Александр П. Мартынов¹, Дмитрий Б. Николаев², Кирилл Д. Ермаков³
СарФТИ Национального исследовательского ядерного университета «МИФИ»,
ул. Духова, 6, Саров, Нижегородская обл., 607184, Россия
¹e-mail: dim010307@yandex.ru, <http://orcid.org/0000-0002-8985-615X>
²e-mail: dim010307@yandex.ru, <http://orcid.org/0000-0003-4618-1022>
³e-mail: ermakov-kir@mail.ru, <http://orcid.org/0000-0002-3723-7111>

РЕАЛИЗАЦИЯ НЕЛИНЕЙНОГО ПРЕОБРАЗОВАНИЯ ПОДСТАНОВКИ
В ВИДЕ ЭЛЕМЕНТОВ СИСТЕМЫ СЧИСЛЕНИЯ
РЯДА ФАКТОРИАЛЬНЫХ МНОЖЕСТВ

DOI: <http://dx.doi.org/10.26583/bit.2021.3.07>

Аннотация. В работе исследуется нелинейное преобразование подстановки, представленное как элемент системы счисления факториальных множеств. Данное представление учитывает характерные особенности подстановок и позволяет минимизировать объем памяти для их хранения. На основе подхода однозначной нумерации подстановок рассмотрено три способа их хранения в памяти: в виде вектора, в виде значений циклических сдвигов элементов тождественной подстановки и в виде десятичного номера подстановки. Приведены результаты анализа объема данных, необходимого для хранения нелинейного преобразования подстановки для криптографических примитивов и определена трудоемкость перевода преобразованных подстановок в стандартный вид хранения вектором. Полученные результаты могут быть применены в программных решениях для обеспечения информационной безопасности с использованием криптографических примитивов, содержащих нелинейное преобразование подстановки. Предложенный подход к записи в виде преобразования подстановок рекомендуется для реализации в комплексах с ограниченным объемом памяти.

Ключевые слова: криптографические примитивы, нелинейное преобразование подстановки, система счисления ряда факториальных множеств.

Для цитирования: МАРТЫНОВ, Александр П.; НИКОЛАЕВ, Дмитрий Б.; ЕРМАКОВ, Кирилл Д. РЕАЛИЗАЦИЯ НЕЛИНЕЙНОГО ПРЕОБРАЗОВАНИЯ ПОДСТАНОВКИ В ВИДЕ ЭЛЕМЕНТОВ СИСТЕМЫ СЧИСЛЕНИЯ РЯДА ФАКТОРИАЛЬНЫХ МНОЖЕСТВ. Безопасность информационных технологий, [S.l.], т. 28, № 3, с. 81–91, 2021. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1365>. DOI: <http://dx.doi.org/10.26583/bit.2021.3.07>.

Alexander P. Martynov¹, Dmitry B. Nikolaev², Kirill D. Ermakov³
SarFTI of National Research Nuclear University MEPHI (Moscow Engineering Physics Institute),
Dukhova Str., 6, Sarov, Nizhny Novgorod Region, 607184, Russia

¹e-mail: dim010307@yandex.ru, <http://orcid.org/0000-0002-8985-615X>

²e-mail: dim010307@yandex.ru, <http://orcid.org/0000-0003-4618-1022>

³e-mail: ermakov-kir@mail.ru, <http://orcid.org/0000-0002-3723-7111>

**Implementation of a nonlinear transformation of a substitution in the form of elements
of a numbering system of a number of factorial sets**

DOI: <http://dx.doi.org/10.26583/bit.2021.3.07>

Abstract. The paper investigates a nonlinear substitution transformation, presented as an element of the number system of factorial sets. This approach takes into account the characteristic features of substitutions and allows you to minimize the amount of memory for storing. Based on the unambiguous numbering approach for substitutions, three methods of storing in memory are considered: in the form of a vector, in the form of values of cyclic shifts of elements of an identical substitution, and in the form of a decimal substitution number. The results of the analysis of the amount of data required for storing the nonlinear substitution transformation for cryptographic primitives are presented. The complexity of translating the transformed substitutions into the standard form of storage by a vector is determined. The obtained results can be applied in software solutions for ensuring information security using cryptographic primitives

containing a nonlinear substitution transformation. The proposed approach to writing in the form of substitution transformations is recommended for implementation in complexes with a limited amount of memory.

