $D(X)$= 2;

при $r \to \infty$ средняя наполняемость накопителя равна $M(X)$= 3/4 с дисперсией $D(X)$=21/16.

**3. Функция распределения времени перехода накопителя из переполненного состояния в нормальное.** Пусть $\eta$ – случайная величина, отражающая время перехода из переполненного состояния накопителя в нормальное состояние, тогда функция $F(t,r)$ нахождения накопителя в переполненном состоянии в течение времени $t \in [0,\infty)$ при обработке требований группами, размером $r$, запишется в виде

$$F(t,r) = P\{\eta \geq t\}.$$

Пусть $s$ – число задач в накопителе, начиная с которого считаем, что накопитель переполнен. Тогда, если система функционирует достаточно долго, то $P\{\eta=0\}=p_{отк}$ где $p_{отк} = 1 - \sum_{k=0}^{s-1} p_k$ постоянна для любого $t \in [0,\infty)$.

Пусть $a = 1 - p_0$, тогда на основании (7) $p_0 = (1-a)a^k$, $p_{\text{отк}} = a^s$.

Далее,

$$P\{\eta \geq t\} = \sum_{k=s}^{m} p_k P_k\{\eta \geq t\},$$

где $P_k\{\eta \geq t\}$ – вероятность того, что на обработку $k$ требований будет затрачено времени не менее $t$, а $m$ – допустимое количество требований, ожидающих обработку в накопителе (в дальнейшем это число будет использовано при оценке погрешности $F(t,r)$).

Принимаем, что в стационарном режиме поток обслуживания простейший, т.е. имеем распределение Пуассона.

***Вывод функции*** $F(t,r)$. Итак, при $k \geq s$ накопитель находится в переполненном состоянии, а обработка требований осуществляется группами по $r$ требований, с интенсивностью $\beta$.

Имеем

$$P_k\{\eta \geq t\} = \sum_{j=0}^{[(k-s)/r]} \frac{(\beta t)^j}{j!} exp(-\beta t).$$

где [x] целая часть числа x.

$$P\{\eta \geq t\} = \sum_{k=s}^{m} (1-a)a^k \sum_{j=0}^{[(k-s)/r]} \frac{(\beta t)^j}{j!} exp(-\beta t).$$

Допускаем $m \to \infty$, тогда

$$\tilde{F}(t,r) = \sum_{k=s}^{\infty} (1-a)a^k \sum_{j=0}^{[(k-s)/r]} \frac{(\beta t)^j}{j!} exp(-\beta t),$$

Учитывая, что при $k \geq s$ (по условию $s > 0$) имеем $p_k = p_{\text{отк}} p_{k-s}$, откуда

$$\tilde{F}(t,r) = exp(-\beta t)a^s \sum_{k=0}^{\infty} (1-a)a^k \sum_{j=0}^{[k/r]} \frac{(\beta t)^j}{j!}$$

Изменяем порядок суммирования и замечаем, что $\sum_{k=0}^{\infty}(1-a)a^k = 1$, тогда

$$\tilde{F}(t,r) = exp(-\beta t)a^s \sum_{j=0}^{\infty} \frac{(\beta t)^j}{j!} (a^r)^j.$$

$$\tilde{F}(t,r) = a^s \, exp(-\beta t) \, exp(a^r \beta t),$$

$$F(t,r) \approx \tilde{F}(t,r) = p_{отк} \, exp(-(1-a^r)\beta t). \quad (16)$$

Приведем погрешность $\Delta(t,m)$ функции $F(t,r) \approx \tilde{F}(t,r)$, определяемой формулой (16), и соответственно, с принятым допущением, что $m \to \infty$. Имеем

$$\Delta(t,m) = a^{m-r+1} \sum_{k=r}^{\infty} (1-a)a^k \sum_{j=0}^{[k/r]-1} \frac{(\beta t)^j}{j!} exp(-\beta t),$$

$$\Delta(t,m) = \sum_{k=m+1}^{\infty} (1-a)a^k \sum_{j=0}^{k-r} \frac{(\beta t)^j}{j!} exp(-\beta t).$$

