МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

DOI: 10.18698/0236-3933-2016-1-89-97

УДК 511.333:511.337

МОДЕЛЬ ФОРМИРОВАНИЯ ПРОСТЫХ ЧИСЕЛ НА ОСНОВЕ СИММЕТРИЧНОГО ПРЕДСТАВЛЕНИЯ КОЛЬЦЕВОЙ ФАКТОРИЗАЦИИ ПРИ ОТБОРЕ СОСТАВНЫХ ЧИСЕЛ

В.А. Минаев[1], **Е.В. Вайц**[1], **Д.В. Никеров**[2], **С.А. Никонов**[2]

[1]МГТУ им. Н.Э. Баумана, Москва, Российская Федерация
e-mail: m1va@yandex.ru; vaitcev@yandex.ru

[2]Российский новый университет, Москва, Российская Федерация
e-mail: dnik@bk.ru; nikonov.simon@yandex.ru

Развитие методов поиска простых чисел, основанных на эффективных алгоритмах просеивания, имеет огромное фундаментальное и прикладное значение для решения проблем обеспечения информационной безопасности. Рассмотрена модель формирования простых чисел, основанная на применении метода симметричной кольцевой факторизации к отбору составных чисел и обобщении теоремы о полном множестве простых чисел.

***Ключевые слова*:** информационная безопасность, простые числа, кольцевая факторизация.

THE PRIME FORMATION MODEL BASED ON THE SYMMETRIC REPRESENTATION OF RING FACTORIZATION IN SELECTING COMPOSITE NUMBERS

V.A. Minaev[1], **E.V. Vayts**[1], **D.V. Nikerov**[2], **S.A. Nikonov**[2]

[1]Bauman Moscow State Technical University, Moscow, Russian Federation
e-mail: m1va@yandex.ru; vaitcev@yandex.ru

[2]Russian New University, Moscow, Russian Federation
e-mail: dnik@bk.ru; nikonov.simon@yandex.ru

The development of prime search methods based on effective sieving algorithms has a tremendous fundamental and applied significance in information security. The article discusses the model of Prime formations based on the method of symmetric ring factorization applied to selection of composite numbers and generalization of the theorem on the complete set of Primes.

***Keywords*:** information security, primes, ring factorization.

Введение. При решении задачи нахождения полного множества простых чисел на определенном отрезке натурального ряда во многих современных алгоритмах используется предварительный отбор составных чисел [1–3]. При этом для предварительного отбора составных чисел, как правило, применяется метод кольцевой фактори-

зации [4]. Суть метода заключается в следующем: перемножаются несколько первых простых чисел, идущих подряд (математическая операция, известная как примориал), например, $3\# = 2 \times 3 = 6$, $5\# = 2 \times$ $\times 3 \times 5 = 30$, $7\# = 2 \times 3 \times 5 \times 7 = 210$ и т.д. Затем строится таблица с числом столбцов, равным полученному примориалу, ячейки которой нумеруются по порядку (рисунок) [5]. При этом для обобщения добавлена кольцевая факторизация для $2\# = 2$. В построенных таблицах выделим столбцы, которые начинаются с единицы, с простых чисел, не участвовавших в получении примориала, а также со всевозможных произведений этих простых чисел, меньших примориала.

Согласно методу кольцевой факторизации, в неотмеченных столбцах находятся только составные числа, за исключением всех участвовавших в получении примориала простых чисел (расположены в первых строках таблиц).

Далее исключим из рассмотрения неотмеченные столбцы, при этом учитывая все участвовавшие в получении примориала простые числа. Очевидно, что в отмеченных столбцах находятся простые числа, а также единица и оставшиеся после предварительного отбора составные числа. Определим понятие “порядок кольцевой факторизации”.

Определение 1. *Порядок кольцевой факторизации — число сомножителей примориала, используемого при построении соответствующей таблицы предварительного отбора составных чисел.*

Метод кольцевой факторизации позволяет отсеять значительную часть составных чисел: для $3\#$ отсеивается 66,66 % всех составных чисел; для $7\#$ — более 77 %; для $251\#$ — около 90 %.