Keywords: cryptographic primitives, nonlinear substitution transformation, number system of a number of factorial sets.

For citation: MARTYNOV, Alexander P.; NIKOLAEV, Dmitry B.; ERMAKOV, Kirill D. Implementation of a nonlinear transformation of a substitution in the form of elements of a numbering system of a number of factorial sets. IT Security (Russia), [S.l.], v. 28, n. 3, p. 81–91, 2021. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1365>. DOI: <http://dx.doi.org/10.26583/bit.2021.3.07>.

Введение

В настоящее время актуальной и важной проблемой является обеспечение информационной безопасности данных. Одним из решений данной проблемы является использование криптографических протоколов и примитивов. В качестве одного из таких примитивов можно выделить блочные алгоритмы шифрования с секретным ключом, которые широко применяются для обеспечения конфиденциальности данных.

Алгоритмы блочного шифрования могут строиться при помощи различных структур, таких как SP-сети, сети Фейстеля, схемы Лая-Мэсси и др., однако все данные подходы состоят из различных преобразований, часто схожих друг с другом [1–3]. Все данные преобразования можно рассматривать как линейные и нелинейные преобразования. Стоит отметить, что при криптоанализе алгоритмов шифрования, стойкость алгоритму обеспечивает в основном использование нелинейных преобразований (если бы алгоритм шифрования состоял только из линейных преобразований, он бы тривиально взламывался противником) [4–6].

Одним из самых популярных видов нелинейных преобразований, используемых в алгоритмах, являются блоки подстановок (S-блоки). Блок подстановки является преобразованием, которое принимает на вход двоичный набор некоторой длины и преобразует его в другой двоичный набор. При исследовании данного преобразования анализируются не только его свойства [7–9], но и применимость в алгоритмах [10, 11]. При программной реализации такого преобразования в памяти обычно хранят вектор, где под индексом входного набора в векторе хранится значение выходного набора. При этом функциональная гибкость устройства преобразования будет зависеть от возможности вариативного изменения значений выходного набора [12, 13]. Следует отметить, что количество перестановок определяется факториалом, и при возрастании размерности выходного вектора количество возможных комбинаций существенно увеличивается [14] и это при условии статичности применяемых S-блоков. В случае применения управляемых блоков [15] объем хранимой информации является ключевым параметром при аппаратной или программной реализации алгоритма, а процесс оценки и, при необходимости, оптимизации данной информации при хранении носит, несомненно, актуальный характер. Ключевым аспектом работы является переход от традиционных подходов представления данных к представлению через формы [16, 17], учитывающие особенности множеств, формируемых из используемых выходных наборов – представление в факториальной системе счисления.

В [18] дано понятие факториального множества, введена система счисления факториальных множеств, а также предложен способ перевода чисел из десятичной системы счисления в систему счисления факториальных множеств и обратно. Кроме того приведен способ однозначной нумерации подстановок, который позволяет представить подстановки при помощи десятичного числа или элемента системы счисления факториальных множеств.

Однако при описании данных подходов не была проведена оценка объемов памяти для хранения параметров нелинейных преобразований в существующих криптографических алгоритмах.

1. Факториальное множество

Для понятия системы счисления ряда факториальных множеств рассмотрим основополагающие понятия.

Факториал $n!$ – это произведение натуральных чисел от 1 до числа n . Множество натуральных чисел $\{1, 2, 3, \dots, n\}$ называется множеством образующих элементов функции факториала.

Факториальное множество Φ_n – множество перестановок из n чисел, мощность которого $P(\Phi_n)$ равняется значению факториала образующих элементов множества ($n!$). Ряд факториальных множеств представлен на рис. 1.

Рис. 1. Представление ряда факториальных множеств
 Fig. 1. Representation of a number of factorial sets

Элементом факториального множества Φ_n является перестановка его образующих элементов $\{1, 2, 3, \dots, n\}$. Так как элементы множества Φ_n мощностью $P(\Phi_n) = n!$ можно переставить $n!$ способами, любое преобразование подстановки можно удобно представить как элемент множества Φ_n .

