МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА

Механико-математический факультет

На правах рукописи

Аборнев Александр Викторович

Нелинейные подстановки, линейно представимые над кольцами Галуа, и их приложения в задачах защиты информации

Специальность 01.01.06 — математическая логика, алгебра и теория чисел

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата физико-математических наук

Москва — 2017

Работа выполнена на кафедре высшей алгебры механико-математического факультета ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова».

Научный руководитель: **Латышев Виктор Николаевич**
доктор физико-математических наук, профессор.

Официальные оппоненты: **Туганбаев Аскар Аканович**
доктор физико-математических наук,
профессор, кафедра высшей математики
Национального исследовательского
университета «МЭИ», профессор.

Малышев Фёдор Михайлович
доктор физико-математических наук,
старший научный сотрудник, отдел дискретной математики
Математического института имени В.А. Стеклова РАН,
ведущий научный сотрудник.

Рожков Михаил Иванович
доктор технических наук,
старший научный сотрудник, кафедра компьютерной
безопасности Московского института электроники
и математики им. А.Н. Тихонова НИУ ВШЭ, профессор.

Защита диссертации состоится 16 февраля 2018 года в 16 часов 45 минут на заседании диссертационного совета МГУ.01.17 Московского государственного университета имени М.В. Ломоносова по адресу: 119234, Москва, ГСП-1, Ленинские горы д.1, ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова», механико-математический факультет, аудитория 14-08.

E-mail: msu.01.17@mail.ru

С диссертацией можно ознакомиться в читальном зале отдела диссертаций Фундаментальной библиотеки ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова» по адресу: Ломоносовский проспект, д.27 и на сайте ИАС «Истина»:
https://www.istina.msu.ru/dissertations/91416017/

Автореферат разослан 30 декабря 2017 года.

Учёный секретарь диссертационного
совета МГУ.01.17 ФГБОУ ВО МГУ,
доктор физико-математических наук,
профессор, член-корр. РАН Шафаревич А.И.

Общая характеристика работы

Актуальность темы исследования. Подстановки (биективные преобразования) на векторном пространстве P^m над полем Галуа $P = \mathrm{GF}(q)$ активно изучаются в связи с различными приложениями, и в том числе в теории защиты информации. Чаще всего подстановки используются как элементы при построении узлов переработки информации. В середине XX века К. Шенноном были теоретически обоснованы основные требования к отображениям, реализуемым в таких узлах. Они получили широкое практическое воплощение и известны как принципы перемешивания, рассеивания и усложнения. В настоящее время при построении биективных преобразований данные требования обеспечиваются композицией нелинейных отображений, заданных таблично над полем $\mathrm{GF}(2)$, и линейных рассеивающих преобразований.

Такой подход обусловлен тем, что известно не достаточно теоретически обоснованных классов биективных отображений. Актуальность темы исследования определяется необходимостью поиска новых теоретически обоснованных способов построения классов подстановок на пространстве большой размерности, имеющих требуемые комбинаторно-алгебраические свойства.

Диссертация посвящена исследованию нелинейных подстановок на векторном пространстве над полем Галуа и модуле над кольцом Галуа большой размерности, представимых линейным преобразованием над кольцом Галуа и операцией выделения разряда элемента кольца.

Степень разработанности темы исследования. В современных узлах переработки информации, построенных по итерационному принципу, на каждой итерации реализуется биективное преобразование элементов множества $\mathrm{GF}(2)^m$.

Для построения таких преобразований используется специально выбранное нелинейное преобразование пространства малой размерности (например 4 или 8) и линейное преобразование пространства. Выбор таких преобразований для итеративных преобразований, используемых в системах за-

щиты информации, имеющих требуемые комбинаторно-алгебраические свойства, в общем случае является трудной задачей. В настоящее время многие отечественные и зарубежные специалисты изучают возможность построения новых классов биективных преобразований с помощью подстановочных многочленов над большим полем $\mathrm{GF}(2^m)$ (например, $\mathrm{GF}(2^{128})$). Известны следующие базовые классы подстановчных многочленов: Голд-функции (Gold), функции Касами (Kasami), функция обращения в поле и функции Брекен-Лендер (Bracken-Leander).

Однако использование таких подстановок при больших значениях m проблематично в связи с тем, что не известны эффективные способы их реализации, зачастую отсутствует алгоритм вычисления обратного преобразования, нет возможности перечислять подстановки из данного класса.

Сложность построения подстановок на пространстве обусловлена тем, что в общем виде эта задача эквивалентна задаче построения ортогональных систем многочленов. В теории известны единичные примеры таких классов ортогональных систем (многочлены Диксона).

При построении узлов переработки информации свою эффективность показала теория линейно представимых отображений над кольцами, которая активно развивается отечественными специалистами. В работах Нечаева А.А.[1] , Кузьмина А.С. [2], Куракина В.Л., Хонольда Т., эта теория применяется для построения кодов, рекуррентных последовательностей и их усложнений. При таком способе построения отображений высокая алгебраические степень преобразования и большая линейная сложность получаемых последовательностей обеспечиваются открытым Нечаевым А.А. "эффектом самоусложнения", который состоит в том, что усложнение обеспечивается нелинейностью функции переноса в старший разряд. Ещё одним достоинством таких отображений является простота их реализации на современных

[1]Нечаев, А. А., Хонольд, Т. Полновесные модули и представления кодов // Пробл. передачи информ. — Новосибирск. — 1999. — Т.35. — №3. — С.18—39.

[2] Кузьмин, А. С., Нечаев А.А. Линейно представимые коды и код Кердока над произвольным полем Галуа характеристики 2 // Успехи математических наук. — 1994. — Т. 49. — №5 (299). — С.165—166.

процессорах.

В настоящей диссертации с использованием теории линейно представимых отображений над кольцами строятся нелинейные подстановки на пространстве векторов большой размерности над полем Галуа и модуле над кольцом Галуа. Каждая из подстановок может быть представлена с помощью одного линейного отображения над кольцом Галуа и операции выделения разряда в p-адическом разложении элементов кольца Галуа. Такие подстановки всюду далее называются *линейно представимыми*. В случае, когда указанное линейное преобразование реализуется некоторым линейным автономным регистром сдвига над кольцом Галуа, линейно представимая подстановка π допускает простую программную и аппаратную реализацию. При этом будем называть подстановку π *рекурсивно-порождённой*.