На следующем этапе для исключения оставшихся составных чисел применяют различные алгоритмы, например, решето Эратосфена, решето Аткина и др., а также современные алгоритмы, основанные на индексном представлении составных чисел в натуральном ряде [1, 4–6]. Сравнение быстродействия индексного алгоритма с решетом Аткина, из результатов которого следует, что индексный алгоритм на исследованном отрезке натурального ряда работает в 12 раз быстрее проведено в работе [7].

1	2
3	4
5	6
...	...

а

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
...	...	...	...	...	...

б

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...

в

Табличное отображение кольцевой факторизации для 2# (*а*), 3# (*б*) и 5# (*в*)

Примем следующие обозначения: $\mathbb{N}_0$ — множество всех натуральных чисел и $\{0\}$; $\mathbb{N}$ — множество всех натуральных чисел; $\{q\}$ — множество всех простых и составных чисел; $\{c\}$ — множество всех составных чисел; $\{p\}$ — множество всех простых чисел.

Для нумерации простых чисел подряд по возрастанию используем левый верхний индекс: ${}^1p = 2$; ${}^2p = 3$; ${}^3p = 5$; ${}^4p = 7$ и т.д. Отметим, что 1 является единственным натуральным числом, не являющимся ни простым, ни составным, т.е. $\{q\} = \mathbb{N}\backslash\{1\}$.

Представление составных чисел через простой сомножитель. Согласно *основной теореме арифметики*, каждое натуральное число $n > 1$ единственным образом представимо в виде

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}, \tag{1}$$

где $k \in \mathbb{N}$; $p_1 < p_2 < \ldots < p_k$ — упорядоченные по возрастанию простые числа; $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}$. Представление числа n в виде (1) называется его *каноническим разложением*.

Используя каноническое разложение для составных чисел, нетрудно показать, что верно утверждение *о единственном представлении составного числа через его наименьший простой делитель*.

Утверждение 1. *Каждое составное число единственным образом представимо в виде*

$$c = p_1 q, \tag{2}$$

где p_1 — наименьший простой делитель c; величина q удовлетворяет условию $p_1 \le q$.

Сформулируем утверждение о представлении составных чисел через их простые делители.

Утверждение 2. *Каждое составное число представимо в виде*

$$c = pq, \tag{3}$$

где p — простой делитель c : $p \le \sqrt{c}$; величина q удовлетворяет условию $p \le q$.

Существование представления (3) следует напрямую из представления (2). При этом условие $p \le \sqrt{c}$ для $c = pq$ следует из условия $p \le q$.

Отметим, что представление составных чисел через их простые делители (3) не всегда является единственным для конкретного составного числа, однако применимо для каждого его простого делителя, не превышающего $\sqrt{c}$.

Обобщение теоремы о полном множестве простых чисел. Определим индексы $i, j, k \in \mathbb{N}$. Введем следующие обозначения: $\{q_{2k}^{+1}\} = \{2k+1\}$ — множество всех нечетных чисел (за исключением 1); $\{c_{2j}^{+1}\} = \{2j+1\}$ — множество всех нечетных составных чисел;

$\{p_{2i}^{+1}\} = \{2i+1\}$ — множество всех простых чисел (за исключением 2). При этом k принимает все значения натурального ряда, а индексы i и j принимают все значения натурального ряда таким образом, что индекс i принимает те значения, которые не принимает индекс j, а индекс j принимает те значения, которые не принимает индекс i.

Теорема о полном множестве простых чисел вида $\{6i \pm 1\}$, основанная на кольцевой факторизации второго порядка для предварительного отбора составных чисел, сформулирована и доказана в работе [1]. Сформулируем и докажем обобщенную теорему о полном множестве простых чисел, основанную на кольцевой факторизации первого порядка.

Теорема 1. *Полное множество простых чисел является объединением* $\{2\}$ *и множества* $\{p_{2i}^{+1}\}$, *которое формируется путем вычитания из множества* $\{q_{2k}^{+1}\}$ *подмножества* $\{c_{2j}^{+1}\}$ *чисел, определяемых по уравнению*

$$c_{p_{2i}^{+1}}^{+1} = p_{2i}^{+1} p_{2i}^{+1} + p_{2i}^{+1} 2m, \tag{4}$$

где $m \in \mathbb{N}_0$; $i \in \mathbb{N}$.