Авторы в [19] представили упорядоченную систему счисления, установив однозначное соответствие между конкретной перестановкой n элементов и ее эквивалентом в системе счисления факториальных множеств.

Как показано на рис. 1, каждое факториальное множество Φ_n содержит в себе n подмножеств Φ_{n-1} меньшей на единицу мощности. На данном факте строится идея формирования позиционной системы счисления ряда факториальных множеств. Этапы формирования позиционной системы счисления [18, 19] описываются следующим образом:

1. Факториальные множества Φ_n раскладываются на подмножества, количество которых равно числу образующих элементов или же номеру факториального множества.
2. Данные подмножества также циклически раскладываются на меньшие по мощности множества, вплоть до множества подстановок, состоящего из одного элемента (Φ_1).
3. Полученные составляющие элементы ряда факториальных множеств записываются в общем виде в соответствии с их позициями.

4. Позиционным коэффициентам $a_1, \dots, a_n$ системы счисления факториальных множеств обозначают соответствующие им множества.

Нулем в данной системе счисления обозначается тот факт, что перестановки образующих элементов множества нет. Этапы формирования системы счисления ряда факториальных множеств на примере первых пяти множеств представлены на рис. 2.

Рис. 2. Формирование системы счисления ряда факториальных множеств
Fig. 2. Formation of the number system of a number of factorial sets

Полученную систему счисления можно представить выражением:

$$X = a_{(n-1)}(n-1)! + \dots + a_3 2! + a_2 1!,$$

где a_i – позиционные коэффициенты. Значение данных коэффициентов зависит от конкретно взятого факториального множества. В данной системе счисления вместо традиционного основания системы счисления q в степени $\{1, \dots, n-1\}$ используются мощности $P(\Phi_i)$ последовательно следующих факториальных множеств.

2. Преобразование чисел из десятичной системы счисления в систему счисления ряда факториальных множеств и наоборот

В [19] представлен алгоритм перевода чисел из различных систем счисления по отношению к системе счисления ряда факториальных множеств. Стоит отметить, что данный способ перевода чисел является оригинальным и разработан авторами статьи. Далее будет представлен метод перевода чисел в данных системах счисления.

Как известно, любой элемент, входящий в факториальное множество, можно представить в виде количества целых частей предыдущего множества и некоего остатка от деления:

$$\frac{X}{(n-1)!} = c + b,$$

где X – делимое, c – целая часть от деления, b – остаток.

Для перевода элементов множеств из системы с основанием 10 в систему счисления факториальных множеств используется описанный выше метод деления, в котором происходит последовательное деление на значение мощности предыдущих факториальных множеств. Любое десятичное число от 0 до $n! - 1$ можно представить элементом факториального множества Φ_n .

Пример. Допустим необходимо перевести десятичное число 100 в систему счисления факториальных множеств. Данное число является элементом Φ_5 , так как в нем содержится менее $5! = 120$ подстановок. Первым делением является деление на мощность $P(\Phi_{n-1})$ предыдущего факториального множества Φ_4 , равную 24. Далее полученные остатки b от деления делятся на последующие меньшие значения мощностей вплоть до множества Φ_2 :

$$\begin{aligned}100 &= 24 \cdot 4 + 4; \\4 &= 6 \cdot 0 + 4; \\4 &= 2 \cdot 2 + 0.\end{aligned}$$

Таким образом, после перевода десятичное число в системе факториальных множеств будет представлено в виде целых частей от деления и последнего остатка, и иметь следующий вид:

$$100 \rightarrow 4\ 0\ 2\ 0$$

Перевод чисел из системы счисления факториальных множеств в десятичную систему счисления происходит при помощи суммирования произведений позиционных коэффициентов элемента множества на мощности факториальных подмножеств. Ниже приведены примеры перевода в десятичную систему счисления:

$$\begin{aligned}1111 &= 1 \cdot 24 + 1 \cdot 6 + 1 \cdot 2 + 1 \cdot 1 = 33_{10}; \\4321 &= 4 \cdot 24 + 3 \cdot 6 + 2 \cdot 2 + 1 \cdot 1 = 119_{10}; \\2210 &= 2 \cdot 24 + 2 \cdot 6 + 1 \cdot 2 + 0 \cdot 1 = 62_{10}; \\301 &= 3 \cdot 6 + 0 \cdot 2 + 1 \cdot 1 = 19_{10}; \\34321 &= 3 \cdot 120 + 4 \cdot 24 + 3 \cdot 6 + 2 \cdot 2 + 1 \cdot 1 = 479_{10}.\end{aligned}$$