После преобразований, аналогичных выводу функции (16), при $a = 1 - p_0$, получаем

$$\Delta(t,m) = (1-p_0)^{m-r+1} F(t,r). \quad (17)$$

Погрешность $\Delta(t,m)$ определяет точность расчета функции $F(t,r) \approx \tilde{F}(t,r)$

Тогда из (15) функция распределения времени перехода накопителя из переполненного состояния в нормальное запишется в виде:

$$G(t,r) = 1 - \frac{F(t,r)}{p_{отк}} = 1 - exp(-(1-(1-p_0)^r)\beta t) \, . \quad (18)$$

Полученные формулы определяют вероятность (16) нахождения накопителя в переполненном состоянии и функцию (18) – распределения времени перехода накопителя из переполненного состояния в нормальное при групповой обработке задач с погрешностью (17).

На рис. 3 представлен пример для функции распределения $G(t,r)$ (см. (18)) при $r$=1, 2 и $r\to\infty$. Из графика видно, как влияет размер группы на обработку задач.

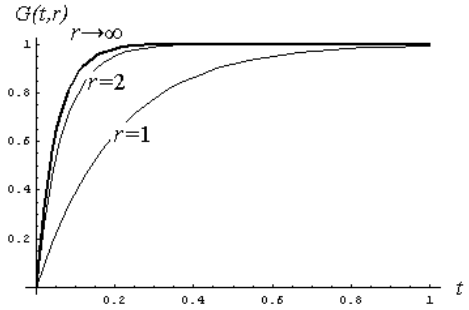


*Рис. 3. Расчет функции $G(t,r)$ для группы r=1, 2 и $r\to\infty$ при α=15 1/ч, β=20 1/ч*

**Заключение**. Представлена математическая модель вычислительной системы с накопителем при групповом обслуживании потока задач. Получена вероятность нахождения накопителя в переполненном состоянии и функция распределения времени перехода накопителя из переполненного состояния в нормальное (штатное), при групповой обработке задач. Предложены формулы для расчета показателей, позволяющих оценить наполненность накопителя в среднем – математическое ожидание, дисперсия. Все формулы обладают наглядностью и простотой, удобны в экспресс анализе функционирования вычислительных систем. Для точных расчетов полученных показателей, как функций времени, требуется решить предложенную систему дифференциальных уравнений, решение которой доступно численными методами

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Dongarra J.J., A.J. van der Steen*. High-performance computing systems: Status and outlook // Acta Numerica. – 2012. – P. 1-96.
2. *Хорошевский В.Г.* Архитектура вычислительных систем. – М.: МГТУ им. Баумана, 2008. – 520 с.
3. TOP500 Supercomputers Official Site. TOP500 Lists 2021. – http://www.top500.org.
4. *Gupta S., Patel T., Engelmann C. and Tiwari D.* Failures in large scale systems: long-term measurement, analysis, and implications SC '17: Proc. of the International Conference for High Performance Computing, Networking, Storage and Analysis (Denver, Colorado). – 2017. – Vol. 44.
5. *Schroeder B. and Gibson Garth.* A 2006 large-scale study of failures in high-performance computing systems // Proceedings of the International Conference on Dependable Systems and Networks (DSN2006) (Philadelphia, PA, USA). – P. 10.
6. *Korobkin V., Melnik E., Klimenko A*. Fault-tolerant architecture for the hazardous object information control systems // Application of information and communication technologies - AICT2015 (IEEE catalog number CFPI556H-PRT): conference proceedings (Rostov-on-Don, Russia 14-16 October 2015). – Rostov-on-Don: SFedU, 2015. – P. 274-276.
7. *Хорошевский В.Г.* Модели анализа и организации функционирования большемасштабных распределенных вычислительных систем // Электронное моделирование. – Киев, 2003. – Т. 25, № 6.
8. *Xie M., Dai Y.S. and Poh K.L.* Computing system reliability: models and analysis. – New York: Kluwer academic publishers, 2004.
9. *Blischke W.R. and Murthy D.N.P*. Reliability. – New York: Wiley, 2000
10. *Hoyland A., Rausand M.* System reliability theory. – New York: Wiley, 1994.
11. *Kuo W., Zuo M.J.* Optimal reliability modeling: principles and applications. – New York: Wiley, 2003.