◀ Поскольку нечетные составные числа не делятся на 2, в соответствии с соотношением (3), представляющем составные числа через их простые делители, каждое нечетное составное число c_{2j}^{+1} может быть представлено в виде

$$c_{p_{2i}^{+1}}^{+1} = p_{2i}^{+1} q_{2k}^{+1} = (2i+1)(2k+1), \tag{5}$$

где p_{2i}^{+1} — простой делитель $c_{p_{2i}^{+1}}^{+1}$; $p_{2i}^{+1} \le q_{2k}^{+1}$.

Следовательно, $i \le k$. Введем индекс $m \in \mathbb{N}_0$: $m = k - i$. Тогда соотношение (5) может иметь вид

$$c_{p_{2i}^{+1}}^{+1} = (2i+1)(2(i+m)+1) = (2i+1)^2 + (2i+1)2m. \tag{6}$$

Соотношение (6) идентично соотношению (4). Таким образом, каждое нечетное составное число c_{2j}^{+1} может быть представлено в виде соответствующего члена как минимум одной аддитивной последовательности (4). Следовательно, полное множество простых чисел является объединением $\{2\}$ и множества $\{p_{2i}^{+1}\}$, которое формируется путем вычитания из множества $\{q_{2k}^{+1}\}$ подмножества $\{c_{2j}^{+1}\}$ чисел, определяемых по уравнению (4). ▶

Переход к симметричному виду кольцевой факторизации. Пусть ${}^n p$ — n-е простое число. При исключении из отрезка натурального ряда $[1;\ {}^n p\#]$ чисел, равных и кратных числам ${}^1 p, {}^2 p, \ldots, {}^n p$, в нем останутся числа из первой строки таблицы кольцевой факторизации n-го порядка. При этом первая строка таблицы кольцевой факторизации первого порядка имеет $2-1=1$ число, первая строка таблицы кольцевой факторизации второго порядка — $(2-1)\times(3-1)=2$ числа,

первая строка таблицы кольцевой факторизации третьего порядка — $(2-1)\times(3-1)\times(5-1)=8$ чисел и т.д. Определим функцию запаздывающего приморіала (retarded primorial).

Определение 2. *Функция запаздывающего приморіала аргумента* $n\in\mathbb{N}$:

$$ {}^{n}p\#_{-1}=\prod_{i=1}^{n}\left\{{}^{i}p-1\right\}. \tag{7}$$

Отметим, что исследование асимптотики функции запаздывающего приморіала представляет собой отдельную задачу.

При исключении из отрезка натурального ряда $[1;\ {}^{n}p\#]$ чисел, равных и кратных ${}^{1}p,{}^{2}p,\ldots,{}^{n}p$, в нем, согласно (7) останется ${}^{n}p\#_{-1}$ чисел из первой строки таблицы кольцевой факторизации *n*-го порядка.

Определим параметр s как следующую функцию от аргумента $n\in\mathbb{N}$:

$$\begin{aligned} &n=1:\ \ s=0;\\ &n\geq 2:\ \ s={}^{n}p\#_{-1}/2-1. \end{aligned} \tag{8}$$

Сформулируем и докажем теорему о симметричном представлении кольцевой факторизации второго и более старших порядков.

Теорема 2. *Таблица кольцевой факторизации* n*-го порядка* $(n\geq 2)$ *имеет* ${}^{n}p\#_{-1}$ *столбцов*, *числа в которых представимы в виде* $\{{}^{n}p\#k\pm_0^n q\}$, $\{{}^{n}p\#k\pm_1^n q\}$, $\ldots$, $\{{}^{n}p\#k\pm_r^n q\}$, $\ldots$, $\{{}^{n}p\#k\pm_s^n q\}$, *где* k *— номер строки таблицы кольцевой факторизации*, $k\in\mathbb{N}$; ${}_0^n q=1$; ${}_1^n q$, $\ldots$, ${}_r^n q$, $\ldots$, ${}_s^n q$ *— не участвовавшие в получении* ${}^{n}p\#$ *простые числа и их произведения*, *меньшие* ${}^{n}p\#/2$ *и записанные по возрастанию*; $s\ (8)$ *— количество простых чисел и их произведений на интервале* $({}^{n}p;\ {}^{n}p\#/2)$; $r\in\{0;1;\ldots;s\}$.