3. Использование подстановок как элементов системы счисления факториальных множеств

Подстановка – однозначное отображение элементов некоторого множества на себя. Так как любая подстановка может быть получена при помощи некоторого числа сдвигов элементов тождественной подстановки, в [19] предложено рассмотреть подстановку как элемент системы счисления факториальных множеств. Однако в данном подходе операция сдвига отдельных элементов заменена операцией сдвига всех элементов конкретного факториального множества.

Каждой подстановке определяется ее образ, который соответствует числу сдвигов для каждого факториального множества. То есть, в данном подходе значение позиционных коэффициентов элемента множества обозначает конкретное значение циклического сдвига вправо элементов подстановки. Последовательность циклических сдвигов для множества Φ_n равна

$$\Phi_n \rightarrow \Phi_{n-1} \rightarrow \dots \rightarrow \Phi_2.$$

Это значит, что сначала циклически сдвигаются на некоторое значение все n элементов подстановки, затем первые $n - 1$ элементов подстановки, вплоть до первых двух элементов подстановки (сдвиг одного элемента смысла не имеет).

Рассмотрим пример. Возьмем элемент факториального множества Φ_5 , данный элемент соответствует подстановке на множестве $\{1, 2, 3, 4, 5\}$. Пусть элемент множества

может быть представлен как $\Phi_5 = 4, \Phi_4 = 0, \Phi_3 = 2, \Phi_2 = 1$. Тогда данные значения сдвигов воздействуют на подстановку следующим образом:

$$12345 \rightarrow 23451 \rightarrow 23451 \rightarrow 34251 \rightarrow 43251.$$

Имея переход элементов счисления факториального множества в конкретные подстановки при помощи операции циклического сдвига частей тождественной подстановки, можно осуществлять перевод чисел из десятичной системы счисления в подстановку и наоборот. Для того, чтобы перевести число от 0 до $n! - 1$ при некотором фиксированном n , операции циклического сдвига будут осуществляться на подстановках с числом элементов, равном n . Графически перевод десятичного числа на примере числа 78 в подстановку и получение значений циклических сдвигов представлено на рис. 3.

Рис. 3. Перевод десятичного числа 78 в подстановку
Fig. 3. Converting Decimal number 78 to Substitution

Как видно из рис. 3, пять элементов подстановки циклически сдвигаются вправо на 3 (частное от деления на 24), затем первые четыре элемента циклически сдвигаются на 1, далее первые три элемента сдвигаются на 0 и два элемента сдвигаются на 0. Циклический сдвиг одного элемента смысла не имеет.

Таким образом, можно сделать вывод, что описанные выше методы и подходы к представлению подстановок могут быть применены как в уже существующих, так и в разрабатываемых криптографических алгоритмах, так как нелинейное преобразование подстановки используется почти во всех криптографических примитивах с секретным ключом. Однако для использования такого вида записи необходимо оценить, эффективна ли запись подстановок в таком виде при программной реализации алгоритмов.

4. Оценка емкости памяти для хранения подстановки стандартным способом

При программной реализации криптографических примитивов нелинейное преобразование биективной подстановки размером $n \times n$ бит обычно реализуется при помощи хранения вектора данных. Данный вектор занимает объем данных, равный

$$n \cdot 2^n \text{ бит,}$$

так как в векторе содержится 2^n элементов, каждый из которых занимает n бит. В табл. 1 приведены объемы памяти, требуемые для хранения подстановок размерности n в виде вектора.

