На правах рукописи

Саранцев Алексей Васильевич

ПОСТРОЕНИЕ ВЗАИМНО ОДНОЗНАЧНЫХ ПРЕОБРАЗОВАНИЙ НА ОСНОВЕ ОДНОТИПНЫХ ДВОИЧНЫХ ФУНКЦИЙ В СВЯЗИ С ЗАДАЧАМИ ЗАЩИТЫ ИНФОРМАЦИИ

05.13.19 — методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание учёной степени кандидата технических наук

Москва — 2010

Работа выполнена на кафедре №713 факультета прикладной математики Института криптографии, связи и информатики Академии ФСБ России

Научный руководитель: доктор технических наук, доцент В. Г. Никонов

Официальные оппоненты: доктор технических наук, профессор Е. Е. Тимонина

кандидат технических наук В. Б. Нетыкшо

Ведущая организация: Пограничная академия ФСБ России

Защита состоится 26 апреля 2010 г. в 14 часов на заседании диссертационного совета Д 212.198.13 при государственном учреждении Российский государственный гуманитарный университет (РГГУ) по адресу: г. Москва, Миусская пл., д. 6 (Профессорский зал).

С диссертацией можно ознакомиться в библиотеке Российского государственного гуманитарного университета.

Автореферат разослан 22 марта 2010 г.

Учёный секретарь
диссертационного совета,
кандидат технических наук,
старший научный сотрудник Д. Б. Халяпин

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Развитие информационных технологий, совершенствование средств обработки и хранения информации способствует расширению сферы использования вычислительных средств. Достижения в области аппаратной и программной реализации алгоритмов обработки данных обеспечивают удобство эксплуатации технических средств. Объём обрабатываемых данных растёт в соответствии с возрастающими потребностями современного общества, поэтому автоматизированное использование компьютерных технологий является одним из самых практичных методов обработки информации.

Решение задач идентификации и аутентификации, контроля целостности и распознавания образов требует построения преобразований фрагментов информации, зависящих от некоторого секрета. Традиционные криптографические методы защиты информации используют обратимые преобразования, зависящие от секретного ключа. Основным требованием, предъявляемым к таким преобразованиям, является стойкость к атакам, направленным на нахождение защищаемой информации, без знания секретного ключа, либо нахождение самого секретного ключа. Стойкость обычно измеряется временем, которое необходимо для успешного выполнения атаки при некоторых фиксированных ресурсах, имеющихся в распоряжении у злоумышленника, реализующего атаки на систему защиты. Повышение стойкости системы защиты путём усложнения аналитической и статистической структуры используемых преобразований приводит к увеличению объёма ресурсов, требуемых для реализации системы защиты. Уровень стойкости системы защиты характеризуется нижней оценкой времени, требуемого на нарушение системы защиты, и определяется в первую очередь вычислительными ресурсами потенциального взломщика, а также временем, в течение которого защищаемая информация должна оставаться недоступной взломщику. Повышение стойкости системы защиты приводит к росту материальных затрат потенциального нарушителя, используемых для оплаты технических, интеллектуальных и организационных средств при проведении атаки. Материальные средства, выделяемые на проведение атаки, определяются выгодой, которую получит нарушитель при нанесении ущерба системе защиты. Такая выгода противника может быть

оценена стоимостью атакуемых активов. Широкое применение приобретают компактные узлы и блоки переработки информации в системах управления, идентификации и контроля, размещённые в условиях, когда основным ценовым параметром становится емкостная сложность реализации преобразования. При этом вопросы стойкости используемой системы защиты не являются первоочередными, поскольку ценность обрабатываемой этими узлами информации стремительно падает с течением времени. Такие узлы используются для контроля доступа, идентификации транспортных средств, отслеживания активов, контроля производственных запасов, автоматизации производства и складской обработки, контроля за перемещением потоков грузов и транспорта и других задач. Особую ценность минимизация емкостной сложности реализации узлов переработки информации приобретает, в частности, в аэрокосмической области при решении задач идентификации удалённых объектов.

Цель работы состоит в разработке новых математических и технических принципов построения просто реализуемых на современной элементной базе биективных преобразований, используемых в средствах защиты информации и обеспечения информационной безопасности.

Методы исследования. В процессе проведения исследования для изучения инженерных вопросов реализации схем защиты информации применялись алгебраические методы и методы математической логики.

Научная новизна диссертации состоит в следующем.

1) Дано теоретическое описание регулярных систем двоичных функций, построенных на основе группы сдвига и произвольной двоичной функции степени нелинейности 2.

2) Проведено исчерпывающее изучение строения регулярных систем, координатные функции которых эквивалентны относительно преобразования циклического сдвига координат, и построены классы двоичных функций степени нелинейности 3, порождающие такие системы.

3) Описано множество регулярных систем, построенных на основе фильтрующего генератора с нелинейной функцией усложнения второй степени.

4) Проведена каталогизация регулярных систем однотипных двоичных функций от четырёх переменных.

Теоретическая ценность представлена следующими содержащимися в работе положениями.

1) Выделены и исследованы инварианты подстановок, задаваемых регулярными системами однотипных двоичных функций, позволяющие существенно сократить количество представителей при каталогизации систем однотипных функций.

2) Описаны классы преобразований, порождаемые нелинейными функциями с помощью операции сдвига и операции циклического сдвига координат векторов пространства V_n.

3) Исследована структура регулярных систем, построенных на основе аффинного регистра сдвига с нелинейной функцией усложнения второй степени нелинейности от трёх переменных.

Практическая значимость работы состоит в том, что предложенный в диссертации способ задания биективного отображения приводит к существенному снижению емкостной сложности реализации этого отображения на новой и перспективной элементной базе. Представленный в приложении к диссертации каталог всех регулярных геометрически эквивалентных систем функций от четырёх переменных позволяет при разработке систем защиты информации выбирать легко реализуемые в пороговой логике преобразования с заданными характеристиками нелинейности.

Апробация работы проведена на XXXI Международной конференции «Информационные технологии в науке, образовании, социологии и бизнесе»; V, VI и VII Всероссийских симпозиумах по прикладной и промышленной математике; совместных семинарах кафедр №711, №712 и №713 Института криптографии, связи и информатики (ИКСИ) Академии ФСБ России. Результаты диссертации включены в отчёт по теме №4 Академии криптографии Российской Федерации, использованы в одном из курсов вузовского потока ИКСИ.

Публикации. Основные результаты диссертации опубликованы в 8 работах, из них три статьи опубликованы в рецензируемых журналах, рекомендованных ВАК для опубликования результатов докторских диссертаций.

Структура и объём работы. Диссертация состоит из введения, трёх глав, каталога, заключения и списка литературы. Она изложена на 141 странице, включает 28 таблиц и 4 рисунка. Список литературы содержит 53 наименования.