◀ Таблица кольцевой факторизации *n*-го порядка имеет ${}^{n}p\#_{-1}$ (7) столбцов, так как первая строка этой таблицы имеет столько же чисел. Число ${}^{n}p\#$ по определению кратно числам ${}^{1}p$, ${}^{2}p$, $\ldots$, ${}^{n}p$, отсюда на отрезке натурального ряда $[1;\ {}^{n}p\#]$ следует симметричность расположения чисел, равных и кратных числам ${}^{1}p$, ${}^{2}p$, $\ldots$, ${}^{n}p$, относительно ${}^{n}p\#/2$ $(\forall n\in\mathbb{N}\ \ {}^{n}p\#\vdots\,2)$. Таким образом, числа первой строки таблицы кольцевой факторизации *n*-го порядка также имеют симметричное расположение относительно ${}^{n}p\#/2$.

Поскольку при $n\geq 2$ количество чисел первой строки таблицы кольцевой факторизации *n*-го порядка будет четным, эти числа представимы в виде $\{{}^{n}p\#\pm_0^n q\}$, $\{{}^{n}p\#\pm_1^n q\}$, $\ldots$, $\{{}^{n}p\#\pm_r^n q\}$, $\ldots$, $\{{}^{n}p\#\pm_s^n q\}$, где ${}_0^n q=1$; ${}_1^n q$, $\ldots$, ${}_r^n q$, $\ldots$, ${}_s^n q$ — не участвовавшие в получении ${}^{n}p\#$ простые числа и их произведения, меньшие ${}^{n}p\#/2$ и записанные по возрастанию; $s(8)$ — количество простых чисел и их произведений на интервале $({}^{n}p;\ {}^{n}p\#/2)$; $r\in\{0;1;\ldots;s\}$.

Каждая следующая строка таблицы увеличивает значения чисел в столбцах на ${}^{n}p\#$, следовательно, числа в k-й строке таблицы кольцевой факторизации n-го порядка представимы в виде $\{{}^{n}p\#k \pm_0^n q\}$, $\{{}^{n}p\#k \pm_1^n q\}$, …, $\{{}^{n}p\#k \pm_r^n q\}$, …, $\{{}^{n}p\#k \pm_s^n q\}$. ►

Определим индексы $i, j, k \in \mathbb{N}$. Введем следующие обозначения: $\{q_{{}^{n}p\#k}\}$ — множество всех простых и составных чисел, не равных и не кратных числам ${}^{1}p$, ${}^{2}p$, …, ${}^{n}p$; $\{c_{{}^{n}p\#j}\}$ — множество всех составных чисел, не кратных числам ${}^{1}p$, ${}^{2}p$, …, ${}^{n}p$; $\{p_{{}^{n}p\#i}\}$ — множество всех простых чисел, кроме чисел ${}^{1}p$, ${}^{2}p$, …, ${}^{n}p$.

В соответствии с теоремой о симметричном представлении кольцевой факторизации второго и более старших порядков, множество $\{q_{{}^{n}p\#k}\}$ можно разбить на ${}^{n}p\#_{-1}$ подмножеств. Представим данные подмножества в виде матрицы $2 \times (s+1)(8)$:

$$\begin{matrix} \left\{q_{{}^{n}p\#k}^{-{}_0^n q}\right\} \left\{q_{{}^{n}p\#k}^{-{}_1^n q}\right\} \dots \left\{q_{{}^{n}p\#k}^{-{}_r^n q}\right\} \dots \left\{q_{{}^{n}p\#k}^{-{}_s^n q}\right\} \\ \left\{q_{{}^{n}p\#k}^{+{}_0^n q}\right\} \left\{q_{{}^{n}p\#k}^{+{}_1^n q}\right\} \dots \left\{q_{{}^{n}p\#k}^{+{}_r^n q}\right\} \dots \left\{q_{{}^{n}p\#k}^{+{}_s^n q}\right\} \end{matrix}. \tag{9}$$