Каждая подстановка на пространстве P^m над полем $P = \mathrm{GF}(q)$ имеет координатное представление $\pi = (\psi_1, \ldots, \psi_m)$, где ψ_j — координатные функции, $j \in \overline{1, m}$. Далее будем говорить, что подстановка π нелинейна, если хотя бы одна из её координатных функций не является линейной функцией. Для случая $P = \mathrm{GF}(2)$ это означает, что степень многочлена Жегалкина одной из координатных функций больше 1.

При исследовании дискретных отображений в защите информации основное внимание уделяется следующим параметрам: алгебраическая степень координатных функций, коэффициент нелинейности, линейная и разностная характеристика, показатель выравнивания, лавинный критерий и его обобщение, корреляционная иммунность и устойчивость, а также перемешивающие свойства.

Обозначим через Σ регулярную подгруппу симметрической группы $\mathfrak{S}(\Omega)$, например, регулярное представление группы $(\Omega, +)$ или циклической группы. Применение одной подстановки из смежного класса $\pi\Sigma$ может быть рассмотрено как один раунд итеративного преобразования $(\pi\Sigma)^k \subset \mathfrak{S}(\Omega)$.

Проблема построения и реализации преобразований итеративного типа состоит в поиске таких подстановок π на пространстве векторов над по-

лем Галуа или модуле над кольцом Галуа размерности m, которые допускают простую и эффективную реализацию, а также обладают необходимыми *комбинаторно-алгебраическими свойствами.* В данной работе к таким свойствам относятся:

- достаточно большая размерность m пространства (модуля) ($m \geq 64$);
- нелинейность подстановки π;
- порождение смежным классом $\pi\Sigma$ знакопеременной группы;
- 2-транзитивность смежного класса $(\pi\Sigma)^k$ при небольших k;
- сходимость последовательности степеней матрицы переходов разностей ненулевых биграмм [3] к равномерной матрице.

В последнее время появились работы зарубежных исследователей, в которых также рассматривается способ прибавления раундовой константы по модулю 2^m, что соответствует циклической группе подстановок на множестве двоичных векторов длины m.

Целью диссертации является построение новых нетривиальных классов нелинейных подстановок на пространстве (свободном модуле) большой размерности, для которых смежные классы по регулярной подгруппе симметрической группы имеют требуемые комбинаторно-алгебраические свойства.

Достижение поставленной цели потребовало решения следующих научных *задач исследования.*

1. Сведение задачи построения линейных преобразований модуля над кольцом Галуа, индуцирующих нелинейные подстановки на пространстве над полем Галуа, к задаче описания ортогональных систем многочленов специального вида над полем.
2. Построение ортогональных систем многочленов, состоящих из квадратичных форм специального вида над полем характеристики 2, которые

[3] Глухов, М. М. О числовых параметрах, связанных с заданием конечных групп системами образующих элементов/ М. М. Глухов // Тр. по дискр. матем: Т.1. — М.: ТВП, 1997. — С.43—66.

являются системой координатных функций линейно представимой подстановки.

3. Описание комбинаторно-алгебраических свойств смежных классов по регулярным подгруппам симметрической группы, соответствующих линейно представимым над кольцом Галуа подстановок:

   - на векторном пространстве над полем Галуа;
   - на модуле над кольцом Галуа, не являющимся полем.

Научная новизна полученных результатов определяется следующими положениями:

1. Впервые установлена возможность построения нелинейных подстановок большой степени в виде композиции линейного преобразования модуля над кольцом Галуа и разрядной функции, применяемой к элементам кольца Галуа.

2. Описаны новые классы ортогональных систем квадратичных форм от большого числа переменных над полем Галуа характеристики 2, а также эффективные способы их перечисления.

3. Предложен оригинальный способ построения множества итеративных преобразований с использованием только просто реализуемых линейно представимых подстановок на пространстве большой размерности.

Методология и методы исследования. При решении задачи построения подстановок применяется и развивается теория многочленов над конечными полями, теория квадратичных форм над полем характеристики 2, теория линейно представимых отображений. При описании класса рекурсивно-порожденных подстановок использовалось представление линейной рекуррентной последовательности с помощью обобщённой функции след в кольце Галуа-Эйзенштейна.

Для описания свойств смежных классов по регулярным подгруппам симметрической группы применяются комбинаторные методы и методы теории конечных групп подстановок.

Теоретическая и практическая значимость диссертации определяется:

1. Развитием математического аппарата теории линейно представимых отображений над кольцами Галуа для исследования класса подстановок специального вида.

2. Построением больших классов нелинейных подстановок с использованием только линейного преобразования и операции выделения разряда элемента кольца Галуа.

3. Разработкой нового критерия ортогональности для широкого класса систем квадратичных форм над полем Галуа характеристики 2.

4. Описанием семейств ЛРП над $\mathbb{Z}_4$, с помощью которых реализуются нелинейные подстановки на двоичном векторном пространстве.

Работа имеет теоретический характер.

Положения, выносимые на защиту.

1. На множестве векторов произвольной фиксированной длины над полем Галуа характеристики 2 построены классы линейно представимых над кольцом Галуа характеристики 4 подстановок, имеющие две нелинейные координатные функции, и эффективно реализуемые классы нелинейных рекурсивно порождённых подстановок.

2. На множестве векторов произвольной длины над произвольным кольцом Галуа, не являющемся полем, построен класс линейно представимых над этим кольцом подстановок с хорошими комбинаторно-алгебраическими свойствами соответствующих матриц переходных вероятностей ненулевых биграмм.

3. Построены классы эффективно реализуемых множеств итеративных преобразований, порождённых линейно представимой подстановкой и

регулярной группой, имеющих гарантированные комбинаторно-алгебраические свойства.

Степень достоверности и апробация результатов. Достоверность полученных результатов определяется наличием строгих математических доказательств. Основные результаты исследования опубликованы в 4 печатных работах, докладывались на конференциях CTCrypt12,13, SIBECRYPT'13,14, конференции "Ломоносовские чтения 2013" в МГУ, а также на научном семинаре МГУ им. Ломоносова.

Структура и объём диссертации. Диссертация состоит из введения, двух глав, заключения, списка условных обозначений и списка литературы.

Основное содержание работы

В первой главе диссертации приводится обзор известных классов подстановок на пространстве большой размерности. Предлагается новый способ построения нелинейных подстановок большой степени, использующий теорию линейно представимых отображений.