5. Оценка емкости памяти для хранения подстановки в системе счисления ряда факториальных множеств

При использовании подхода, основанного на системе счисления ряда факториальных множеств, каждую подстановку из 2^n элементов можно однозначно представить в виде десятичного числа от 0 до $2^n! - 1$ (так как у множества из 2^n элементов может существовать $2^n!$ биективных отображений на себя). При хранении в памяти номера подстановки, вместо ее самой, необходимо выделение такого числа бит, которое способно представлять число до $2^n!$. В табл. 1 приведено количество бит необходимое для хранения номера подстановки. Как видно из табл. 1, хранение номера подстановки, вместо ее самой, дает существенное уменьшение требуемой памяти. Например, при хранении подстановки из 16 элементов экономится примерно 30% занимаемой памяти.

Также существует еще один способ уменьшения объема памяти требуемой для хранения подстановки. Так как при переводе номера подстановки в саму подстановку при помощи операции деления вычисляются значения сдвигов, которые впоследствии последовательно воздействуют на тождественную подстановку, в памяти можно хранить не номер подстановки, а значения используемых в ее генерации сдвигов. В данном случае экономится меньший объем памяти, однако операция деления для получения сдвигов будет совершаться заранее, тем самым вычисление подстановки менее трудозатратно при выполнении алгоритма криптографического примитива.

Для подстановки, состоящей из 2^n элементов, при помощи операции деления генерируется $2^n - 1$ значений сдвигов, причем диапазон значений отличается для каждого сдвига. Например, для хранения подстановки из 16 элементов необходимо 15 сдвигов, где первый принимает значения от 0 до 15, второй от 0 до 14 и так далее. Для данного способа объем памяти, необходимый для хранения значений циклических сдвигов для n разрядной подстановки, можно определить так:

$$\sum_{i=1}^n i \cdot 2^{i-1} \text{ бит.}$$

В табл. 1 приведено количество бит необходимое для хранения подстановок при помощи значений циклических сдвигов.

Таблица 1. Объем памяти для хранения подстановки

Размерность подстановки, n бит	Объем памяти, бит		
	Стандартный подход	Номер подстановки	Циклический сдвиг
2	8	5	5
3	24	16	17
4	64	45	49
5	160	117	129
6	384	298	321
7	896	716	769
8	2048	1684	1793
9	4608	3876	4097
10	10240	8770	9217

Как видно из табл. 1, способ хранения значений циклических сдвигов требует большего объема памяти, например, для 4-х битной подстановки необходимо на 6% больше памяти. Однако данный способ дает существенный прирост в производительности, так как вычисление значений сдвигов будет осуществляться до начала работы алгоритма,

использующего подстановку. Зависимости требуемого объема памяти для трех способов задания нумерации подстановок приведены на рис. 4. Как видно из рис. 4 объем памяти растет экспоненциально при увеличении размерности n подстановки. При этом хранение номера подстановки требует меньшего объема памяти. Стоит отметить, что так как рост функции факториала происходит быстрее степенной функции, то при больших значениях n хранение подстановок в виде элементов факториальной системы счисления будет менее эффективным, чем стандартный подход. Однако так как на данный момент основными используемыми подстановками являются преобразования размерностями 4 и 8 бит, предложенный метод хранения может использоваться в существующих алгоритмах.

Рис. 4. Зависимость объема памяти от разрядности подстановки
Fig. 4. Dependence of the amount of memory on the substitution digit capacity

При хранении номера подстановки трудоемкость ее развертывания в подстановку заключается в нахождении значений циклических сдвигов тождественной подстановки при помощи последовательного деления ее номера на значения факториалов. Число операций деления для n битной подстановки равно $2^n - 1$. После получения значений сдвигов они циклически воздействуют на тождественную подстановку. Трудоемкость получения подстановки при помощи сдвигов для n битной размерности можно определить так:

$$2^n \cdot \sum_{i=2}^n i \text{ битовых операций.}$$

Заключение

В данной статье преобразование подстановки рассмотрено как элемент системы счисления ряда факториальных множеств. Проведен анализ трех способов хранения нумерации подстановок в памяти: в виде вектора (стандартный метод), в виде значений циклических сдвигов элементов тождественной подстановки и в виде десятичного номера подстановки. Проведена оценка объема памяти, требуемого для хранения подстановки каждым способом. При больших значениях размерности подстановки, хранение стандартным подходом будет более эффективным.

