На правах рукописи

Фомичев Николай Владимирович

ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ СВОЙСТВ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ С ПОМОЩЬЮ МАТЕМАТИЧЕСКОЙ МОДЕЛИ ПРИЗНАКОВ В КОНЕЧНЫХ ПОЛУГРУППАХ И ГРУППАХ ПРЕОБРАЗОВАНИЙ

Специальность: 05.13.19 — методы и системы защиты информации, информационная безопасность (физико-математические науки)

АВТОРЕФЕРАТ
диссертации на соискание учёной степени
кандидата физико-математических наук

Автор: _____

Москва – 2008

Работа выполнена в ГОУВПО Московском инженерно-физическом институте (государственном университете)

Научный руководитель: доктор физ.-мат. наук, доцент
Фомичев Владимир Михайлович

Официальные оппоненты: доктор физ.-мат. наук, доцент
Физули Камилович Алиев,
в/ч 45807-Т

кандидат физ.-мат. наук, с.н.с.
Солодовников Владимир Игоревич,
в/ч 71330

Ведущая организация:
Институт проблем
информационной безопасности
МГУ им. М. В. Ломоносова

Защита состоится "____"_____ 2008 г. в _____часов
на заседании диссертационного совета ДМ 212.130.08 в ЦИТиС по адресу:
123557, г. Москва, Пресненский Вал, 19.

С диссертацией можно ознакомиться в библиотеке ГОУВПО Московского инженерно-физического института (государственного университета).

Отзывы в двух экземплярах, заверенные печатью, просьба направлять по адресу: 115409, Москва, Каширское ш., 31, диссертационные советы МИФИ (тел. 323-95-26).

Автореферат разослан "____"_____ 2008 года.

Учёный секретарь
диссертационного совета к.т.н., доцент Горбатов В.С.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Одной из приоритетных задач в международном сообществе является обеспечение информационной безопасности. Развивается сотрудничество между государствами в данной области. В Российской Федерации особое внимание уделяется вопросам защиты государственной тайны и конфиденциальной информации. В функционировании, как коммерческих организаций, так и государственных предприятий первостепенную роль играет обеспечение мер, необходимых для защиты информации, представляющей научно-техническую, технологическую, производственную и финансово-экономическую ценность. В последнее время проблемы информационной безопасности приобрели особую значимость в связи с необходимостью усиления борьбы с проявлениями терроризма, приобретающего международные масштабы.

Основополагающим документом, регламентирующим политику России в области информационной безопасности, является Доктрина информационной безопасности Российской Федерации, утверждённая в сентябре 2000 года Президентом Российской Федерации. Секция Научного совета при Совете Безопасности Российской Федерации на основе Доктрины разработала Перечень приоритетных научных проблем в области информационной безопасности, включающий ряд междисциплинарных проблем. Решение этих проблем требует совместных усилий различных специалистов: математиков, физиков, специалистов по информационным технологиям, юристов, социологов, экономистов. Среди проблем Перечня, включающих математические задачи, особое место занимает «Разработка фундаментальных проблем теоретической криптографии и смежных с ней областей математики» (п.54 Перечня). В основных документах ведущих международных и российских конференций и форумов по информационной безопасности подчёркивается, что криптографические методы защиты занимают важное место в системе методов обеспечения информационной безопасности.

Качество криптографических методов определяется в основном криптографической стойкостью системы защиты информации. Основной количественной мерой стойкости является вычислительная сложность решения задачи преодоления выстроенной защиты, то есть задачи дешифрования. Количественная оценка уровня защиты информации с использованием криптосистемы определяется как вычислительная сложность наиболее эффективного из известных алгоритмов дешифрования криптосистемы. Величина оценки измеряется, как правило, временными затратами или числом условных операций ЭВМ, необходимых для реализации алгоритма преодоления защиты.