Дадим необходимые определения и обозначения. Пусть $R = GR(q^2, p^2)$ — кольцо Галуа с полем вычетов $\overline{R} = R/pR = GF(q)$, $q = p^r$. Подмножество $P = \Gamma(R) = \{a \in R : \ a^q = a\}$ называют *p-адическим разрядным множеством или разрядным множеством Тейхмюллера* кольца R.

Каждый элемент $a \in R$ однозначно представляется в виде

$$a = a_0 + pa_1, \qquad a_s \in P, \qquad s = 0, 1, \tag{1}$$

называемом *p-адическим разложением элемента* a. Возникающие при этом отображения

$$\gamma_s \colon R \to P, \qquad \gamma_s(a) = a_s, \qquad s = 0, 1, \tag{2}$$

называются *разрядными функциями в разрядном множестве* P, а элементы $a_s = \gamma_s(a)$ — *p-адическими разрядами элемента* a.

Алгебра $(P, \oplus, \cdot)$ с естественным умножением и операцией сложения

$$\forall a, b \in P: \qquad a \oplus b = \gamma_0(a + b), \tag{3}$$

есть поле, изоморфное $\overline{R}$.

Пусть $R_{m,n}$ — множество $m \times n$-матриц над R. Понятия p-адического разложения и значения функции γ_s естественным образом (поэлементно) распространяются на матрицы $A = (a(ij)) \in R_{m,n}$:

$$A_s = \gamma_s(A) = (\gamma_s(a(ij))) \in P_{m,m}.$$

В диссертации предлагаются следующие способы построения семейств подстановок, каждая из которых реализуется одним линейным преобразованием модуля $R^{(m)}$ над кольцом Галуа $R = \mathrm{GR}(q^2, p^2)$ и операцией выделения разрядов элементов кольца R:

1. Подстановки на пространстве столбцов $P^{(m)}$ длины m.
2. Подстановки на модуле столбцов $R^{(m)}$ длины m.

1. Подстановки на пространстве столбцов $P^{(m)}$ длины m. Каждой матрице $A \in R_{m\times m}$ можно поставить в соответствие отображение $\pi_A : P^{(m)} \to P^{(m)}$, действующее по правилу:

$$\forall u^{\downarrow} \in P^{(m)}: \quad \pi_A(u^{\downarrow}) = \gamma_1(Au^{\downarrow}). \tag{4}$$

В случае, когда преобразование π_A является подстановкой, матрица A называется *разрядно-подстановочной* или (*РП-матрицей*). Если при этом подстановка π_A нелинейна, то будем говорить, что РП-матрица A *нетривиальна*.

Наибольший интерес для приложений представляют РП-матрицы вида $A = S(F)^m$, где $S(F)$ — сопровождающая матрица многочлена $F(x) = x^m - \sum_{i=0}^{m-1} f_i x^i \in R[x]$. В данном случае подстановка π_A имеет эффективную реализацию на основе линейного регистра сдвига. Унитарный многочлен $F(x)$ степени m, для которого $S(F)^m$ — РП-матрица, называется *РП-многочленом*. РП-многочлен $F(x)$ будем называть *нетривиальным*, если РП-матрица $S(F)^m$ нетривиальна.

Существование РП-матриц для $m \leq 14$ впервые было установлено автором экспериментально при исследовании свойств линейных рекуррентных последовательностей.

В первой главе диссертации подробно изучается случай кольца Галуа характеристики 4. Задача построения линейно представимых подстановок сведена к задаче построения ортогональных систем квадратичных функций. Описаны условия, при которых система квадратичных функций может быть дополнена до подстановки диагональными квадратичными функциями.

Построен критерий ортогональности для широкого класса систем квадратичных форм над полем Галуа характеристики 2. Для любого $m > 2$ описаны системы из двух квадратичных функций

$$\begin{cases} g_1(x_1, \ldots, x_m) = \sigma_2(x_1, \ldots, x_k) \oplus d_{11}x_1^2 \oplus \ldots \oplus d_{1m}x_m^2, \\ g_2(x_1, \ldots, x_m) = \sigma_2(x_s, \ldots, x_t) \oplus d_{21}x_1^2 \oplus \ldots \oplus d_{2m}x_m^2, \end{cases} \tag{5}$$

где $1 < s \leq k < t \leq m$, σ_2 — элементарная симметрическая функция 2 порядка, которые дополняются некоторыми диагональными квадратичными функциями $d_3, \ldots, d_m$ до ортогональной системы

$$\begin{aligned} g_1 &= \sigma_2(x_1, \ldots, x_k) \oplus d_{11}x_1^2 \oplus \ldots \oplus d_{1m}x_m^2, \\ g_2 &= \sigma_2(x_s, \ldots, x_t) \oplus d_{21}x_1^2 \oplus \ldots \oplus d_{2m}x_m^2, \\ d_3 &= d_{31}x_1^2 \oplus \ldots \oplus d_{3m}x_m^2, \\ &\vdots \\ d_m &= d_{m1}x_1^2 \oplus \ldots \oplus d_{mm}x_m^2. \end{aligned} \tag{6}$$

По каждой такой системе можно построить РП-матрицу $A = A_0 + 2A_1 \in R_{m,m}$, где $A_1 = (d_{ij})$, A_0 — некоторая обратимая матрица вида

$$A_0 = \begin{pmatrix} \underbrace{e \ldots\ldots e}_{k} 0 \ldots\ldots 0 \\ \underbrace{0 \ldots 0}_{s-1} \underbrace{e \ldots\ldots e}_{t-s+1} 0 \ldots\ldots 0 \\ \ldots \end{pmatrix}$$

и каждая из строк A_0 с номерами $i \in \overline{3, m}$ содержит ровно по одному ненулевому элементу.

Обозначим через $f_{\overline{n,l}}(\vec{x},\vec{y}),\ 1 \le n < l \le m$ билинейную функцию, ассоциированную с квадратичной формой $\sigma_2(x_n,\dots,x_l)$ на P^m, и через $V^{\perp}_{f_{\overline{n,l}}}$ — ядро билинейной функции $f_{\overline{n,l}}$. Для чисел s,k,t из (5) определим ядро: $V_0^{\perp} = V^{\perp}_{f_{\overline{1,k}}} \cap V^{\perp}_{f_{\overline{s,t}}}$. Далее будем использовать обозначение $a \overset{2}{\equiv} b$ для неотрицательных чисел a,b, таких что $a \equiv b \pmod 2$.