СОДЕРЖАНИЕ РАБОТЫ

В первой главе диссертации введены понятия регулярной системы однотипных функций и функции, порождающей эту систему, определено понятие типа регулярной системы. Описаны классы регулярных систем функций, эквивалентных относительно просто реализуемых групп преобразований: группы сдвигов и группы, порождённой преобразованием циклического сдвига координат векторов. Получен ряд необходимых условий того, что данная двоичная функция порождает регулярную систему. Описаны регулярные системы функций, порождаемые двоичными функциями степени нелинейности 2 с помощью преобразований сдвига векторов. Исследованы свойства подстановок, координатные функции которых эквивалентны относительно преобразования циклического сдвига переменных.

Во второй главе диссертационной работы построены классы регулярных систем функций, эквивалентных относительно преобразования, реализуемого за один такт работы регулярного регистра сдвига с аффинной двоичной функцией обратной связи. Доказано, что подстановки, задаваемые этим классом систем, имеют вторую степень нелинейности. Найдены классы двоичных функций степени нелинейности 3, порождающие регулярные системы с помощью преобразования циклического сдвига переменных. Указан в явном виде способ построения системы координатных функций обратной подстановки.

В третьей главе предложен принцип каталогизации регулярных систем геометрически эквивалентных двоичных функций, основанный на перечислении представителей типов систем. С помощью этого принципа получено полное описание рассматриваемых регулярных систем двоичных функций от четырёх переменных, которое в виде каталога представлено в приложении. Среди всех классов геометрической эквивалентности сбалансированных

функций выделены классы, порождающие регулярные системы. Для каждого из этих классов построены порождаемые соответствующими функциями подстановки, для классификации которых использовано введённое автором отношение эквивалентности. Для каждой подстановки, приведённой в каталоге, указаны характеристики нелинейности.

Перейдём к краткому изложению основных результатов диссертационной работы.

Пусть V_n — пространство двоичных векторов длины n, множество всех двоичных функций от n переменных обозначим через $\mathcal{F}_n$, а множество всех отображений пространства V_n в пространство V_m через $\mathcal{F}_{n,m}$. Произвольное отображение $\Phi \in \mathcal{F}_{n,m}$ может быть задано упорядоченным набором или системой координатных функций $(f_1, \ldots, f_m)$, где $f_i \in \mathcal{F}_n$, $i \in \overline{1,m}$. При таком задании действие отображения

$$\Phi : \boldsymbol{x} \mapsto \boldsymbol{y}, \qquad \boldsymbol{x} = (x_1, \ldots, x_n) \in V_n, \quad \boldsymbol{y} = (y_1, \ldots, y_m) \in V_m,$$

определяется системой уравнений

$$\left\{ \; y_i \; = f_i(\boldsymbol{x}) \, , i \in \overline{1,m}. \right. \tag{1.1}$$

Одним из важных требований, предъявляемых к отображениям $\mathcal{F}_{n,m}$, является сбалансированность или уравновешенность. Напомним, что отображение $\Phi \in \mathcal{F}_{n,m}$ $(m \leq n)$ называется сбалансированным, если мощность полного прообраза любого вектора из V_m равна 2^{n-m}. В случае, когда длины входных и выходных векторов совпадают, то есть $m{=}n$, сбалансированное отображение $\Phi \in \mathcal{F}_{n,n}$ является биективным. Биективные отображения из $\mathcal{F}_{n,m}$ задают подстановки степени 2^n на множестве V_n. Множество всех подстановок на V_n будем обозначать $S(V_n)$.

Система координатных функций $(f_1, \ldots, f_n)$, $f_i \in \mathcal{F}_n$, $i \in \overline{1,n}$, биективного отображения называется регулярной системой. Систему координатных функций подстановки $\pi \in S(V_n)$ будем обозначать через $\mathcal{C}_\pi$.

Известные критерии регулярности преобразований пространства V_n, заданных двоичными координатными функциями, не дают достаточных условий для задания координатных функций регулярных систем в явном виде.

Всесторонне изучены такие классы регулярных преобразований пространства V_n как линейные и аффинные преобразования, регистровые пре-

образования, перестановочные многочлены полей характеристики, преобразования «треугольного» типа и другие. Известны также способы построения классов регулярных преобразований, задаваемых системами координатных функций ограниченной степени нелинейности.

В диссертации исследуется класс преобразований пространства V_n, координатные функции которых могут быть получены из одной и той же двоичной функции посредством преобразования её координат с помощью легко реализуемых сервисных команд. Для описания свойств этих отображений и их классификации удобнее рассматривать множества таких преобразований переменных, которые образуют некоторую группу G в группе $S(V_n)$. В этом случае координатные функции рассматриваемых отображений принадлежат одному и тому же классу эквивалентности относительно группы. Определим действие группы $G < S(V_n)$ на множестве $\mathcal{F}_n$ двоичных функций от n переменных формулой

$$f^{\alpha}(\boldsymbol{x}) = f\left(\boldsymbol{x}^{\alpha^{-1}}\right), \qquad f \in \mathcal{F}_n, \alpha \in G, \boldsymbol{x} \in V_n.$$

Функции f и h называются эквивалентными относительно группы G, или G-эквивалентными (G-однотипными), если существует элемент $\alpha \in G$, такой, что $h = f^{\alpha}$. В этом случае будем использовать обозначение $f \overset{G}{\sim} h$.

Отношение $\overset{G}{\sim}$ разбивает множество $\mathcal{F}_n$ на классы эквивалентных элементов, которые будем называть G-типами. G-тип, содержащий функцию f, будем обозначать $[f]_G$.

Определение 1.1. Система двоичных функций $(f_1, \ldots, f_n)$ от n переменных называется G-однотипной, если все функции этой системы принадлежат одному G-типу.

Система G-однотипных функций может быть задана в виде

$$(f, f^{\alpha_1}, \ldots, f^{\alpha_{n-1}}), \qquad \alpha_i \in G, i \in \overline{1, n-1}. \tag{1.2}$$

Будем говорить, что система (1.2) порождается функцией f с помощью подстановок $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$ из группы G, а саму функцию f будем называть порождающей.

Представляют интерес G-однотипные системы, обладающие свойством регулярности. Для реализации действия подстановки $\pi \in S(V_n)$ с помощью

системы G-однотипных координатных функций $\mathcal{C}_\pi$ достаточно реализовать одну порождающую функцию и $n-1$ сервисную команду, определяемую подстановку из группы G. Требование к снижению емкостной сложности реализации преобразования обуславливает необходимость уменьшения объёма памяти, используемой для реализации порождающей функции и соответствующих сервисных команд. В связи с этим в диссертации рассматриваются такие преобразования векторов из V_n, которые с одной стороны легко реализуются программными и аппаратными способами, а с другой — при действии на переменные порождающей функции сохраняют её характеристики нелинейности. В частности, к таким преобразованиям относятся аффинные преобразования пространства V_n.