Решение задач по преодолению криптографической защиты информации с использованием вычислительных алгоритмов основано на разработке математических моделей, адекватно описывающих функционирование криптографической системы защиты информации, а также моделей вычислительных алгоритмов вскрытия криптосистемы. Математическая

формализация таких задач во многих случаях приводит к задачам решения систем уравнений в различных алгебраических структурах. В связи с этим одной из важнейших и активно развиваемых областей криптографии является разработка методов решения различных систем уравнений, связывающих элементы неизвестного ключа криптографической системы защиты информации с известными данными.

К настоящему времени известно несколько классов систем уравнений (линейные, треугольные и др.), разрешимых со сложностью, полиномиальной от $(n+m)$, где n – количество уравнений в системе, а m – количество неизвестных. Список эффективно решаемых классов систем уравнений со временем расширяется в результате прогресса, как в развитии вычислительных средств, так и в расширении класса исследуемых в криптографии систем уравнений, а также в развитии методов их решения. Криптосистема защиты информации признаётся ненадёжной, если соответствующая ей система уравнений эффективно решается с использованием подходящих средств вычислений.

При канонической записи системы уравнений, в которой все неизвестные элементы записаны в левой части системы, имеется биекция между всевозможными левыми частями систем уравнений и отображениями множеств. В криптографических задачах эти множества, как правило, конечны. Поэтому классам систем уравнений, решаемых на ЭВМ с невысокой трудоёмкостью, соответствуют классы отображений, которые характеризуются как слабые с точки зрения криптографической защиты информации. Таким образом, актуальной задачей при исследовании криптографических систем защиты информации является описание подмножества слабых отображений, реализуемых этими системами.

Криптосистемы защиты информации обычно построены на основе композиции нескольких отображений, допускающих удобную аппаратную и/или программную реализацию. При этом криптосистема в целом реализует некоторое множество подстановок, а в некоторых случаях – группу подстановок. В то же время во многих криптосистемах защиты информации можно выделить функциональную часть, множество реализуемых отображений которой образует полугруппу или некоторое подмножество полугруппы, так как построении криптографических алгоритмов используются не только обратимые (групповые), но и необратимые (полугрупповые) отображения. Например, в блочных криптосистемах полугрупповые преобразования могут использоваться при построении раундовых отображений. В поточных шифрах полугрупповые преобразования нередко используются в алгоритмах выработки гаммы. Например, функционирование алгоритма Solitaire описывается математической моделью автомата с частичными функциями переходов, порождающими полугруппу. Существуют классы генераторов гаммы, построенных на основе необратимых преобразований (например, генераторы самоусечения). Принципиальной идеей построения таких генераторов является усложнение слабых, в частности, линейных преобразований с целью повышения уровня защиты информации при несущественном усложнении

реализации.

Таким образом, композиции обратимых и необратимых отображений сочетаются при построении криптографических алгоритмов защиты информации. Это обуславливает необходимость изучения криптографических свойств композиций преобразований информации, построенных с использованием как групповых, так и полугрупповых преобразований. Базовые критерии качества шифрующих отображений были сформулированы еще Клодом Шенноном в известном докладе 1949 года. Дальнейшая их конкретизация применительно к различным классам шифров привела к исследованию разнообразных криптографических свойств отображений информации. Результаты этих исследований нашли отражение в многочисленных работах как отечественных, так и зарубежных специалистов (М.М. Глухов, Б.А. Погорелов, В.Н. Сачков, А. Шамир, М. Хеллман, Р. Рюппель и многие другие).

Имеется немало примеров, показывающих, что не всякая композиция отображений имеет хорошие криптографические свойства с точки зрения защиты информации. Поэтому для оценки уровня криптографической защиты информации важным является описание подмножеств слабых элементов полугруппы или группы, описывающей функционирование криптосистемы. Такое описание может быть использовано для построения тех или иных методов дешифрования. Подмножества слабых элементов полугруппы (группы), определенные в данной работе как подмножества элементов с заданным признаком, являются основным предметом исследования настоящей диссертации.

Одним из наиболее изученных классов криптографически слабых преобразований являются линейные и аффинные преобразования векторных пространств и преобразования, имеющие хорошие приближения в этих классах. В открытой литературе активно изучались многочисленные характеристики нелинейности отображений, связанные с их потенциальными слабостями.