Теорема 1 (1.16). *Для системы* (5) *существует система функций* (6), *такая что*

$$\Pi = (g_1, g_2, d_3, \dots, d_m) : P^m \to P^m \tag{7}$$

является биекцией тогда и только тогда, когда существует пара векторов $\vec{u},\vec{v} \in P^m$, *удовлетворяющая одному из следующих условий* $1-6$*:*

1. *(a)* $\vec{u},\vec{v} \in V_0^{\perp}$,

   (b) система векторов $(g_1(\vec{u}), g_2(\vec{u}))$, $(g_1(\vec{v}), g_2(\vec{v}))$ *линейно-независима над* P.

2. *(a)* $\vec{u} \in V_0^{\perp}$, $\vec{v} \in V^{\perp}_{c_1 f_{\overline{1,k}} \oplus c_2 f_{\overline{s,t}}} \setminus V_0^{\perp}$, *для некоторых* $c_1, c_2 \in P$,

   (b) $(g_1(\vec{u}), g_2(\vec{u})) \neq (0,0)$, $(c_1 g_1 \oplus c_2 g_2)(\vec{u}) = 0$, $(c_1 g_1 \oplus c_2 g_2)(\vec{v}) \neq 0$.

3. *(a)* $s-1 \overset{2}{\equiv} t-k \overset{2}{\equiv} k-s+1 \overset{2}{\equiv} 1$ *и*

$$\vec{u} = (0,\dots,0,0,\dots,0,e,\dots,e,*,\dots,*),$$
$$\vec{v} = (\underbrace{e,\dots,e}_{s-1},\underbrace{0,\dots,0}_{k-s+1},\underbrace{0,\dots,0}_{t-k+1},*,\dots,*);$$

   (b) многочлен $D_1(x) = g_1(\vec{u}) \oplus x g_2(\vec{u}) \oplus x^2 g_1(\vec{v}) \oplus x^3 g_2(\vec{v})$ *не имеет корней в* P, $g_2(\vec{v}) \neq 0$.

4. *(a)* $s-1 \overset{2}{\equiv} t-k \overset{2}{\equiv} 1, k-s+1 \overset{2}{\equiv} 0$, *и*

$$\vec{u} = (e,\ \dots\ ,e,e,\dots,e,\delta_1,\dots,\delta_1,*,\dots,*);$$
$$\vec{v} = (\underbrace{\delta_2,\dots,\delta_2}_{s-1},\underbrace{e,\dots,e}_{k-s+1},\underbrace{e,\dots,e}_{t-k+1},*,\dots,*);$$

   где $\delta_1 \neq e, \delta_2 \neq e$.

(b) *многочлен* $D_2(x) = g_1(\vec{u}) \oplus x\frac{\delta_2 \oplus e}{\delta_1 \oplus e} g_2(\vec{u}) \oplus x^2 g_1(\vec{v}) \oplus x^3 \frac{\delta_2 \oplus e}{\delta_1 \oplus e} g_2(\vec{v})$ *не имеет корней в* P, $g_2(\vec{v}) \neq 0$.

5. *(a)* $s-1 \overset{2}{\equiv} 1, t-k \overset{2}{\equiv} 0, k-s+1 \overset{2}{\equiv} 0$ *и*

$$\vec{u} = (e, \ldots, e, e, \ldots, e, 0, \ldots, 0, *, \ldots, *);$$
$$\vec{v} = (\underbrace{e, \ldots, e}_{s-1}, \underbrace{0, \ldots, 0}_{k-s+1}, \underbrace{0, \ldots, 0}_{t-k+1}, *, \ldots, *);$$

(b) *многочлен* $D_3(x) = g_1(\vec{u}) \oplus x g_2(\vec{u}) \oplus x^2 g_1(\vec{v}) \oplus x^3 g_2(\vec{v})$ *не имеет корней в* P, $g_2(\vec{v}) \neq 0$.

6. *(a)* $s-1 \overset{2}{\equiv} 0, t-k \overset{2}{\equiv} 1, k-s+1 \overset{2}{\equiv} 0$ *и*

$$\vec{u} = (\underbrace{0, \ldots, 0}_{s-1}, \underbrace{0, \ldots, 0}_{k-s+1}, \underbrace{e, \ldots, e}_{t-k+1}, *, \ldots, *);$$
$$\vec{v} = (0, \ldots, 0, e, \ldots, e, e, \ldots, e, *, \ldots, *);$$

(b) *многочлен* $D_4(x) = g_1(\vec{u}) \oplus x g_2(\vec{u}) \oplus x^2 g_1(\vec{v}) \oplus x^3 g_2(\vec{v})$ *не имеет корней в* P, $g_2(\vec{v}) \neq 0$.

Для классов подстановок на пространстве $\mathrm{GF}(2)^m$, описанных в теореме, получен эффективный способ их перечисления при произвольном $m \geq 3$.

Линейные рекуррентные последовательности долгое время остаются востребованными при построении псевдослучайных последовательностей. В диссертации описано новое применение ЛРП над кольцом $\mathbb{Z}_4$. Ниже приводятся классы нелинейных подстановок, представимых с помощью линейных преобразований, заданных рекуррентным законом.

Пусть $F(x) = x^m - \sum\limits_{i=0}^{m-1} f_i x^i \in R[x]$.

Подстановка π_F, порождённая РП-многочленом $F(x)$, для любого $u \in L_R(F)$, такого что $u_1[\,\overline{0, m-1}\,] = (0, ..., 0)$, удовлетворяет равенству

$$\pi_F(u_0[\,\overline{0, m-1}\,]) = u_1[\,\overline{m, 2m-1}\,]. \tag{8}$$

Поэтому для нахождения значения $\pi_F(u_0[\,\overline{0, m-1}\,])$ достаточно вычислить m элементов $u[\,\overline{m, 2m-1}\,]$ последовательности $u \in L_R(F)$.

Получены два больших нетривиальных класса РП-многочленов.