Обозначим через $\boldsymbol{GF}(2)^*_{n,n}$ множество всех обратимых матриц порядка n над полем $\boldsymbol{GF}(2)$. Пусть $A \in \boldsymbol{GF}(2)^*_{n,n}$ и $\boldsymbol{b} \in V_n$. Действие подстановок ϕ_A и $\psi_{A,\boldsymbol{b}}$ из $S(V_n)$ определим формулами

$$\forall \boldsymbol{x} \in V_n : \qquad \boldsymbol{x}^{\phi_A} = \boldsymbol{x}A, \qquad \boldsymbol{x}^{\psi_{A,\boldsymbol{b}}} = \boldsymbol{x}A + \boldsymbol{b}.$$

Обозначим через

$$\begin{aligned} \boldsymbol{GL}(n,2) &= \left\{ \phi_A : A \in \boldsymbol{GF}(2)^*_{n,n} \right\} \text{ и} \\ \boldsymbol{AGL}(n,2) &= \left\{ \psi_{A,\boldsymbol{b}} : A \in \boldsymbol{GF}(2)^*_{n,n}, \boldsymbol{b} \in V_n \right\} \end{aligned}$$

полную линейную и полную аффинную группы размерности n над полем $\boldsymbol{GF}(2)$ соответственно.

В диссертации рассмотрены следующие подгруппы группы $\boldsymbol{AGL}(n,2)$.

Группа H_n сдвигов пространства V_n. Для $\eta_{\boldsymbol{a}} \in H_n$

$$\eta_{\boldsymbol{a}} : \boldsymbol{x} \mapsto \boldsymbol{x} + \boldsymbol{a}, \quad \boldsymbol{a} \in V_n.$$

Группа $\widehat{S}_n$ перестановок переменных. Для подстановки $\widehat{\tau} \in \widehat{S}_n$, соответствующей подстановке $\tau \in S_n = S(\overline{1,n})$,

$$\widehat{\tau} : \boldsymbol{x} = (x_1, \ldots, x_n) \mapsto \left(x_{\tau^{-1}(1)}, x_{\tau^{-1}(2)}, \ldots, x_{\tau^{-1}(n)} \right).$$

Группа Q_n — группа Джевонса или группа однотипных преобразований, $Q_n = \widehat{S}_n H_n$.

Группа $\langle\sigma\rangle$ — циклическая группа, порождённая преобразованием циклического сдвига координат вектора,
$\sigma^{-1} : \boldsymbol{x} = (x_1, \ldots, x_n) \mapsto (x_2, \ldots, x_n, x_1)$, $\boldsymbol{x} \in V_n$.

Группа $\langle\rho_l\rangle$ — циклическая группа, порождённая преобразованием, реализуемым за один такт работы регистром сдвига с аффинной функцией обратной связи,
$\rho_l^{-1} : \boldsymbol{x} = (x_1, \ldots, x_n) \mapsto (x_2, \ldots, x_n, l(\boldsymbol{x}))$,
$\boldsymbol{x} \in V_n$, $l(\boldsymbol{x}) = x_1 + \sum_{i=2}^{n} a_i x_i + a_0$, $\quad a_2, \ldots, a_n, a_0 \in \boldsymbol{GF}(2)$.

Без каких-либо ограничений на выбор группы G задача построения регулярных систем G-однотипных функций являлась бы тривиальной, поскольку любая подстановка на V_n задаётся регулярной системой $S(V_n)$-однотипных функций. Более того, согласно приведённому далее утверждению 1.1 любая подстановка $\pi \in S(V_n)$ может быть задана системой координатных функций вида $\left(f, f^{\alpha}, \ldots, f^{\alpha^{n-1}}\right)$, $\alpha \in S(V_n)$, которую будем обозначать через $\mathcal{C}(f; \alpha)$.

Утверждение 1.1. Для произвольной подстановки $\pi \in S(V_n)$ справедливо равенство

$$\mathcal{C}_{\pi} = \mathcal{C}\left(f; \pi\sigma\pi^{-1}\right),$$

где f — первая координатная функция подстановки π, $\sigma \in S(V_n)$ — подстановка циклического сдвига вектора вправо.

Пусть подстановка $\pi \in S(V_n)$ задаётся системой G-однотипных координатных функций $\mathcal{C}_{\pi}$. Для всех подстановок $\alpha, \beta \in S(V_n)$ система функций $\mathcal{C}_{\alpha\pi\beta}$ всегда будет регулярной, а вот свойство G-однотипности её координатных функций может быть нарушено, что подтверждается приведёнными в диссертации примерами систем функций от произвольного числа переменных.

Обозначим через $N_{S(V_n)}(M) = \{\alpha \in S(V_n) \mid \alpha M = M\alpha\}$ нормализатор множества $M \subset S(V_n)$ в группе $S(V_n)$.

Утверждение 1.2. Пусть $G < S(V_n)$ и подстановка $\pi \in S(V_n)$ задаётся системой G-однотипных координатных функций. Тогда для любых $\alpha \in N_{S(V_n)}(G)$ и $\beta \in \widehat{S}_n$ система координатных функций подстановки $\alpha\pi\beta$ является регулярной системой G-однотипных функций.

Следствие 1.1. Пусть $G < S(V_n)$ и подстановка $\pi \in S(V_n)$ задаётся системой $\mathcal{C}_\pi = (f_1, \ldots, f_n)$ G-однотипных координатных функций такой, что $\overline{f}_1 \in [f_1]_G$, где $\overline{f}_1 = f_1 + 1$. Тогда для любых $\alpha \in N_{S(V_n)}(G)$ и $\beta \in Q_n$ система координатных функций подстановки $\alpha\pi\beta$ является регулярной системой G-однотипных функций.

Следствие 1.2. Свойство функции $f \in \mathcal{F}_n$, состоящее в том, что она порождает регулярную систему G-однотипных функций, является инвариантом G-типа $[f]_G$.

Из следствия 1.2 вытекает корректность определений 1.2 и 1.3.

Определение 1.2. G-тип $[f]_G$ называется порождающим, если его представитель f порождает регулярную систему G-однотипных функций.

Определение 1.3. G-типом регулярной системы G-однотипных функций называется G-тип порождающей функции системы.

Утверждение 1.3. Пусть $G < S(V_n)$ и $f \in \mathcal{F}_n$. Если функция f порождает регулярную систему G-однотипных функций, являющуюся системой координатных функций некоторой подстановки $\pi \in S(V_n)$, то система координатных функций подстановки $\pi\theta$ порождается функцией $\overline{f}$, где θ — преобразование, осуществляющее инвертирование значений координат вектора, $\theta : \boldsymbol{x} \mapsto \boldsymbol{x} + \mathbf{1}$, для любого $\boldsymbol{x} \in V_n$.