Вместе с тем, слабости криптографических преобразований не обязательно сводятся к их линейности. Например, система уравнений, в которой несколько уравнений несущественно зависят от определенной части переменных (треугольно-ступенчатая система уравнений, соответствующая несовершенному преобразованию), может эффективно решаться методами типа последовательного опробования. В связи с этим актуальными задачами являются как разработка общего подхода к исследованию различного вида слабых преобразований, так и развитие этого подхода на основе учета особенностей исследуемых признаков и полугрупп (групп) преобразований.

В 2005 г. было сформулировано новое алгебраическое направление исследований, связанное с дифференциацией элементов конечных групп по заданным признакам, и представлены первые результаты. В 2006 году это направление получило активное продолжение в ряде публикаций В.М. Фомичева, в которых общий подход к дифференциации по наследственным признакам был развит для конечных групп, групп подстановок и отображений конечных автоматов. Получены результаты для ряда частных классов

наследственных признаков, в том числе, связанных со свойством линейности и аффинности подстановок векторного пространства.

В настоящей работе общий подход к изучению слабых отображений распространяется на полугрупповые преобразования. Актуальность данного направления исследований вытекает из необходимости исследования возможных слабостей отображений информации для широкого класса криптосистем с целью оценки уровня защиты информации.

Целью диссертационной работы является развитие математических принципов создания перспективных средств защиты информации на основе исследования признаков в полугруппах и группах преобразований, определяющих криптографические свойства систем защиты информации.

В соответствии с поставленной целью в диссертационной работе **решаются следующие задачи**:

- Развитие математического аппарата исследования признаков в конечных группах для конечных полугрупп, в том числе, для полугрупп преобразований.
- Исследование свойств наследственных признаков в группах подстановок, обобщающих свойство треугольно-ступенчатости для подстановок векторного пространства.
- Исследование свойств линейного признака в полугруппах и в группах преобразований векторного пространства.
- Разработка математических моделей и исследование способов реализации криптографических протоколов, построенных с использованием наследственных признаков в полугруппах и в группах преобразований.

Методы исследования: теоретическая криптография, теория групп, полугрупп, комбинаторный анализ, теория графов, теория решеток.

Научная новизна работы характеризуется следующими результатами:

1. Математический аппарат исследования признаков в конечных группах обобщен на конечные полугруппы. Дано описание признака в циклической полугруппе $\langle g \rangle$ через характеристики определяющего соотношения.

2. Исследованы характеристики нового класса наследственных признаков π-конгруэнтности в группах подстановок, обобщающего свойства треугольно-ступенчатых подстановок декартовой степени конечного множества.

3. Установлено, что линейная подполугруппа полугруппы преобразований G содержится в пересечении шести наследственных подмножеств полугруппы G. Дано описание этих наследственных подмножеств циклической полугруппы $\langle g \rangle$ через характеристики графа преобразования g.

4. Исследован линейный признак в полугруппе генератора гаммы с неравномерным движением типа [1,2]-самоусечения, используемого при построении криптосистем защиты информации.

5. Разработаны математические модели криптографических протоколов аутентификации пользователей в информационных системах на базе структурного наследственного признака в полугруппах линейных

преобразований векторного пространства, предложен вариант реализации протокола на интеллектуальных картах.

На защиту выносятся следующие результаты:

1. Описание в конечной циклической (моногенной) полугруппе $\langle g \rangle$ наследственных признаков с использованием циклической глубины и периода порождающего элемента g.

2. Описание в циклических группах подстановок наследственных признаков, определяемых π-конгруэнтностью подстановок.

3. Теоретико-множественное включение линейной подполугруппы полугруппы преобразований G векторного пространства над конечным полем в пересечение ряда наследственных признаков в полугруппе G, уточняющее известное включение для случая групп.

4. Доказательство отсутствия линейного признака в циклической полугруппе, порождаемой генератором гаммы [1,2]-самоусечения.