Использование предлагаемых способов дает возможность затрачивать меньший объем памяти для хранения подстановок малой размерности, однако требует использования дополнительных вычислительных ресурсов для определения номера подстановки или значений циклических сдвигов. Благодаря введению в криптопримитивы дополнительных операций по вычислению подстановки, сложность алгоритма будет возрастать, что приведет к замедлению скорости работы примитива. Это может показаться отрицательным фактором, однако такой подход можно использовать для замедления таких примитивов как криптографические хеш-функции для улучшения стойкости к словарным атакам и другим атакам, основанным на большом переборе входных значений.

Данные подходы к хранению подстановок целесообразно использовать в малоресурсных программно-аппаратных комплексах, ограниченных в объемах используемой памяти.

Предложенные способы нумерации подстановок могут быть применены в криптографических блочных алгоритмах шифрования, в которых частью секретного ключа являются подстановки, используемые на каждом раунде. Применение данных способов позволит увеличить длину секретной информации, а также увеличит стойкость алгоритма к дифференциальным и линейным методам криптоанализа, так как алгоритм основывается на незнании противником используемых в конкретном шифровании подстановок, увеличив тем самым область возможного перебора.

СПИСОК ЛИТЕРАТУРЫ:

1. Гнуда В.Д. Структурный анализ преобразования типа «подстановка» / В.Д. Гнуда, В.Т. Карасев, Р.Ж. Тополян // СПБНТОРЭС: труды ежегодной НТК. 2019. № 1 (74). С. 102–103. URL: <https://www.elibrary.ru/item.asp?id=39133391> (дата обращения: 01.02.2021).
2. Буров Д.А., Погорелов Б.А. Рассеивающие свойства линейных преобразований с точки зрения теории групп подстановок // Математические вопросы криптографии. 2018. Т. 9. № 2. С. 47–58. DOI: <https://doi.org/10.4213/mvk252>.
3. Грибунин В.Г., Костюков В.Е., Мартынов А.П., Николаев Д.Б., Фомченко В.Н. Современные методы обеспечения безопасности информации в атомной энергетике: Монография / Под ред. А.И. Асайкина. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2014. – 636 с. DOI: <http://dx.doi.org/10.53403/9785951502650>.
4. Борисенко Н.П. Построение «лёгких» шифров с использованием подстановок с тривиальной группой инерции по отношению к аффинным преобразованиям // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019): сборник научных статей VIII Международной научно-технической и научно-методической конференции. В 4 т., Санкт-Петербург, 27–28 февраля 2019 года. – СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2019. С. 154–159. URL: <https://www.elibrary.ru/item.asp?id=41383511> (дата обращения: 01.02.2021).
5. Мартынов А.П., Фомченко В.Н. Криптография и электроника / Под редакцией А.И. Астайкина. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2006. – 452 с.
6. Пичкур А.Б. Описание класса подстановок, представимых в виде произведения двух подстановок с фиксированным числом мобильных точек // Математические вопросы криптографии. 2012. Т. 3. № 2. С. 79–95. URL: <https://www.elibrary.ru/item.asp?id=18024011> (дата обращения: 01.02.2021).
7. Мартынова И.А., Сплюхин Д.В. Анализ основных характеристических свойств элементов рядов факториальных множеств в процессе защиты информационных систем // Наука. Мысль. 2017. № 5. С. 13–16. URL: <https://www.elibrary.ru/item.asp?id=30742615> (дата обращения: 01.02.2021).
8. Sudoplatov S.V. Distributions of Countable Models of Disjoint Unions of Ehrenfeucht Theories. Lobachevskii J Math 42. 2021. P. 195–205. DOI: <https://doi.org/10.1134/S1995080221010248>.
9. Мартынова И.А., Мартынов А.П., Николаев Д.Б. Криптографические системы и метод факториального сжатия // Известия института инженерной физики. 2016, № 4 (42). С. 54–57. URL: <https://www.elibrary.ru/item.asp?id=27697857> (дата обращения: 01.02.2021).
10. Lanini, M. Twisted quadratic foldings of root systems / M. Lanini, K.V. Zainoulline // Algebra and Analysis. 2021. Vol. 33. No. 1. P. 93–118. URL: <https://arxiv.org/abs/1806.08962> (дата обращения: 01.02.2021).