В диссертации исследован способ построения регулярных систем с использованием преобразований сдвига векторов пространства V_n. Действие подстановки $\eta_{\boldsymbol{a}}$ из группы сдвигов H_n на вектор $\boldsymbol{x} \in V_n$ состоит в покоординатном сложении векторов $\boldsymbol{x}$ и $\boldsymbol{a}$. В случае, когда длины суммируемых векторов не превосходят разрядность процессора, операция покоординатного сложения двоичных векторов может быть выполнена за один такт его работы. Поэтому реализация подстановки, координатные функции которой образуют регулярную систему H_n-однотипных функций, состоит в реализации одной двоичной функции от n переменных и $n-1$ операции покоординатного сложения в V_n.

На основе результатов аффинной классификации квадратичных форм над полем $\boldsymbol{GF}(2)$, в диссертации описаны все регулярные системы H_n-однотипных функций, порождаемые функцией степени нелинейности 2.

Утверждение 1.4. Функция $f \in \mathcal{F}_n$ второй степени нелинейности порождает регулярную систему H_n-однотипных функций в том и только том случае, когда выполнены следующие два условия:

1) n — нечётно;

2) f аффинно эквивалентна функции
$x_1x_2 + x_3x_4 + \ldots + x_{n-2}x_{n-1} + x_n$.

Одним из основных результатов диссертации является теорема 1.1, в которой описаны все регулярные системы H_n-однотипных функций второй степени нелинейности.

Теорема 1.1. Квадратичная форма над полем $\boldsymbol{GF}(2)$

$$f(\boldsymbol{x}) = x_1x_2 + x_3x_4 + \ldots + x_{n-2}x_{n-1} + x_n$$

порождает регулярную систему H_n-однотипных функций

$$\left(f, f^{\eta_{\boldsymbol{a}_1}}, \ldots, f^{\eta_{\boldsymbol{a}_{n-1}}}\right), \qquad \eta_{\boldsymbol{a}_i} \in H_n, i \in \overline{1, n-1},$$

в том и только том случае, когда n нечётно и векторы

$$\left(0, \ldots, 0, 1\right), \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{n-1}$$

линейно независимы.

Задав на множестве всех элементов группы сдвигов отношение частичного порядка, отвечающее лексикографическому порядку векторов из V_n, и используя формулы для вычисления мощности класса аффинно эквивалентных функций, в диссертации найдено количество H_n-однотипных регулярных систем.

Следствие 1.3. Пусть $n \geqslant 3$ — нечётно, $f(\boldsymbol{x}) = x_1x_2 + \ldots + x_{n-2}x_{n-1} + x_n$. Тогда имеет место равенство

$$\left|[f]_{\boldsymbol{AGL}(n,2)}\right| = \frac{2 \cdot \prod_{i=0}^{n-1}\left(2^n - 2^i\right)}{2^{\left(\frac{n-1}{2}\right)^2} \cdot (2^2-1) \cdot (2^4-1) \cdot \ldots \cdot (2^{n-1}-1)}$$

и существует

$$\left(2^n - 2\right)\left(2^n - 2^2\right) \cdot \ldots \cdot \left(2^n - 2^{n-1}\right)$$

регулярных систем вида $\left(f, f^{\eta_1}, \ldots, f^{\eta_{n-1}}\right)$ H_n-однотипных функций, у которых порождающие преобразования упорядочены в соответствии с отношением частичного порядка.

Таким образом, в случае, когда n — нечётное число, в работе описаны все регулярные системы H_n-однотипных функций, порождаемые двоичной функцией второй степени нелинейности. Непосредственной проверкой с помощью вычислительной техники автором диссертации установлено, что описанными выше системами исчерпываются все регулярные системы H_3- и H_5-однотипных функций, а регулярных систем H_4-однотипных функций не существует. В то же время показано, что существуют функции, порождающие регулярные системы H_n-однотипных функций, степень нелинейности которых больше 2. Для построения такого примера была использована известная аффинная классификация кубических форм от шести переменных.

Далее в диссертации изучено строение регулярных систем, задаваемых с помощью преобразований, реализуемых перестановкой переменных порождающей функции. Техническая реализация таких преобразований состоит в изменении порядка считывания содержимого ячеек памяти, в которых записаны значения координат входного вектора $\boldsymbol{x}$, а программная — в умножении вектора $\boldsymbol{x}$ на подстановочную матрицу, соответствующую подстановке τ. Использование только одного преобразования перестановки переменных порождающей функции позволяет сократить емкостную сложность реализации регулярной системы. В диссертации обоснован выбор в качестве преобразования, используемого для порождения регулярной системы, преобразования циклического сдвига переменных. Пусть далее $\sigma \in \widehat{S}_n$ — такая подстановка, что

$$\sigma^{-1} : \boldsymbol{x} = (x_1, \ldots, x_n) \mapsto (x_2, \ldots, x_n, x_1)\,, \boldsymbol{x} \in V_n.$$

Используя алгоритм построения всех порождающих функций систем вида $\mathcal{C}(f;\sigma)$, аннонсированный Рожковым М. В., в диссертации описано множество всех подстановок, задаваемых рассматриваемыми системами.

Утверждение 1.5. Множество подстановок, системы координатных функций которых имеют вид $\mathcal{C}(f;\sigma)$, образует группу, являющуюся централизатором подстановки σ в группе $S(V_n)$.

Алгоритм построения всех регулярных систем вида $\mathcal{C}(f;\sigma)$ позволяет задать порождающую функцию f только вектором её значений. Такое задание функции при больших значениях n не приемлемо в виду значительных емкостных затрат. Поэтому практическую значимость представляет описание

классов порождающих функций, допускающих простую реализацию, а также способов построения новых функций на основе комбинации известных.

Пусть $\omega \in S(V_n)$ — подстановка такая, что

$$\omega : \boldsymbol{x} = (x_1, \ldots, x_n) \mapsto (x_n, x_{n-1}, \ldots, x_1), \quad \boldsymbol{x} \in V_n.$$

Поскольку множество подстановок, координатные функции которых $\langle\sigma\rangle$-эквивалентны, образуют группу, для каждой подстановки $\pi \in S(V_n)$ такой, что $\mathcal{C}_\pi = \mathcal{C}(f;\sigma)$, $f \in \mathcal{F}_n$, система координатных функций подстановки π^{-1} есть $\mathcal{C}(h;\sigma)$ для некоторой функции $h \in \mathcal{F}_n$.

Утверждение 1.6. Пусть $\pi \in S(V_n)$ такая подстановка, что системой её координатных функций $\mathcal{C}_\pi$ является система функций $\mathcal{C}(f;\sigma)$, а системой координатных функций обратной подстановки π^{-1} — система $\mathcal{C}(h;\sigma)$, для некоторых функций $f, h \in \mathcal{F}_n$ соответственно. Тогда для произвольного $l \in \mathbb{Z}$ системы $\mathcal{C}\left(f^{\sigma^l\omega};\sigma\right)$ и $\mathcal{C}\left(h^{\sigma^{-(l+2)}\omega};\sigma\right)$ регулярны и подстановки, задаваемые этими системами координатных функций взаимно обратны.