12. *Mor Harchol-Balter*. Performance Modeling and Design of Computer Systems: Queueing Theory in Action. – Cambridge University Press, 2013.
13. *Чечельницкий А.А., Кучеренко О.В.* Стационарные характеристики параллельно функционирующих систем обслуживания с двумерным входным потоком // Сб. научных статей. – Минск, 2009. Вып. 2. – С. 262-268.
14. *Pavsky V.A., Pavsky K.V.* Stochastic models and calculations of distributed computer systems reserve size // Proc. of 2019 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon), Vladivostok, Russia, 2019. – P. 1-5.
15. *Назаров А.А., Терпугов А.Ф.* Теория массового обслуживания. – Томск: Изд-во НТЛ, 2010. – 228 с.
16. *Саати Т.Л.* Элементы теории массового обслуживания и ее приложения. – 3-е изд. – М.: Книжный дом «ЛИБРОКОМ», 2010. – 520 с.
17. *Клейнрок Л.* Теория массового обслуживания. – М.: Машиностроение, 1979. – 432 с.
18. *Боровков А.А.* Вероятностные процессы в теории массового обслуживания. – М.: Наука, 1972. – 368 с.
19. *Вентцель Е.С.* Теория случайных процессов и ее инженерные приложения. – М.: Наука, 1991. – 384с.
20. *Феллер В.* Введение в теорию вероятностей и ее приложения: в 2-х т. – Т. 1. – М: ЛИБРОКОМ, 2010. – 528 с.

REFERENCES

1. *Dongarra J.J., A.J. van der Steen*. High-performance computing systems: Status and outlook, *Acta Numerica*, 2012, pp. 1-96.
2. *khoroshevskiy V.G.* Arkhitektura vychislitel'nykh system [Architecture of computing systems]. Moscow: MGTU im. Baumana, 2008, 520 p.
3. TOP500 Supercomputers Official Site. TOP500 Lists 2021. Available at: http://www.top500.org.
4. *Gupta S., Patel T., Engelmann C. and Tiwari D.* Failures in large scale systems: long-term measurement, analysis, and implications *SC '17: Proc. of the International Conference for High Performance Computing, Networking, Storage and Analysis (Denver, Colorado), 2017*, Vol. 44.
5. *Schroeder B. and Gibson Garth.* A 2006 large-scale study of failures in high-performance computing systems, *Proceedings of the International Conference on Dependable Systems and Networks (DSN2006) (Philadelphia, PA, USA)*, pp. 10.
6. *Korobkin V., Melnik E., Klimenko A*. Fault-tolerant architecture for the hazardous object information control systems, *Application of information and communication technologies - AICT2015 (IEEE catalog number CFPI556H-PRT): conference proceedings (Rostov-on-Don, Russia 14-16 October 2015)*. Rostov-on-Don: SFedU, 2015, pp. 274-276.
7. *Khoroshevskiy V.G.* Modeli analiza i organizatsii funktsionirovaniya bol'shemasshtabnykh raspredelennykh vychislitel'nykh sistem [Models of analysis and organization of functioning of large-scale distributed computing systems], *Elektronnoe modelirovanie* [Electronic modeling]. Kiev, 2003, Vol. 25, No. 6.
8. *Xie M., Dai Y.S. and Poh K.L.* Computing system reliability: models and analysis. New York: Kluwer academic publishers, 2004.
9. *Blischke W.R. and Murthy D.N.P*. Reliability. New York: Wiley, 2000
10. *Hoyland A., Rausand M.* System reliability theory. New York: Wiley, 1994.
11. *Kuo W., Zuo M.J.* Optimal reliability modeling: principles and applications. New York: Wiley, 2003.
12. *Mor Harchol-Balter*. Performance Modeling and Design of Computer Systems: Queueing Theory in Action. Cambridge University Press, 2013.
13. *Chechel'nitskiy A.A., Kucherenko O.V.* Statsionarnye kharakteristiki parallel'no funktsioniruyushchikh sistem obsluzhivaniya s dvumernym vkhodnym potokom [Stationary characteristics of parallel functioning service systems with a two-dimensional input stream], *Sb. nauchnykh statey* [Collection of scientific articles]. Minsk, 2009. Issue 2, pp. 262-268.
14. *Pavsky V.A., Pavsky K.V.* Stochastic models and calculations of distributed computer systems reserve size, *Proc. of 2019 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon), Vladivostok, Russia, 2019*, pp. 1-5.