5. Разработка математических моделей криптографических протоколов аутентификации пользователей в информационных системах с использованием наследственного признака, основанного на неинъективности полугрупповых преобразований.

Практическая значимость результатов определяется следующим.

Рассмотренные бинарные классификации элементов конечных полугрупп и групп преобразований имеют существенное значение для разделения на «сильные» и «слабые» множества функций, реализуемых в криптосистемах обеспечения целостности информации, шифрования, идентификации и имитозащиты. Использование «слабых» функций в системах защиты информации даёт возможность криптоаналитику вычислить ключ криптосистемы и получить доступ к ценной информации. Таким образом, разделение функций, реализуемых в криптосистемах, на «сильные» и «слабые» существенным образом определяет принципы создания перспективных средств защиты информации, направленные на устранение опасности обработки информации с помощью некоторых «слабых» функций.

Результаты диссертации по исследованию наследственных признаков в конечных полугруппах и группах могут использоваться для анализа конкретных криптографических систем защиты информации с помощью определения признаков в группах подстановок и в полугруппах преобразований, соответствующих итеративным блочным шифрам, генераторам гаммы (например, генераторам самоусечения) и другим криптографическим схемам. В частности, результаты описания в группах подстановок наследственных признаков, определяемых согласованностью подстановок с заданным разбиением основного множества, позволяют оценивать защищенность информации в криптографических системах относительно методов определения ключевой информации с помощью последовательного опробования.

Результаты по исследованию криптографических протоколов могут быть использованы для создания программного обеспечения с целью решения ряда задач информационной безопасности в информационно-

телекоммуникационных сетях пользователей. К таким задачам относятся, например, аутентификация пользователей сети и распределение секретной ключевой информации между пользователями сети.

В рамках диссертации осуществлены применения полученных теоретических результатов. Построен криптографический протокол аутентификации пользователей сети на основе структурного наследственного признака в полугруппах преобразований. Проанализированы варианты реализации этого протокола и протоколов аутентификации и распределения ключей с использованием линейного признака в группах подстановок. Предложены варианты реализации протоколов на интеллектуальных картах.

Таким образом, совокупность полученных в диссертации результатов можно квалифицировать как новый существенный вклад в развитие и обоснование математических принципов создания средств защиты информации на основе исследования дифференциации элементов конечных полугрупп и групп по наследственным признакам, определяющим криптографические свойства систем защиты информации.

Внедрение результатов исследований. Результаты диссертации использованы во ФГУП "НТЦ Атлас":

1) при построении методов аутентификации информации, хранящейся на интеллектуальных картах;
2) при создании испытательного стенда, предназначенного для разработки методов аутентификации коммерческой информации, обрабатываемой в системах защиты информации, построенных на базе технологии интеллектуальных карт.

Публикации и апробация работы. Результаты диссертации изложены в 10 публикациях и докладывались на конференциях и семинарах различного уровня:

- в МГУ им. М.В. Ломоносова на конференции с международным участием «Математика и безопасность информационных технологий» (МаБИТ-2005),
- на Седьмом Всероссийском Симпозиуме по прикладной и промышленной математике (весенняя сессия) в г. Кисловодске, 2006 г.,
- на V Сибирской научной школе-семинаре с международным участием «Компьютерная безопасность и криптография» в Шушенском - SIBECRYPT′06,
- на научных семинарах МИФИ и ИПИБ МГУ им. М.В. Ломоносова в 2005-2007 г.г.
- на научных семинарах МГТУ им. Баумана в 2007 году.

Структура и объём работы. Диссертация состоит из введения, четырёх глав, заключения и списка литературы из 54 наименований. Работа изложена на 137 страницах с вычислительными примерами, таблицами и исходными текстами программ.

СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность темы диссертации, выделяются и формулируются цели и задачи исследования, отражена научная новизна результатов, описывается структурно-логическая схема диссертационного исследования.

В **первой главе** развивается и распространяется математический аппарат для исследования признаков в конечных группах на конечные полугруппы.