Через $C_t(\boldsymbol{a})$ обозначим правый t-циркулянт с порождающим вектором $\boldsymbol{a} \in V_n$, то есть квадратную $n \times n$-матрицу над полем $\boldsymbol{GF}(2)$, первая строка которой является вектором $\boldsymbol{a}$, а остальные строки отличаются от предыдущей строки циклическим сдвигом на t позиций вправо. Далее речь пойдёт только о правых t-циркулянтах, поэтому правые t-циркулянты будем называть просто t-циркулянтами. Поскольку группа $\boldsymbol{GF}(2)^*_{n,n}$ обратимых матриц над полем $\boldsymbol{GF}(2)$ изоморфна полной линейной группы $\boldsymbol{GL}(n,2)$, подстановку $\alpha = \phi_A \in \boldsymbol{GL}(n,2)$, соответствующую обратимому t-циркулянту $A \in \boldsymbol{GF}(2)^*_{n,n}$, будем также называть t-циркулянтом. Отметим, что в этом случае t и n взаимно простые числа.

Утверждение 1.7. Пусть $\alpha \in \boldsymbol{GL}(n,2)$ — обратимый t-циркулянт. Если функция $f \in \mathcal{F}_n$ порождает регулярную систему $\mathcal{C}(f;\sigma)$, то функция f^α также порождает регулярную систему $\mathcal{C}(f^\alpha;\sigma)$.

Если при этом $\mathcal{C}(f;\sigma)$=$\mathcal{C}_\pi$, $\pi \in S(V_n)$, то

$$\mathcal{C}(f^\alpha;\sigma) = \mathcal{C}_{\alpha^{-1}\pi\beta}, \text{ где } \beta = \phi_{C_1(1,0,\ldots,0)}.$$

Утверждение 1.8. Пусть $A = C_t(\boldsymbol{a}) \in \boldsymbol{GF}(2)^*_{n,n}$ для вектора $\boldsymbol{a} \in V_n$ веса k

$$\boldsymbol{a} = (0, \ldots, 0, \underbrace{1}_{i_1}, 0, \ldots, 0, \underbrace{1}_{i_k}, 0, \ldots, 0),$$

$0 \leqslant i_1 < \ldots < i_k \leqslant n-1$, $i_1, \ldots, i_k \in \mathbb{N}_0$; $\alpha = \phi_{A^T}$, а подстановка $\pi \in S(V_n)$, такая, что $\mathcal{C}_\pi = \mathcal{C}(f;\sigma)$ для некоторой функции $f \in \mathcal{F}_n$. Тогда система координатных функций подстановки $\pi\alpha$ имеет вид:

$$\mathcal{C}_{\pi\alpha} = \mathcal{C}\left(f^{\sigma^{i_1}} + \ldots + f^{\sigma^{i_k}}; \sigma\right).$$

Утверждения 1.7 и 1.8 показывают, что для любой подстановки $\pi \in S(V_n)$, заданной системой координатных функций $\mathcal{C}(f;\sigma)$, и произвольных t- и r-циркулянтов α и β соответственно, подстановка $\alpha\pi\beta$ задаётся системой координатных функций $\mathcal{C}(g;\sigma)$ для некоторой функции $g \in \mathcal{F}_n$. Способ нахождения функции g по известным f, α и β вытекает из этих утверждений.

В первой главе диссертационной работы показано, что в целях минимизации емкостной сложности реализации регулярной системы G-однотипных функций $(f, f^{\alpha_1}, \ldots, f^{\alpha_{n-1}})$, $\alpha_i \in G < S(V_n)$, $i \in \overline{1, n-1}$, подстановки α_i должны быть технически просто реализуемы. Более того, даже в случае, когда $\alpha_i = \alpha^i$, $i \in \overline{1, n-1}$, для некоторого $\alpha \in S(V_n)$, вопрос выбора простой реализации подстановки α остаётся актуальным. В связи с этим во второй главе описываются классы регулярных систем вида $\mathcal{C}(f;\rho_l)$, при построении которых используется преобразование ρ_l^{-1}, реализуемое за один такт работы линейного регистра сдвига длины n с аффинной функцией обратной связи $l(\boldsymbol{x}) = a_0 + x_1 + \sum\limits_{i=1}^{n-1} a_i x_i$, $\boldsymbol{x} = (x_1, \ldots, x_n) \in V_n$, $a_i \in \boldsymbol{GF}(2)$, $i \in \overline{1, n-1}$.

В отечественной и зарубежной литературе исследованы свойства фильтрующих генераторов с аффинной функцией обратной связи и нелинейной двоичной функцией выхода f. В двоичном случае фильтрующий генератор позволяет из начального состояния $\boldsymbol{x} \in V_n$ выработать двоичную последовательность $\gamma_1, \gamma_2, \ldots$, знак с номером i, $i \in \mathbb{N}$, которой равен

$$\gamma_i = f^{\rho_l^{i-1}}(\boldsymbol{x}).$$

За n тактов работы фильтрующий генератор реализует преобразование

$$(x_1, \ldots, x_n) \mapsto (\gamma_1, \ldots, \gamma_n), \qquad (x_1, \ldots, x_n), (\gamma_1, \ldots, \gamma_n) \in V_n,$$

задаваемое системой координатных функций $\left(f, f^{\rho_l}, \ldots, f^{\rho_l^{n-1}}\right)$. Во введённых обозначениях эта система обозначается $\mathcal{C}(f;\rho_l)$. Система $\mathcal{C}(f;\rho_l)$ является $\langle\rho_l\rangle$-однотипной, где $\langle\rho_l\rangle$ — циклическая группа, порождённая подстановкой ρ_l. Регулярность системы функций $\mathcal{C}(f;\rho_l)$ эквивалентна условию единственности решения системы нелинейных уравнений рекуррентного типа

$$\left\{ f^{\rho_l^i}(\boldsymbol{x}) = \gamma_{i+1}, \qquad i \in \overline{0, n-1}, \right. \tag{2.3}$$

для всех векторов $(\gamma_1, \gamma_2, \ldots, \gamma_n) \in V_n$.

В общем случае задача решения систем нелинейных, в том числе и квадратичных уравнений, относится к классу NP-сложных задач. В рассматриваемом случае необходимо исследовать 2^n систем уравнений с различными правыми частями. При решении поставленного вопроса во второй главе диссертации получено описание класса функций второй степени нелинейности, порождающих регулярные системы вида $\mathcal{C}(f;\rho_l)$, и вычислены степени нелинейности подстановок, задаваемых этими системами.