15. *Nazarov A.A., Terpugov A.F.* Teoriya massovogo obsluzhivaniya [Queuing theory]. Tomsk: Izd-vo NTL, 2010, 228 p.
16. *Saati T.L.* Elementy teorii massovogo obsluzhivaniya i ee prilozheniya [Elements of the theory of queuing and its applications]. 3 ed. Moscow: Knizhnyy dom «LIBROKOM», 2010, 520 p.
17. *Kleynrok L.* Teoriya massovogo obsluzhivaniya [Theory of queuing]. Moscow: Mashinostroenie, 1979, 432 p.
18. *Borovkov A.A.* Veroyatnostnye protsessy v teorii massovogo obsluzhivaniya [Probabilistic processes in the theory of queuing]. Moscow: Nauka, 1972, 368 p.
19. *Venttsel' E.S.* Teoriya sluchaynykh protsessov i ee inzhenernye prilozheniya [Theory of random processes and its engineering applications]. Moscow: Nauka, 1991, 384 p.
20. *Feller V.* Vvedenie v teoriyu veroyatnostey i ee prilozheniya [Introduction to probability theory and its applications]: In 2 vol. Vol. 1. Moscow: LIBROKOM, 2010, 528 p.

Статью рекомендовал к опубликованию д.т.н., профессор Б.М. Глинский.

**Павский Валерий Алексеевич** – Кемеровский государственный университет (КемГУ); e-mail: pavva46@mail.ru; г. Кемерово, Россия; тел.: +73842396832; д.т.н.; профессор; профессор кафедры общей математики и информатики

**Павский Кирилл Валерьевич** – Институт физики полупроводников им. А.В. Ржанова СО РАН (ИФП СО РАН); e-mail: pkv@isp.nsc.ru; г. Новосибирск, Россия; тел.: +73833332171, 3305626; д.т.н.; доцент; зав. лабораторией вычислительных систем; профессор кафедры вычислительных систем Сибирского государственного университета телекоммуникаций и информатики (СибГУТИ).

**Pavsky Valery Alekseevich** – Kemerovo State University; e-mail: pavva46@mail.ru; Kemerovo, Russia; phone: +73842396832; dr. of eng. sc.; professor; professor of department of general mathematics and informatics.

**Pavsky Kirill Valerievich** – Rzhanov Institute of Semiconductor Physics Siberian Branch of Russian Academy of Sciences; e-mail: pkv@isp.nsc.ru; Novosibirsk, Russia; phone: +73833332171, 3305626; dr. of eng. sc.; head of computer systems laboratory; professor of computer systems department, SibSUTIS.

УДК 004.056 DOI 10.18522/2311-3103-2022-4-103-112

**И.Д. Русаловский, Л.К. Бабенко, О.Б. Макаревич**

## РАЗРАБОТКА МЕТОДОВ ГОМОМОРФНОГО ДЕЛЕНИЯ*

*Рассматриваются проблемы гомоморфной криптографии. Гомоморфная криптография – одно из молодых направлений криптографии. Его отличительная особенность заключается в том, что можно обрабатывать зашифрованные данные без их предварительной расшифровки таким образом, что результат операций над зашифрованными данными эквивалентен после расшифровки результату операции над открытыми данными. Гомоморфное шифрование может эффективно применяться для реализации защищенных облачных вычислений. Для решения различных прикладных задач требуется поддержка всех математических операций, в том числе и операции деления, однако эта тема недостаточно проработана. Возможность выполнить операцию деления гомоморфно позволит расширить возможности прикладного применения гомоморфного шифрования и позволит выполнить гомоморфную реализацию многих алгоритмов. В работе рассматриваются существующие гомоморфные алгоритмы и возможность реализации операции деления в рамках этих алгоритмов. Также в работе предлагаются два метода гомоморфного деления. Первый метод основан на представлении шифротекстов в виде простых дробей и*

* Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-37-90140.