Введём обозначения

$$F_0(x) = x^m \oplus \bigoplus_{i=0}^{m-1} \gamma_0(f_i)x^i, \quad F_1(x) = \bigoplus_{i=0}^{m-1} \gamma_1(f_i)x^i.$$

Теорема 2 (1.17). *Пусть $R = \mathbb{Z}_4$, $F(x) \in R[x]$ — многочлен степени $m \geq 3$.*

Если $F_0(x) = x^m \oplus x^{m-1} \oplus x \oplus e$, то $F(x)$ является РП-многочленом тогда и только тогда, когда

$$(F_0(x), e \oplus F_1(x)) = e, \quad (F_0(x), x \oplus F_1(x)) = e. \tag{9}$$

Для описания второго класса РП-многочленов рассмотрим унитарный многочлен $F(x) \equiv (x-e)^m \pmod{2R}$ степени $m \geq 3$ над кольцом $R = \mathbb{Z}_4$. Его можно представить в виде

$$F(x) = C(x-e), \quad C(x) = x^m - 2c_{m-1}x^{m-1} - \ldots - 2c_0 \in R[x], \tag{10}$$

где $c_0, \ldots, c_{m-1} \in \{0, 1\}$.

Теорема 3 (1.18). *Пусть $R = \mathbb{Z}_4$. Многочлен $F(x) \in R[x]$ вида* (10) *степени $m \geq 3$ является РП-многочленом тогда и только тогда, когда $F(e) \neq 0$, то есть $c_0 = e$.*

2. Линейно представимые подстановки на свободном модуле R^m строк длины m над кольцом Галуа R.

Построены новые классы линейно представимых подстановок на свободном модуле R^m строк длины m над кольцом Галуа R.

Матрица W размеров $m \times n$ над кольцом Галуа R называется *разрядно-инъективной* (*РИ-матрицей*), если любая ненулевая строка $\vec{u} \in R^m$ однозначно восстанавливается по строке $\gamma_1(\vec{u}W) \in P^n$.

Пусть $n = 2m$ и $W \in R_{m,2m}$ — разрядно-инъективная матрица. Заметим, что умножение вектора $\gamma_1(\vec{x}W) = (\vec{y}' \mid \vec{y}'') \in P^{2m}$ на матрицу $\binom{E}{pE}$ дает вектор $\vec{y}' + p\vec{y}'' \in R^m$. Поэтому отображение $\eta_W : R^m \to R^m$ вида

$$\eta_W(\vec{x}) = \gamma_1(\vec{x}W)\binom{E}{pE}, \tag{11}$$

где $E \in R_{m,m}$ — единичная матрица, является подстановкой на модуле R^m.

Профессором Нечаевым А.А. предложен способ построения большого класса РИ-матриц размеров $m \times 2m$, который приводится в следующей теореме.

Теорема 4 (1.21). *Если $U_{m\times m}$ — обратимая матрица над кольцом R, $G_{m\times m}$ — обратимая матрица над полем P, то матрица $W_{m\times 2m}$ над кольцом R вида*

$$W = U(E \mid E + pG) = (U \mid V) \tag{12}$$

является разрядно-инъективной.

Показано, что среди таких матриц также существуют РИ-матрицы, которые могут быть просто реализованы с использованием линейного рекуррентного закона.

Во второй главе изучаются свойства линейно представимых подстановок, построенных в первой главе, и комбинаторно-алгебраические свойства итеративных преобразований, построенных с использованием линейно представимых подстановок и регулярной группы подстановок.

При исследовании дискретных отображений основное внимание уделяется исследованию следующих криптографических параметров: алгебраическая степень координатных функций, нелинейность, линейная и разностная характеристика, перемешивающие свойства.

Некоторые из указанных параметров определяются параметрами координатных функций подстановки. Для построенных подстановок π_A координатные функции $\psi_1, \ldots, \psi_m$ являются квадратичными формами или линейными функциями, поэтому их свойства удаётся выразить через элементы матрицы A.

Построенный класс позволяет также эффективно использовать подстановки из множества $\pi_A^k,\ k \in \mathbb{N}$.

Алгебраическая степень такой подстановки π_F равна 2, и $\deg \pi_F^k \geq k + 1,\ \ k \in \overline{2,m}$.

Пусть $\Omega \in \{P^{(m)}, R^{(m)}\},\ |\Omega| = N$.

Пусть $\pi \in \mathfrak{S}(\Omega)$ — линейно представимая подстановка. Обозначим через Σ регулярную подгруппу симметрической группы $\mathfrak{S}(\Omega)$, например, регулярное представление группы $(\Omega, +)$ или циклической группы. Применение одной подстановки из смежного класса $\pi\Sigma$ может быть рассмотрено как один раунд итеративного преобразования из $(\pi\Sigma)^k \subset \mathfrak{S}(\Omega)$.

Для преобразований итеративного типа на основе линейно представимых подстановок изучаются следующие комбинаторно-алгебраические свойства:

- группа, порождаемая смежным классом $\pi\Sigma$;
- свойства матрицы переходов разностей ненулевых биграмм смежного класса $\pi\Sigma$;
- показатель $d_2(\pi\Sigma)$ 2-транзитивности класса $\pi\Sigma$

$$d_2(\pi\Sigma) = \min\{k \geq 1 : (\pi\Sigma)^k \text{ 2-транзитивно}\}.$$

Пусть далее $R = \mathbb{Z}_{p^2}$, $P = \mathbb{Z}_p$, где p — простое. В работе исследуются свойства смежных классов, соответствующих подстановокам на пространстве $\Omega = P^{(m)}$ столбцов длины m над полем P. Пусть $\pi_A = (\psi_1, \ldots, \psi_m)$ — подстановка вида (4), соответствующая некоторой разрядно-подстановочной матрице $A \in R_{m,m}$. Через Σ обозначим регулярную подгруппу в $\mathfrak{S}(\Omega)$. В работе рассматривается два класса преобразований:

1. Итеративные преобразования, порождённые циклической группой;
2. Итеративные преобразования, порождённые группой сдвигов.

Итеративные преобразования, порождённые циклической группой.

Для данного класса преобразований описаны условия, при которых смежный класс порождает симметрическую группу.