Теорема 2.1. Пусть $n \geq 3$, n — нечётно, $f, l \in \mathcal{F}_n$. Тогда в каждом из следующих четырёх случаев:

1) $f = x_2 + x_3 + x_1x_2 + a$ и $l = x_1 + bx_{n-1}$,

2) $f = x_1 + x_3 + x_1x_2 + a$ и $l = x_1 + bx_{n-1} + b$,

3) $f = x_1 + x_2 + x_2x_3 + a$ и $l = x_1 + bx_3$,

4) $f = x_1 + x_3 + x_2x_3 + a$ и $l = x_1 + bx_3 + b$,

где $a, b \in \boldsymbol{GF}(2)$, система функций $\mathcal{C}(f;\rho_l)$ регулярна и является системой координатных функций подстановки $\pi \in S(V_n)$ с характеристиками

$$\lambda_\pi = 2 \text{ и } \lambda_{\pi^{-1}} = \frac{n+1}{2}.$$

При доказательстве теоремы 2.1 в явном виде получено решение соответствующей системы нелинейных уравнений и указаны алгебраические связи между подстановками, порождаемыми представленными в теореме функциями.

Преобразование циклического сдвига вектора является частным случаем преобразований, реализуемых аффинным регистром сдвига. Доказательство регулярности соответствующих систем функций также основывается на

нахождении решения системы нелинейных уравнений. При этом используется свойство преобразований задаваемых системами вида $\mathcal{C}(f;\sigma)$, состоящее в задании обратного преобразования системой функций такого же вида. Это свойство и лемма 2.1 позволяют доказать теорему 2.2, для удобства формулировки которой нумерация координат векторов из V_n начинается с 0.

Лемма 2.1. Пусть $f \in \mathcal{F}_n$. Если для некоторой функции $h \in \mathcal{F}_n$ суперпозиция функций $h\left(f, f^\sigma, \ldots, f^{\sigma^{n-1}}\right)$ тождественно равна функции x_0, то системы функций $\mathcal{C}(f;\sigma)$ и $\mathcal{C}(h;\sigma)$ являются регулярными, и подстановки $\alpha, \beta \in S(V_n)$, задаваемые этими системами, являются взаимно обратными, то есть $\alpha = \beta^{-1}$.

Теорема 2.2. Пусть $f \in \mathcal{F}_n$. Система $\mathcal{C}(f;\sigma)$ регулярна в каждом из следующих случаев:

1) $n \geqslant 5$, $f = x_1 + x_0\overline{x}_2x_3$ или $f = x_2 + x_0\overline{x}_1x_3$;

2) $n \geqslant 5$, n — нечётное, $f = x_1 + x_0x_2\overline{x}_3$ или $f = x_2 + \overline{x}_0x_1x_3$;

3) $n \geqslant 5$, n не делится на 3,

   (a) $f = x_0 + x_1x_2\overline{x}_3$ или $f = x_3 + \overline{x}_0x_1x_2$,

   (b) $f = x_0 + \overline{x}_1x_2x_3$ или $f = x_3 + x_0x_1\overline{x}_2$.

Каждая из указанных функций порождает регулярную систему с помощью циклического сдвига координат только для представленных значений n.

При доказательстве регулярности систем функций, порождаемых функциями, представленными в теореме 2.2, были получены в явном виде порождающие функции систем, задающих обратные преобразования.

Новые классы функций третьей степени нелинейности, порождающих регулярные системы $\langle\sigma\rangle$-однотипных функций, могут быть построены с использованием утверждений, доказанных в первой главе диссертации.

Прикладной задачей исследования регулярных систем G-однотипных функций является описание всех таких систем для фиксированной группы G преобразований пространства V_n. В третьей главе диссертации эта задача решается для систем Q_n-однотипных функций, $n = 4$. Выбор в качестве группы преобразований группы Джевонса Q_n обусловлен тем, что эта группа является максимальной среди всех групп преобразований пространства V_n, которые

не нарушают геометрического строения двоичной функции. Q_n-однотипные двоичные функции представляют собой одну и ту же логическую форму, записанную в разных системах координат, поэтому значительная часть свойств этих функций либо остаётся неизменной внутри типа, либо меняется несущественно.

В соответствии с общими принципами классификации отображений на множестве подстановок, задаваемых регулярными системами Q_n-однотипных функций, вводится следующее отношение эквивалентности. Две подстановки $\pi_1, \pi_2 \in S(V_n)$ называются эквиалентными, если существуют такие подстановки $\alpha \in N_{\boldsymbol{AGL}(n,2)}(Q_n)$, $\beta \in Q_n$, что $\pi_1 = \alpha\pi_2\beta$. Из утверждения 1.2 и следствия 1.1 следует, что разбиение на классы эквивалентности относительно введённого отношения эквивалентности не нарушает свойства геометрической эквивалентности координатных функций систем, задающих эквивалентные подстановки. Из утверждения 3.1, следует, что в случае чётного n в качестве нормализатора $N_{\boldsymbol{AGL}(n,2)}(Q_n)$ группы Джевонса Q_n в полной аффинной группе $\boldsymbol{AGL}(n,2)$ может быть выбрано произведение группы Q_n на линейную подстановку ϕ_A.

Утверждение 3.1. Для любого чётного $n \in \mathbb{N}$ группа Джевонса Q_n является нормальным делителем в группе Q_n^*, равной $Q_n\phi_A$, где $A = I + J$, I — единичная $n \times n$-матрица, J — $n \times n$-матрица, все элементы которой равны 1.

Введённое отношение эквивалентности позволило при составлении «Каталога регулярных систем Q_4-однотипных двоичных функций» использовать «Классификацию минимальных базисных представлений всех булевых функций от четырёх переменных», составленную В. Г. Никоновым. «Каталог...» составлен с использованием разработанного автором лично программного обеспечения в среде СУБД Paradox. Для вычислений характеристик функций и порождаемых ими систем использовалось разработанное автором программное обеспечение. Достоверность проведённых вычислений подтверждается непосредственным сравнением результатов вычислений, полученных с помощью пакетов прикладных программ, разработанных другими исследователями, а также апробацией в учебном процессе ИКСИ. Вёрстка «Каталога...» осуществлялась в издательской системе LaTeX, что обеспечивает совместимость отображения результатов каталогизации в системах, поддерживающих

форматированный вывод данных. В «Каталоге...» использован принцип классификации двоичных функций с помощью графов связности вершин, что значительно облегчает работу с каталогом и позволяет устанавливать корреляционные связи с классификационными исследованиями, проводимыми В. Г. Никоновым, В. А. Носовым и С. А. Гизуновым.

Дополнением к оглавлению «Каталога...» служит «Таблица представителей классов геометрической эквивалентности», представленная в диссертации. В этой таблице содержатся записи, однозначно соответствующие каждому из 58 типов сбалансированных функций. Каждая запись имеет следующий формат:

Тип	Мин. тип	ReG	стр.
$8.b.c.d$	$\to 8.b'.c'.d'$	r	s

В таком формате отражены:

1) $8.b.c.d$ — номер типа по каталогу «...минимальных базисных представлений всех булевых функций от четырёх переменных»;

2) $8.b'.c'.d'$ — номер типа, который принадлежит тому же классу, что и тип с номером $8.b.c.d$. Если данное поле не пусто, то в каталоге приводятся регулярные системы, порождаемые типом с номером $8.b'.c'.d'$. В противном случае в каталоге представлен тип с номером $8.b.c.d$.