11. Бабанов Н.Ю., Мартынов А.П., Николаев Д.Б., Фомченко В.Н., Новиков А.В. Виртуальная интерактивная система формирования и отработки управляющей информации. Вестник НГИЭИ. 2016. № 4 (59). С. 15–29. URL: <https://www.elibrary.ru/item.asp?id=26083908> (дата обращения: 01.02.2021).
12. Зубей Е.В. О перестановочности силовских подгрупп с коммутантами B -подгрупп. Журнал Белорусского государственного университета. Математика. Информатика. 2019. № 1. С. 12–17. DOI: <https://doi.org/10.33581/2520-6508-2019-1-12-17>.
13. Dimitrov R.D., Harizanov V.S., Morozov A.S. Turing Degrees and Automorphism Groups of Substructure Lattices. Algebra Logic 59. P. 18–32 (2020). DOI: <https://doi.org/10.1007/s10469-020-09576-x>.
14. Аборнев А.В. Построение подстановок с использованием разрядно-подстановочных преобразований модуля над кольцом Галуа характеристики // Прикладная дискретная математика. 2014. № 1 (23). С. 9–19. URL: <https://www.elibrary.ru/item.asp?id=21403880> (дата обращения: 01.02.2021).
15. Молдовян А.А. и др. Криптография: скоростные шифры. СПб.: БХВ-Петербург, 2002. – 496 с.
16. Мартынов А.П., Мартынова И.А. Функции перестановки в системе счисления ряда факториальных наборов // Вестник ВГУ. Серия: Системный анализ и информационные технологии. 2016, № 3. С. 21–22. URL: <https://www.elibrary.ru/item.asp?id=27296781> (дата обращения: 01.02.2021).
17. Пчелинцев С.В. О тождествах первичных альтернативных алгебр. Алгебра и логика. 2020. Т. 59. № 2. С. 215–238. DOI: <https://doi.org/10.33048/alglg.2020.59.204>.
18. Мартынова И.А., Машин И.Г., Фомченко В.Н. Теория поля и защита информации: Монография. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2017. – 209 с.
19. Мартынов А.П., Мартынова И.А., Фомченко В.Н. Аксиоматические основы функции подстановки в системе счисления ряда факториальных множеств и их характеристики. Монография. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2019. – 209 с.

REFERENCES:

- [1] Gnuda V.D. Structural analysis of the transformation of the «substitution» type. V.D. Gnuda, V.T. Karasev, R. Zh. Topolyan. SPbNTORES: Proceedings of the Annual Scientific and Technical Conference. 2019. No. 1 (74). P. 102–103. URL: <https://www.elibrary.ru/item.asp?id=39133391> (accessed: 01.02.2021) (in Russian).
- [2] Burov D.A., Pogorelov B.A. The permutation group insight on the diffusion property of linear mappings. Mathematical problems of cryptography. 9:2 (2018). P. 47–58. DOI: <https://doi.org/10.4213/mvk252> (in Russian).
- [3] Gribunin V.G., Kostyukov V.E., Martynov A.P., Nikolaev D.B., Fomchenko V.N. Modern methods of ensuring the safety of information in nuclear power: Monograph. Ed. A.I. Asaykin. Sarov: FSUE RFNC-VNIIIEF, 2014. – 636 p. DOI: <http://dx.doi.org/10.53403/9785951502650> (in Russian).
- [4] Borisenko N.P. Construction of "light" ciphers using substitutions with a trivial group of inertia in relation to affine transformations / N. P. Borisenko // Actual problems of information telecommunications in science and education (APINO 2019): collection of scientific articles of the VIII International scientific-technical and scientific-methodical conference: in 4 volumes, St. Petersburg, February 27–28, 2019. – St. Petersburg: St. Petersburg State University of Telecommunications named after prof. M.A. Bonch-Bruевич, 2019. P. 154–159. URL: <https://www.elibrary.ru/item.asp?id=41383511> (accessed: 01.02.2021) (in Russian).
- [5] Martynov A.P., Fomchenko V.N. Cryptography and Electronics. Edited by A.I. Astaykin. Sarov: FSUE RFNC-VNIIIEF, 2006. – 452 p. (in Russian).
- [6] Pichkur, A.B. Description of the class of substitutions representable as a product of two substitutions with a fixed number of mobile points. Mathematical problems of cryptography. 2012. Vol. 3. No. 2. P. 79–95. URL: <https://www.elibrary.ru/item.asp?id=18024011> (accessed: 01.02.2021) (in Russian).
- [7] Martynova I.A., Splyukhin D.V. Analysis of the main characteristic properties of the elements of the series of factorial sets in the process of protecting information systems. Nauka. Think. 2017. No. 5. P. 13–16. URL: <https://www.elibrary.ru/item.asp?id=30742615> (accessed: 01.02.2021) (in Russian).
- [8] Sudoplatov S.V. Distributions of Countable Models of Disjoint Unions of Ehrenfeucht Theories. Lobachevskii J Math 42. 2021. P. 195–205. DOI: <https://doi.org/10.1134/S1995080221010248>.
- [9] Martynova I.A., Martynov A.P., Nikolaev D.B. Cryptographic systems and the factorial compression method. Bulletin of the Institute of Engineering Physics. 2016, no. 4 (42). P. 54–57. URL: <https://www.elibrary.ru/item.asp?id=27697857> (accessed: 01.02.2021) (in Russian).
- [10] Lanini, M. Twisted quadratic foldings of root systems. M. Lanini, K.V. Zainoulline. Algebra and Analysis. 2021. Vol. 33. No 1. P. 93–118. URL: <https://arxiv.org/abs/1806.08962> (accessed: 01.02.2021).
- [11] Babanov N.Yu., Martynov A.P., Nikolaev D.B., Fomchenko V.N., Novikov A.V. Virtual interactive system for generating and processing control information Vestnik NGIEI. 2016. No. 4 (59). P. 15–29. URL: <https://www.elibrary.ru/item.asp?id=26083908> (accessed: 01.02.2021) (in Russian).

- [12] Zubei E.V. On the permutability of Sylow subgroups with commutators of B-subgroups. Journal of the Belarusian State University. Mathematics and Informatics. 2019. No. 1. P. 12–17. DOI: <https://doi.org/10.33581/2520-6508-2019-1-12-17> (in Russian).
- [13] Dimitrov R.D., Harizanov V.S., Morozov A.S. Turing Degrees and Automorphism Groups of Substructure Lattices. Algebra Logic 59. P. 18–32 (2020). DOI: <https://doi.org/10.1007/s10469-020-09576-x>.
- [14] Abornev A.V. Construction of substitutions using bit-substitution transformations of a module over a Galois ring of characteristic. Applied discrete mathematics. 2014. No. 1 (23). P. 9–19. URL: <https://www.elibrary.ru/item.asp?id=21403880> (accessed: 01.02.2021) (in Russian).
- [15] Moldovyan A.A. and other Cryptography: high-speed ciphers. SPb.: BHV-Petersburg, 2002. – 496 p. (in Russian).
- [16] Martynov A.P., Martynova I.A. Permutation functions in the number system of a number of factorial sets. Vestnik VSU. Series: System Analysis and Information Technology. 2016. No. 3. P. 21–22. URL: <https://www.elibrary.ru/item.asp?id=26083908> (accessed: 01.02.2021) (in Russian).
- [17] Pchelintsev S.V. Identities of Prime Alternative Algebras. Algebra Logic. Vol. 59. P. 147–164 (2020). DOI: <https://doi.org/10.1007/s10469-020-09587-8>.
- [18] Martynova I.A., Mashin I.G., Fomchenko V.N. Field theory and information protection: Monograph. Sarov: FSUE RFNC-VNIIEF, 2017. – 209 p. (in Russian).
- [19] Martynov A.P., Martynova I.A., Fomchenko V.N. Axiomatic foundations of the substitution function in the number system of a number of factorial sets and their characteristics. Monograph. Sarov: FSUE RFNC-VNIIEF, 2019. – 209 p. (in Russian).

*Поступила в редакцию – 11 февраля 2021 г. Окончательный вариант – 20 августа 2021 г.
Received – February 11, 2021. The final version – August 20, 2021.*