Пусть $\Sigma = G$ — регулярное представление циклической группы $(\mathbb{Z}_{p^m}, +)$ в $\mathfrak{S}(\mathbb{Z}_p^{(m)})$, порождённой полным циклом $t = (0, 1, 2, \ldots, p^m - 1)$. При этом для

$a^{\downarrow}, b^{\downarrow} \in \mathbb{Z}_p^{(m)}$, $a^{\downarrow} = (a_1, \ldots, a_m)^T$, $b^{\downarrow} = (b_1, \ldots, b_m)^T$ операция $+$ определяется из равенства

$$a^{\downarrow} + b^{\downarrow} = (c_1, \ldots, c_m), \tag{13}$$

где элементы $c_1, \ldots, c_m \in \mathbb{Z}_p$ определяются из равенства

$$c_1 + \ldots + p^{m-1} c_m = (a_1 + pa_2 + \ldots + p^{m-1} a_m) + (b_1 + pb_2 + \ldots + p^{m-1} b_m) \pmod{p^m}.$$

Зададим ориентированный граф $\mathcal{G}(\pi_{\mathcal{A}})$ с множеством вершин $\overline{1, m}$ и имеющий дугу из s в i, в точности если $s \leq i$ или координатная функция ψ_i отображения π_A существенно зависит от переменной y_s. Граф $\mathcal{G}(\pi_{\mathcal{A}})$ просто строится по матрице A. Дуга из s в i существует в одном из следующих случаев:

(a) $s \leq i$;

(b) $a_1(is) \neq 0$;

(c) $a_0(is) \neq 0$ и строка $(a_0(i1), \ldots, a_0(im))$ имеет более, чем 1 ненулевую координату.

Следующая теорема доказана в предположении, что верна S-гипотеза (все конечные простые группы известны).

Теорема 5 (2.1). *Пусть при введённых выше обозначениях граф $\mathcal{G}(\pi_{\mathcal{A}})$ сильно связен. Тогда справедливы следующие утверждения:*

1. *Если $p = 2$ и $2^m - 1$ составное число, то $\langle \pi_A G \rangle = \mathfrak{S}(P^{(m)})$.*
2. *Если $p \geq 3$, S-гипотеза верна и*

$$p^m \notin \left\{ 11,\ 23,\ \frac{p_1^n - 1}{p_1 - 1},\ p_1^3 + 1,\ d^{d(2n+1)} + 1 :\ \ p_1 \text{ – простое}, d \in \{2, 3\},\ n \geq 1 \right\}, \tag{14}$$

то $\langle \pi_A G \rangle \supseteq \mathfrak{A}(P^m)$.

Следствие 5.1 (2.1.1). *Пусть $p = 2$ и $2^m - 1$ составное число. Если первая координатная функция подстановки π_A существенно зависит от последней переменной, то $\langle \pi_A G \rangle = \mathfrak{S}(P^{(m)})$.*

Для оценки разностных свойств отображений, построенных с использованием полученных подстановок, изучаются элементы матрицы переходов

разностей ненулевых биграмм для соответствующего смежного класса, порожденного группой G.

Элементы матрицы переходов разностей ненулевых биграмм определяются количеством решений $x^{\downarrow} \in \Omega$ уравнения

$$\pi_A(x^{\downarrow} + a^{\downarrow}) - \pi_A(x^{\downarrow}) = b^{\downarrow}, \qquad a^{\downarrow}, b^{\downarrow} \in \Omega.$$

В общем виде описание данной матрицы является сложной задачей. Для значений $m < 17$ такую матрицу можно вычислить в явном виде и из её свойств делать выводы о показателе 2-транзитивности и скорости сходимости последовательности её степеней к равномерной матрице.

В диссертации приводятся примеры рекурсивно порождённых линейно представимых подстановок, для которых показатель 2-транзитивности соответствующего смежного класса равен 3, то есть достигает минимально возможного значения.

1. π_F — квадратичная подстановка, где

   $$F(x) = x^{11} - x^{10} - 2x^7 - 3x^6 - 3x^5 - 3x^4 - 3x^2 - 2x - 1 \in \mathbb{Z}_4[x],$$

   для обеих регулярных групп (группы сдвигов Σ и циклической группы G). При этом $\langle \pi_F G \rangle = \mathfrak{S}(P^{(11)})$ и $\langle \pi_F \Sigma \rangle = \mathfrak{A}(P^{(11)})$.

2. π_F — подстановка на $\mathrm{GF}(2)^{16}$, индуцированная РП-многочленом

   $$F(x) = x^{16} + 3x^{15} + 2x^{14} + 2x^{12} + 2x^{11} + 2x^{10} + 2x^9 + 2x^7 + 2x^5 + 2x^4 + 2x^2 + x + 3.$$

   для случая циклической группы G. При этом $\langle \pi_F G \rangle = \mathfrak{S}(P^{(16)})$

3. π_F подстановка на $\mathrm{GF}(2)^8$, индуцированная РП-многочленом

   $$F(x) = x^8 + x^7 + 2x^4 + 3x + 3.$$

   для случая циклической группы G. При этом $\langle \pi_F G \rangle = \mathfrak{S}(P^{(16)})$.

4. Степень π_F^4 подстановки π_F из пункта 3, для группы сдвигов Σ.

Аналитическая сложность раундового преобразования определяется координатными функциями подстановки π_A и функциями переноса в старшие разряды при прибавлении раундовой константы. Раундовое преобразование задаётся выражением

$$\mathcal{R}_+(x^{\downarrow}, k^{\downarrow}) = \pi_A(x^{\downarrow} + k^{\downarrow}). \tag{15}$$

В координатной форме оно имеет вид

$$\mathcal{R}_+(x^{\downarrow}, k^{\downarrow}) = \begin{pmatrix} \rho_1(x^{\downarrow}, k^{\downarrow}) \\ \vdots \\ \rho_m(x^{\downarrow}, k^{\downarrow}) \end{pmatrix}. \tag{16}$$

При этом для каждого $i \in \overline{1, m}$ справедливо равенство

$$\rho_i(x^{\downarrow}, k^{\downarrow}) = \psi_i(x_1 \oplus k_1, x_2 \oplus k_2 \oplus \delta_1(x_1^{\downarrow}, k_1^{\downarrow}), \ldots, x_m \oplus k_m \oplus \delta_{m-1}(x_{m-1}^{\downarrow}, k_{m-1}^{\downarrow})), \tag{17}$$

где $x_s^{\downarrow} = (x_1, x_2, \ldots, x_s)^T$, $s = \overline{1, m-1}$ и $\delta_s(x_s^{\downarrow}, y_s^{\downarrow})$ — функция переноса в s-й двоичный разряд суммы $x_1 + 2x_2 + \ldots + 2^{s-1}x_s + y_1 + 2y_2 + \ldots + 2^{s-1}y_s$. Необходимо заметить, что степень нелинейности многочлена ρ_i определяется коэффициентами матрицы A. Поэтому матрицу можно выбирать так, чтобы указанные степени нелинейности были достаточно большими.