Здесь $r \in \{0; 1; \dots; s\}$; $\forall n \geq 2$, k принимает все значения натурального ряда для каждого элемента матрицы подмножеств (9) $\{q_{{}^{n}p\#k}\}$, элементы которой представимы как

$$\begin{aligned} q_{{}^{n}p\#k}^{\pm{}_r^n q} &= {}^{n}p\#k \pm {}_r^n q; \\ c_{{}^{n}p\#j}^{\pm{}_a^n q} &= {}^{n}p\#j \pm {}_a^n q; \\ p_{{}^{n}p\#i}^{\pm{}_b^n q} &= {}^{n}p\#i \pm {}_b^n q, \end{aligned} \tag{10}$$

при этом $a, b \in \{0; 1; \dots; s\}$; знаки в левой и правой частях в каждом соотношении (10) расставлены соответственно; $\forall n \geq 2$ при $a = b$ для одинаковых знаков второго и третьего соотношений (10); индексы i и j совместно принимают все значения натурального ряда так, что индекс i принимает те значения, которые не принимает индекс j, а индекс j — те значения, которые не принимает индекс i. Таким образом, множество $\{c_{{}^{n}p\#j}\}$ также можно разбить на ${}^{n}p\#_{-1}$ подмножеств в виде матрицы $2 \times (s+1)$

$$\begin{matrix} \left\{c_{{}^{n}p\#j}^{-{}_0^n q}\right\} \left\{c_{{}^{n}p\#j}^{-{}_1^n q}\right\} \dots \left\{c_{{}^{n}p\#j}^{-{}_a^n q}\right\} \dots \left\{c_{{}^{n}p\#j}^{-{}_s^n q}\right\} \\ \left\{c_{{}^{n}p\#j}^{+{}_0^n q}\right\} \left\{c_{{}^{n}p\#j}^{+{}_1^n q}\right\} \dots \left\{c_{{}^{n}p\#j}^{+{}_a^n q}\right\} \dots \left\{c_{{}^{n}p\#j}^{+{}_s^n q}\right\} \end{matrix},$$

а множество $\{p_{{}^{n}p\#\cdot i}\}$ — на ${}^{n}p\#_{-1}$ подмножеств в виде матрицы $2 \times$ $\times (s+1)$

$$\begin{matrix} \left\{p_{{}^{n}p\#i}^{-{}_0^n q}\right\} \left\{p_{{}^{n}p\#i}^{-{}_1^n q}\right\} \dots \left\{p_{{}^{n}p\#i}^{-{}_b^n q}\right\} \dots \left\{p_{{}^{n}p\#i}^{-{}_s^n q}\right\} \\ \left\{p_{{}^{n}p\#i}^{+{}_0^n q}\right\} \left\{p_{{}^{n}p\#i}^{+{}_1^n q}\right\} \dots \left\{p_{{}^{n}p\#i}^{+{}_b^n q}\right\} \dots \left\{p_{{}^{n}p\#i}^{+{}_s^n q}\right\} \end{matrix}.$$

Поскольку принадлежащие множеству $\{c_{^np\#j}\}$ составные числа не делятся на ${}^1p$, ${}^2p$, …, ${}^np$, в соответствии с соотношением (3) каждое принадлежащее множеству $\{c_{^np\#j}\}$ составное число $c_{^np\#j}^{\pm_a^n q}$ может быть представлено в виде:

$$\forall n \in \mathbb{N},\ \forall a \in \{0; 1; \ldots; s\};$$

$$\exists\, i, k \in \mathbb{N},\ b, r \in \{0; 1; \ldots; s\};$$

$$c_{^np\#j}^{\pm_a^n q} = p_{^np\#i}^{\pm_b^n q} q_{^np\#k}^{\pm_r^n q},$$

где $p_{^np\#i}^{\pm_b^n q}$ — простой делитель $c_{^np\#j}^{\pm_a^n q}$, при этом $p_{^np\#i}^{\pm_b^n q} \le q_{^np\#k}^{\pm_r^n q}$.