3) r — количество представителей классов эквивалентности регулярных систем, порождаемых типом;

4) s — номер страницы, на которой представлена содержательная часть каталога, соответствующая рассматриваемому типу.

В содержательной части каталога результаты классификационных исследований для каждого из класса эквивалентности сбалансированных двоичных функций представлены в следующей последовательности. Сначала указывается заголовок:

Класс №t [8.b.c.d$\leftarrow 8.b'.c'.d' : B, \boldsymbol{b}$]

в котором отражены:

1) t — номер класса эквивалентности;

2) $B, \boldsymbol{b}$ — обратимая 4×4-матрица $B\in\boldsymbol{GF}(2)^*_{4\times4}$ и вектор $\boldsymbol{b}\in V_4$ такие, что функции f и f', являющиеся представителями типов Q_4-эквивалентности с номерами $8.b.c.d$ и $8.b'.c'.d'$ соответственно, связаны соотношением $f(\boldsymbol{x}) = f'\left(\boldsymbol{x}^{\psi_{B,\boldsymbol{b}}}\right)$, $\boldsymbol{x}\in V_4$, $\psi_{B,\boldsymbol{b}}\in Q_4^*$.

Далее для каждого из типов, входящих в класс эквивалентности представлена следующая информация о представителе типа:

- номер типа;
- вектор значений;
- кратчайшая дизъюнктивная нормальная форма;
- многочлен Жегалкина.

Информация о типе представляется в формате:

8.b.c.d

$\overrightarrow{f} =$

КДНФ:

$f(x) =$

Затем указывается номер типа, представитель которого исследовался, и данные соответствующие каждому из типов, входящих в рассматриваемый класс:

- мощность типа геометрической эквивалентности;
- количество представителей регулярных систем, порождаемых представителем типа;
- общее количество регулярных систем, порождаемых представителем типа.

Далее в виде таблиц перечисляются все r представителей регулярных систем, порождённых представителем типа.

$\ldots$ | i | $N(\alpha_1)$ | $N(\alpha_2)$ | $N(\alpha_3)$ | χ | z | $\ldots$

Записи, соответствующие каждому из представителей систем, отражают следующие данные.

1) i — порядковый номер системы;

2) $N(\alpha_1)$, $N(\alpha_2)$, $N(\alpha_3)$ — номера элементов α_1, α_2, α_3 группы Q_4, которые вместе с функцией f порождают регулярную систему двоичных функций $(f(\boldsymbol{x}), f(\boldsymbol{x}^{\alpha_1}), f(\boldsymbol{x}^{\alpha_2}), f(\boldsymbol{x}^{\alpha_3}))$. Для получения подстановки $\alpha = \widehat{\tau}\eta_{\boldsymbol{a}} \in Q_4$, $\widehat{\tau} \in \widehat{S}_4$, $\eta_{\boldsymbol{a}} \in H_4$, по её номеру $N(\alpha)$ необходимо найти строку и столбец «Таблицы номеров элементов группы Q_4», представленной в диссертации, на пересечении которых находится искомое число $N(\alpha)$. Строка таблицы определяет подстановку $\tau \in S_4$, а столбец — вектор $\boldsymbol{a} \in V_4$.

3) χ — константа, по значению которой из таблицы «Мощности классов эквивалентных систем», представленной в диссертации, устанавливается мощность класса эквивалентности регулярной системы функций $(f(\boldsymbol{x}), f(\boldsymbol{x}^{\alpha_1}), f(\boldsymbol{x}^{\alpha_2}), f(\boldsymbol{x}^{\alpha_3}))$, а также общее количество классов эквивалентности такой мощности, представленных в классификации.

4) z — константа, по значению которой из таблицы «Характеристики нелинейности систем-представителей», представленной в диссертации, устанавливаются значения разностной характеристики μl, порядка нелинейности μt и степени нелинейности λ. Характеристики нелинейности μl, μt и λ вычисляются по формулам

$$\mu l_\pi = \max_{\boldsymbol{a} \in V_n \setminus \{\boldsymbol{0}\}, \boldsymbol{b} \in V_n} \left| \{\boldsymbol{x} \in V_n : (\boldsymbol{x} + \boldsymbol{a})^\pi + \boldsymbol{x}^\pi = \boldsymbol{b}\} \right|,$$

$$\mu t_\pi = \max_{\boldsymbol{a} \in V_n, \boldsymbol{b} \in V_n \setminus \{\boldsymbol{0}\}} \left| \left| \{\boldsymbol{x} \in V_n : \langle \boldsymbol{a}, \boldsymbol{x} \rangle + \langle \boldsymbol{b}, \boldsymbol{x}^\pi \rangle\} \right| - 2^{n-1} \right|,$$

где $\langle \boldsymbol{a}, \boldsymbol{b} \rangle = \sum\limits_{i=1}^{n} a_i b_i$ — скалярное произведение векторов $\boldsymbol{a} = (a_1, \ldots, a_n)$, $\boldsymbol{b} = (b_1, \ldots, b_n)$ из V_n,

$$\lambda_\pi = \min_{\boldsymbol{a} = (a_1, \ldots, a_n) \in V_n \setminus \{\boldsymbol{0}\}} \deg \left(\sum_{i=1}^{n} a_i f_i \right).$$

Суммарные результаты проведённой каталогизации позволяют сделать вывод в том что, среди 402 классов геометрически эквивалентных двоичных функций содержится 58 классов сбалансированных функций, которые относительно введённого в диссертации отношения эквивалентности образуют 37 классов Q_4^*-эквивалентности. Из этих 37 классов 24 класса порождают регулярные системы Q_4-однотипных функций. Возможные значения характеристик нелинейности систем-представителей представлены в таблице 3.1. Следует отметить, что среди построенных классов систем содержатся классы, обладающие оптимальными или близкими к ним характеристиками нелинейности.

λ	μt	μl	N
3	4	2	8
3	4	4	27
2	4	2	350
2	4	4	274
2	4	6	1
3	4	6	1
3	6	2	9

λ	μt	μl	N
3	6	4	131
3	6	6	48
3	6	8	2
2	6	2	167
2	6	4	1952
2	6	6	384
2	6	8	32

λ	μt	μl	N
2	6	12	8
2	6	16	4
1	8	4	542
1	8	6	298
1	8	8	395
1	8	10	33
1	8	16	37

Таблица 3.1. Характеристики нелинейности систем-представителей (N — количество представителей с заданными характеристиками нелинейности)

Для обращения в «Каталог...» и использования результатов классификационных исследований для произвольной сбалансированной функции $g \in \mathcal{F}_4$ необходимо выполнить следующую последовательность действий.