Прибавление раундовой константы реализуется сложением по модулю p^m. Скорость выполнения данной операции на современной вычислительной технике имеет тот же порядок, что и сложение векторов по модулю p. В случае выполнения операций по модулю 2^m, который представляет наибольший интерес, трудоемкость сложения линейно зависит от длины битового представления состояний.

Для программной реализации подстановки π_A в общем случае требуется m^2 ячеек памяти, содержащих элементы кольца R. Для рекурсивно порождённых разрядно-подстановочных матриц, требуется лишь m ячеек памяти, содержащих элементы кольца R.

При выполнении аппаратной реализации такие подстановки могут быть реализованы без использования памяти.

Таким образом, в случае, когда группа G является регулярным представлением циклической группы, построенный класс итеративных преобразований обладает следующими достоинствами:

- для больших классов линейно представимых подстановок порождается вся симметрическая группа;
- получен способ простой реализации;
- большая доля элементов матрицы переходов разностей ненулевых биграмм ненулевые;
- высокая алгебраическая степень координатных функций результирующего отображения, обусловленная нелинейностью функции переноса в старшие разряды.

Данные результаты подтверждают необходимость дальнейшего исследования свойства итеративных преобразований, построенных с использованием циклической группы подстановок. Такие работы проводились отечественными специалистами уже в 70-х годах и продолжаются в настоящее время (Малышев Ф.М.). В последнее время зарубежные авторы (К. Нюберг, Д. Валлен и др.) также исследуют линейные и дифференциальные свойства сложения по модулю 2^m.

Итеративные преобразования, порождённые группой сдвигов.

Опишем свойства смежного класса $\pi_A\Sigma$ в случае, когда Σ — регулярное представление группы сдвигов $(P^{(m)}, \oplus)$ в $\mathfrak{S}(P^{(m)})$.

Для описания группы, порождаемой смежным классом $\pi_A\Sigma$, в общем виде применима классификация Ли примитивных групп, содержащих регулярную абелеву подгруппу. Данный результат является развитием известной теоремы О'Нэна-Скотта.

Более точное описание порождаемой группы в общем случае для линейно представимых подстановок является сложной задачей. Проведённые вычисления на ЭВМ показывают, что для большой доли РП-матриц над кольцом $\mathbb{Z}_4$ порождается знакопеременная группа.

Для описания матрицы переходов разностей ненулевых биграмм смежного класса $\pi_A\Sigma$ в случае, когда $P = \mathrm{GF}(q), q = 2^r$, применим следующий подход.

Пусть π_A – линейно представимая подстановка вида

$$\pi_A = (\psi_1, \psi_2, \ldots, \psi_m)^T, \tag{18}$$

где ψ_i — квадратичные формы над P, $i = \overline{1,m}$. Пусть f_i — билинейная форма, ассоциированная с квадратичной формой ψ_i, $i \in \overline{1,m}$. Опишем свойства матрицы $Q_{\pi_A} = \dfrac{1}{q^m}(q^{\pi_A}_{a^\downarrow,b^\downarrow})_{a^\downarrow,b^\downarrow \in P^m \setminus \{\mathbf{0}\}}$ переходов разностей ненулевых биграмм множества подстановок $\pi_A\Sigma$.

Предложение 6 (2.4)**.** *При введённых выше обозначениях элемент $q^{\pi_A}_{a^\downarrow,b^\downarrow}$ матрицы Q_{π_A} равен количеству решений системы уравнений*

$$\begin{cases} f_1(x^\downarrow, a^\downarrow) = \psi_1(a^\downarrow) \oplus b_1 \\ f_2(x^\downarrow, a^\downarrow) = \psi_2(a^\downarrow) \oplus b_2 \\ \ldots \\ f_m(x^\downarrow, a^\downarrow) = \psi_m(a^\downarrow) \oplus b_m \end{cases} \tag{19}$$

где $b^\downarrow = (b_1, \ldots, b_m)^T$, относительно неизвестного $x^\downarrow \in P^{(m)}$.

В диссертации удалось построить класс разрядно-подстановочных матриц A размеров $m \times m$, определяющая подстановка π_A которых имеет одну нелинейную координатную функцию и обладает следующими свойствами:

1. Группа $\langle \pi_A\Sigma \rangle$ 2-транзитивна;
2. $d_2(\pi_A\Sigma) = m + 2$.

Необходимо отметить, что эффективно реализуемыми подстановками являются также подстановки π_A^k, $k \in \mathbb{N}$. Они обладают лучшими комбинаторно-алгебраическими свойствами, нежели подстановка π_A. Построенный класс преобразований расширяется естественным образом и допускает параметрическое задание подстановок при реализации.

Итеративные преобразования на основе разрядно-инъективных матриц.

В качестве приложения разрядно-инъективных матриц изучается итеративное преобразование, реализующее подстановки из множества $(\eta_W\Sigma)^k$, где Σ — регулярное представление группы $(R^m,+)$ в группе $\mathfrak{S}(R^m)$, η_W — подстановка на R^m, индуцированная разрядно-инъективной матрицей W.

Получена оценку снизу показателя 2-транзитивности $d_2(\eta_W\Sigma)$ для класса подстановок η_W вида (11).

Теорема 7 (2.12). *Пусть η_W — подстановка на R^m, определенная равенством* (11). *Тогда $d_2(\eta_W\Sigma)\geq 4$.*

Построено два больших класса РИ-матриц, для которых доказанная оценка достигается.

Пусть $R=\mathrm{GR}(q^2,p^2),\ P=\Gamma(R),\ q=p^r,\ m=1,p>2$. В этом случае преобразование одного раунда будем записывать в виде

$$\eta(x)=\gamma_1(xu(e\mid e+pg))Z=\gamma_1(xu)+p(\gamma_1(xu)\oplus x_0u_0g_0), \tag{20}$$

где $u\in R^*, g\in\Gamma(R)$.

Заметим, что всегда справедливо включение $\{\gamma_1(a+e)\ominus\gamma_1(b+e):a,b\in P\}\subset P$. Следующая теорема описывает условия для колец Галуа при $p>2$, при выполнении которых любая нетривиальная РИ-матрица индуцирует 2-транзитивное множество подстановок с минимально возможным показателем 2-транзитивности.