Заключение. Обосновано симметричное представление кольцевой факторизации при отборе составных чисел и приведено доказательство соответствующей теоремы. Полученные оценки показывают, что использование симметричного алгоритма поиска простых чисел по сравнению с несимметричным алгоритмом позволяет ускорить время расчета. Например, для факторизации числа RSA-768, длившейся около 20 месяцев, симметричный алгоритм потребовал около 20 дней работы используемого не самого мощного вычислительного кластера. Кроме того, предварительные исследования показывают, что использование симметричного алгоритма по сравнению с несимметричным алгоритмом позволяет на разных интервалах натурального ряда в диапазоне до 10^{12} ускорить время расчета на 3…7 %.

Усовершенствована модель поиска простых чисел, основанная на применении метода кольцевой факторизации и обобщении теоремы о полном множестве простых чисел при отборе составных чисел. Получены важные фундаментальные и прикладные результаты, использование которых позволяет более эффективно решать задачи обеспечения информационной безопасности [2, 3, 8, 9].

ЛИТЕРАТУРА

1. *Минаев В.А.* Простые числа: новый взгляд на закономерности формирования. М.: Логос, 2011. 80 с.
2. *Курушин В.Д.*, *Минаев В.А.* Компьютерные преступления и информационная безопасность. Справочник. М.: Новый юрист, 1998. 256 с.
3. *Карпычев В.Ю.*, *Минаев В.А.* Цена информационной безопасности // Системы безопасности. 2003. № 5. С. 128–130.
4. *Высокопроизводительный* алгоритм генерации простых чисел в произвольном диапазоне / В.А. Минаев, Н.П. Васильев, В.В. Лукьянов, С.А. Никонов, Д.В. Никеров // Материалы XIV международной научной конференции “Цивилизация знаний: проблемы и смыслы образования”. 2013. М.: Изд-во РосНОУ. С. 494–498.
5. *Минаев В.А.*, *Никонов С.А.*, *Никеров Д.В.* Симметричные формы индексных алгоритмов вычисления простых чисел // Спецтехника и связь. 2014. № 5. С. 40–48.
6. *Минаев В.А.*, *Никеров Д.В.*, *Никонов С.А.* Аддитивный индексный алгоритм вычисления простых чисел // Спецтехника и связь. 2015. № 1. С. 46–50.

7. *Минаев В.А.*, *Никонов С.А.*, *Никеров Д.В.* Сравнение быстродействия модифицированного индексного алгоритма с решетом Аткина при поиске простых чисел // Спецтехника и связь. 2015. № 2. С. 38–41.
8. *Минаев В.А.*, *Саблин В.Н.*, *Фисун А.П.* Теоретические основы информатики и информационная безопасность. М.: Радио и связь. 2000. 468 с.
9. *Минаев В.А.*, *Скрыль С.В.* Основы информационной безопасности. Воронеж: Изд-во Воронежского института МВД России, 2001. 464 с.

REFERENCES

[1] Minaev V.A. Prostye chisla: novyy vzglyad na zakonomernosti formirovaniya [Prime Numbers: New Insight into the Patterns of Forming]. Moscow, Logos Publ., 2011. 80 p.

[2] Kurushin V.D., Minaev V.A. Komp'yuternye prestupleniya i informatsionnaya bezopasnost'. Spravochnik [Computer Crimes and Information Security. Handbook]. Moscow, Novyy yurist Publ., 1998. 256 p.

[3] Karpychev V.Yu., Minaev V.A. Tsena informatsionnoy bezopasnosti [The Cost of Information Security]. *Sistemy bezopasnosti* [Security Systems], 2003, no. 5, pp. 128–130 (in Russ.).