1) Определяем класс $[f]_{Q_4^*}$, $f \in \mathcal{F}_4$, Q_4^*-эквивалентности, в который входит функция g. При этом определяем подстановку $\alpha \in Q_4$, для которой $f(\boldsymbol{x}) = g(\boldsymbol{x}^\alpha)$, $\boldsymbol{x} \in V_4$, если $[f]_{Q_4^*} = [f]_{Q_4}$. Если же $[f]_{Q_4^*} = [f]_{Q_4} \bigcup [f']_{Q_4}$, $f' \in \mathcal{F}_4$, то есть класс Q_4^*-эквивалентности состоит из двух типов Q_4-эквивалентности с представителями f и f', то определяем подстановку $\alpha \in Q_4$, для которой $f(\boldsymbol{x}) = g(\boldsymbol{x}^\alpha)$ или $f'(\boldsymbol{x}) = g(\boldsymbol{x}^\alpha)$, $\boldsymbol{x} \in V_4$. Если данный класс Q_4^*-эквивалентности, а значит и рассматриваемая функция g, порождает регулярные системы Q_4-однотипных функций, то можно пе-

реходить к построению системы регулярных функций с требуемыми характеристиками.

2) По таблицам представителей типа, анализируя значения расмотренной выше константы z, выбираем систему функций, обладающую заданными характеристиками, и указываем подстановки $\alpha_i = \widehat{\tau}_i \eta_{\boldsymbol{b}_i} \in Q_4$, $\widehat{\tau}_i \in \widehat{S}_4$, $\eta_{\boldsymbol{a}_i} \in H_4$, $i \in \overline{1,3}$, для которых система функций

$$\left(f(\boldsymbol{x}), f(\boldsymbol{x}^{\alpha_1}), f(\boldsymbol{x}^{\alpha_2}), f(\boldsymbol{x}^{\alpha_3})\right)$$

регулярна и является системой координатных функций некоторой подстановки $\pi \in S(V_4)$. Если $[f]_{Q_4^*} = [f]_{Q_4} \bigcup [f']_{Q_4}$, $f' \in \mathcal{F}_4$, и $f'(\boldsymbol{x}) = g(\boldsymbol{x}^{\alpha})$, где α — найденная на предыдущем этапе подстановка из Q_4, то, определив по каталогу подстановку $\psi \in Q_4^*$, для которой $f(\boldsymbol{x}) = f'\left(\boldsymbol{x}^{\psi}\right)$, указываем подстановки $\beta_i = (\psi\alpha)^{-1} \alpha_i (\psi\alpha) = \widehat{\kappa}_i \eta_{\boldsymbol{b}_i} \in Q_4$, $\widehat{\kappa}_i \in \widehat{S}_4$, $\eta_{\boldsymbol{b}_i} \in H_4$, $i \in \overline{1,3}$, для которых система функций $\left(g(\boldsymbol{x}), g\left(\boldsymbol{x}^{\beta_1}\right), g\left(\boldsymbol{x}^{\beta_2}\right), g\left(\boldsymbol{x}^{\beta_3}\right)\right)$ регулярна и является системой координатных функций подстановки $\pi^* = (\psi\alpha)^{-1} \pi \in S(V_4)$.

Если же на предыдущем этапе установлено, что $[f]_{Q_4^*} = [f]_{Q_4}$ и $f(\boldsymbol{x}) = g(\boldsymbol{x}^{\alpha})$, то искомые подстановки $\beta_i \in Q_4, i \in \overline{1,3}$, равны $\alpha^{-1}\alpha_i\alpha$, $i \in \overline{1,3}$, соответственно.

В диссертации получены следующие основные **результаты, выносимые на защиту**.

1) Для синтеза взаимно однозначного отображения двоичных векторов длины n в диссертации предложено использовать не n координатных функций, а одну функцию с совокупностью легко реализуемых сервисных команд.

2) Для предложенного способа построения подстановок проведено исследование аналитических свойств систем функций и порождаемых ими преобразований в системах защиты информации.

3) Предложен метод каталогизации всех двоичных функций и составлен каталог регулярных систем, порождаемых функциями от четырёх переменных.

Публикации автора по теме диссертации

1. *Никонов В. Г., Саранцев А. В.* Методы компактной реализации биективных отображений, заданных регулярными системами однотипных булевых функций // *Вестник Российского университета дружбы народов Сер. Прикладная и компьютерная математика.* — 2003. — Т. 2, № 1. — С. 94–105.

2. *Никонов В. Г., Саранцев А. В.* Построение и классификация регулярных систем однотипных функций // Материалы XXXI Международной конференции «Информационные технологии в науке, образовании, телекоммуникации и бизнесе». — Т. 5 из *Прил. 1.* — М.: «Академия естествознания», 2004. — С. 173–174.

3. *Саранцев А. В.* Биективные отображения, заданные регулярными системами однотипных двоичных функций // Обозрение прикладной и промышленной математики. — Т. 11 из *Вып. 3.* — М.: Редакция журнала «ОПиПМ», 2004. — С. 583–584.

4. *Саранцев А. В.* Построение регулярных систем нелинейных двоичных функций на базе аффинного регистра сдвига // Материалы XXXI Международной конференции «Информационные технологии в науке, образовании, телекоммуникации и бизнесе». — Т. 5 из *Прил. 1.* — М.: «Академия естествознания», 2004. — С. 176–177.

5. *Саранцев А. В.* Построение регулярных систем однотипных двоичных функций с использованием регистра сдвига // *Вестник МГУЛ "Лесной вестник".* — 2004. — № 1(32). — С. 164–169.

6. *Саранцев А. В.* Классификация регулярных систем однотипных функций, построенных с помощью циклического сдвига // Обозрение прикладной и промышленной математики. — Т. 12 из *Вып. 1.* — М.: Редакция журнала «ОПиПМ», 2005. — С. 182–184.

7. *Саранцев А. В.* Подходы к классификации регулярных систем однотипных двоичных функций, построенных с помощью циклического сдвига // *Вестник МГУЛ "Лесной вестник"*. — 2005. — № 6(42). — С. 176–180.

8. *Саранцев А. В.* Регулярные системы однотипных двоичных функций степени 3, построенные с помощью циклического сдвига // Обозрение прикладной и промышленной математики. — Т. 14 из *Вып. 1.* — М.: Редакция журнала «ОПиПМ», 2007. — С. 147–148.

Подписано в печать 18.03.2010
Формат 60×84 1/16. Бумага офсетная.
Печать офсетная. Усл. печ. л. 1,5.
Тираж 100 экз. Заказ №484.
Типография «Реглет»
119526, г. Москва, пр-т Вернадского, 39
(495)363-78-90, www.reglet.ru