Теорема 8 (2.13). *Пусть для кольца Галуа $R=\mathrm{GR}(q^2,p^2), p>2$, выполнено условие*

$$\{\gamma_1(a+e)\ominus\gamma_1(b+e):a,b\in P\}=P, \tag{21}$$

и η — подстановка вида (20). *Тогда имеет место равенство $d_2(\eta\Sigma)=4$.*

Экспериментально подтверждено, что равенство (21) справедливо для $\mathbb{Z}_{p^2}$, где $p\leq 283$, а также для колец Галуа $\mathrm{GR}(9^2,3^2)$, $\mathrm{GR}(27^2,3^2)$. Описание колец Галуа, для которых выполнено условие (21) остается открытой задачей.

Важно отметить, что примеров, когда условие (21) не выполняется, не найдено.

Предложение 9 (2.14)**.** *Пусть* $p = 3, q = p^r,\ R = \mathrm{GR}(q^2, p^2)$*, тогда выполнено равенство* (21)*.*

В предположении, что верна S-гипотеза (все конечные простые группы известны), удается описать свойства группы $\langle \eta\Sigma \rangle$.

Предложение 10 (2.15)**.** *Пусть верна S-гипотеза,* $R = \mathbb{Z}_{p^2}$*. Если множество* Σ *содержит подстановку, заданную равенством* $t(x) \equiv x+1 \pmod{p^2}$ *(полный цикл), то* $\langle \eta\Sigma \rangle \supseteq \mathfrak{A}(R)$*.*

Второй класс подстановок описывает следующая теорема.

Теорема 11 (2.16)**.** *Пусть* $R = \mathrm{GR}(q^2, 4),\ P = \Gamma(R), m \in \mathbb{N}$*, матрица* W *вида* (12) *выбрана так, что все миноры матрицы* U_0 *отличны от нуля. Тогда* $d_2(\eta_W\Sigma) = 4$*.*

Заключение

В диссертации получены следующие основные результаты.

Показано, что существуют классы нелинейных подстановок на пространстве (модуле) произвольной размерности над полем (кольцом) Галуа характеристики p (характеристики p^2). Такие подстановки могут быть построены, например, композицией линейного преобразования модуля и операцией выделения 1-го разряда.

Доказано, что задача построения подстановок, линейно представимых над кольцом Галуа характеристики 4, эквивалентна сложной задаче построения ортогональных систем квадратичных форм специального вида. Получен способ эффективного решения этой задачи, состоящий в дополнении двух нелинейных квадратичных функций специального вида диагональными квадратичными формами до ортогональной системы.

Описаны классы подстановок, реализуемые с помощью некоторого линейного закона рекурсии. Для реализации такой подстановки на пространстве $GF(2)^m$ достаточно вычислить m знаков ЛРП над $\mathbb{Z}_4$.

Линейно представимые подстановки могут использоваться в качестве раундового преобразования итеративных преобразований. Для случая, когда прибавление раундовой константы осуществляется по модулю 2^m, то есть преобразование порождено циклической группой, существуют большие классы подстановок на пространстве $\mathrm{GF}(2)^m$, для которых соответствующий смежный класс порождает всю симметрическую группу.

Линейно представимые подстановки допускают эффективную реализацию без использования памяти и обеспечивают высокую скорость работы алгоритма. С помощью таких подстановок могут быть реализованы 2-транзитивные множества подстановок, а также множества, порождающие знакопеременную группу.

Существуют большие классы разрядно-инъективных матриц, индуцирующих подстановки на модуле с минимально возможным значением показателя 2-транзитивности.

В качестве дальнейшей разработки темы диссертации могут быть рассмотрены следующие направления: обобщение критерия ортогональности систем квадратичных форм, описание всех рекурсивно-порождённых линейно представимых подстановок и их комбинаторно-алгебраических свойств, обобщение полученных результатов на кольца Галуа характеристики $p > 2$.

Благодарности

Автор выражает искреннюю благодарность научному руководителю доктору физико-математических наук, профессору Латышеву Виктору Николаевичу и доктору физико-математических наук, профессору Александру Александровичу Нечаеву за постановку задачи, внимание к работе, поддержку и ценные советы.

Публикации автора по теме диссертации

[1] **Abornev, A. V.** Nonlinear permutations on a space over a finite field induced by linear transformations of a module over a Galois ring/ A. A. Nechaev, A. V. Abornev// *Математические вопросы криптографии.*— 2013.— Т. 4. — №2. — С. 81—100.
(Индекс в базе RSCI Web of Science: RSCI:20134175, ISSN:2220-2617. Лично автору принадлежат доказательство критерия ортогональности системы квадратичных функций и доказательство свойств группы, порождаемой смежным классом по циклической подгруппе симметрической группы.)

[2] **Аборнев, А. В.** Подстановки, индуцированные разрядно-инъективными преобразованиями модуля над кольцом Галуа/ А. В. Аборнев// *Прикладная дискретная математика.*— 2013.— №4(22). — С. 5—15 (Индекс в базе RSCI Web of Science: RSCI:21155546, ISSN:2071-0410).

[3] **Аборнев, А. В.** Построение подстановок с использованием разрядно-подстановочных преобразований модуля над кольцом Галуа характеристики 4/ А. В. Аборнев// *Прикладная дискретная математика.*— 2014.— №1(23). — С. 9—19.
(Индекс в базе RSCI Web of Science: RSCI:21403880, ISSN:2071-0410)

[4] **Abornev, A. V.** Recursively-generated permutations of a binary space/ A. V. Abornev// *Математические вопросы криптографии.*— 2014.— Т. 5. — №2. — С. 7—20.
(Индекс в базе RSCI Web of Science: RSCI:23048430, ISSN:2220-2617)

[5] **Аборнев, А. В.** Разрядно-инъективные преобразования модуля над кольцом Галуа/ А. В. Аборнев// *ПДМ. Приложение.*— 2013.— №6. — С. 6—7.

[6] **Аборнев, А. В.** Нелинейные подстановки на векторном пространстве, рекурсивно-порождённые над кольцом Галуа характеристики 4/ А. В. Аборнев// *ПДМ. Приложение.*— 2014.— №7. — С. 40—41.