[4] Minaev V.A., Vasil'ev N.P., Luk'yanov V.V., Nikonov S.A., Nikerov D.V. High-Performance Algorithm for Generating Prime Numbers in an Arbitrary Range. *Mat. XIV mezhdunar. nauch. konf. "Tsivilizatsiya znaniy: problemy i smysly obrazovaniya"* [Proc. of XIV International Scientific Conference "Civilization of Knowledge: Problems and Significance of Education"], Moscow, RosNOU Publ., 2013, pp. 494–498 (in Russ.).

[5] Minaev V.A., Nikonov S.A., Nikerov D.V. The Symmetric Forms of the Index Algorithms for Computing Prime Numbers. *Spetstekhnika i svyaz'* [Specialized Machinery and Communication], 2014, no. 5, pp. 40–48 (in Russ.).

[6] Minaev V.A., Nikerov D.V., Nikonov S.A. Additive Index Algorithm for Computing Prime Numbers. *Spetstekhnika i svyaz'* [Specialized Machinery and Communication], 2015, no. 1, pp. 46–50 (in Russ.).

[7] Minaev V.A., Nikonov S.A., Nikerov D.V. Comparison of Processing Speed of the Modified Index Algorithm and Atkin Sieve When Searching for Primes. *Spetstekhnika i svyaz'* [Specialized Machinery and Communication], 2015, no. 2, pp. 38–41 (in Russ.).

[8] Minaev V.A., Sablin V.N., Fisun A.P. Teoreticheskie osnovy informatiki i informatsionnaya bezopasnost' [Fundamental Theory of Informatics and Information Security]. Moscow, Radio i svyaz' Publ., 2000. 468 p.

[9] Minaev V.A., Skryl' S.V. Osnovy informatsionnoy bezopasnosti [Fundamentals of Information Security]. Voronezh, Voronezhskiy institut MVD Rossii Publ., 2001. 464 p.

Статья поступила в редакцию 15.06.2015

Минаев Владимир Александрович — д-р техн. наук, профессор кафедры "Защита информации" МГТУ им. Н.Э. Баумана.
МГТУ им. Н.Э. Баумана, Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5.

Minaev V.A. — Dr. Sci. (Eng.), Professor of Information Security department, Bauman Moscow State Technical University.
Bauman Moscow State Technical University, 2-ya Baumanskaya ul. 5, Moscow, 105005 Russian Federation.

Вайц Екатерина Викторовна — старший преподаватель кафедры “Защита информации” МГТУ им. Н.Э. Баумана.
МГТУ им. Н.Э. Баумана, Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5.

Vayts E.V. — Senior Lecturer of Information Security department, Bauman Moscow State Technical University.
Bauman Moscow State Technical University, 2-ya Baumanskaya ul. 5, Moscow, 105005 Russian Federation.

Никеров Дмитрий Викторович — аспирант Российского нового университета.
Российский новый университет, Российская Федерация, 105005, Москва, ул. Радио, д. 22.

Nikerov D.V. — post-graduate student of Russian New University.
Russian New University, ul. Radio 22, Moscow, 105005 Russian Federation.

Никонов Семен Андреевич — аспирант Российского нового университета.
Российский новый университет, Российская Федерация, 105005, Москва, ул. Радио, д. 22.

Nikonov S.A. — post-graduate student of Russian New University.
Russian New University, ul. Radio 22, Moscow, 105005 Russian Federation.

Просьба ссылаться на эту статью следующим образом:

Минаев В.А., Вайц Е.В., Никеров Д.В., Никонов С.А. Модель формирования простых чисел на основе симметричного представления кольцевой факторизации при отборе составных чисел // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2016. № 1. С. 89–97. DOI: 10.18698/0236-3933-2016-1-89-97

Please cite this article in English as:

Minaev V.A., Vayts E.V., Nikerov D.V., Nikonov S.A. The prime formation model based on the symmetric representation of ring factorization in selecting composite numbers. *Vestn. Mosk. Gos. Tekh. Univ. im. N.E. Baumana, Priborostr.* [Herald of the Bauman Moscow State Tech. Univ., Instrum. Eng.], 2016, no. 1, pp. 89–97.
DOI: 10.18698/0236-3933-2016-1-89-97