Вводится ряд новых понятий и величин, связанных с наличием признака в конечной полугруппе, сформулированы исследовательские задачи и установлены определяющие свойства признаков.

Пусть Ф — конечная полугруппа, H — подмножество полугруппы Ф или, иначе говоря, множество элементов полугруппы Ф с признаком H, $G=\langle S\rangle$ и $\varnothing\neq Q\subseteq G$, где $S=\{s_1,s_2,\ldots,s_p\}\subset\Phi$ – система образующих элементов полугруппы G, $e\notin S$.

Определим, что элемент g полугруппы G имеет H-признак, если $g\in H$. Полугруппа G (множество Q) имеет H-признак, если $G\cap H\neq\varnothing$ ($Q\cap H\neq\varnothing$), при этом H-признак называется тривиальным (нетривиальным), если $G\cap H$ ($Q\cap H$) – одноэлементное множество (содержит более одного элемента).

Показателем H-признака в полугруппе G (во множестве Q), обозначаемым $\mathrm{pok}_S H$ ($\mathrm{pok}_S(Q\cap H)$), назовём натуральное число, равное $\min\limits_{g\in G\cap H} L(g,S)$ ($\min\limits_{g\in Q\cap H} L(g,S)$), где $L(g,S)$ – длина элемента g в системе образующих S. Показатель H-признака в циклической полугруппе $\langle g\rangle$, обозначаемый $\mathrm{pok}_g H$, равен наименьшему натуральному числу t, при котором $g^t\in H$.

Важными задачами исследования признаков в полугруппе являются распознавание наличия H-признака в полугруппе G, описание множества $G\cap H$ и определение его алгебраических характеристик (показатель в заданной системе образующих, условия тривиальности и др.).

Существенное продвижение в изучении признака в группе достигается при определённых ограничениях на множество $G\cap H$. В связи с этим в разделе 1.2 признаки в группе классифицируются по алгебраическим свойствам: полугрупповой, групповой, наследственный, тривиальный.

H-признак в полугруппе G называется полугрупповым (групповым), если $G\cap H$ — подполугруппа (подгруппа) полугруппы G (обозначается $G\cap H<G$).

Наследственный признак H является обобщением полугруппового признака и определяется условием: если элемент g полугруппы G принадлежит H, то $\langle g\rangle\subseteq H$. Для определения множества $G\cap H$ рассмотрим полугруппу G как множество с квазипорядком: $g\leq g'$ для $g,g'\in G\Leftrightarrow\langle g\rangle<\langle g'\rangle$. Фактормножество $G/\cong$, где $g\cong g'$ для $g,g'\in G\Leftrightarrow\langle g\rangle=\langle g'\rangle$, частично упорядочено, поэтому наследственное подмножество Q полугруппы G определено как наследственное подмножество фактормножества $G/\cong$. Следовательно, из теории решёток следует, что

множество Q имеет единственное представление в виде объединения всех максимальных в Q циклических подполугрупп (полугруппа $\langle g\rangle$ максимальна в Q, если $\langle g\rangle\subseteq Q$ и $\langle g\rangle$ не является собственной подполугруппой циклической полугруппы, содержащейся в Q): $Q=\bigcup\limits_{g\in B_Q}\langle g\rangle$, где B_Q – система элементов полугруппы G, порождающих максимальные в Q циклические подполугруппы. Систему B_Q назовём c-базисом множества Q, а величину $h_c(Q)$, равную $|B_Q|$, назовём c-шириной множества Q.

Таким образом, по аналогии с конечными группами получаем способ определения множества всех элементов полугруппы G с заданным наследственным признаком H, основанный на определении элементов из H во всех максимальных в полугруппе G циклических подполугруппах.

Теорема 1.5. Если полугруппа G имеет наследственный H-признак, то

а) $B_{G\cap H}\subseteq\bigcup\limits_{g\in B_G}B_{\langle g\rangle\cap H}$;

б) $h_c(G\cap H)\le\sum\limits_{g\in B_G}h_c(\langle g\rangle\cap H)$;

в) равенства $B_{G\cap H}=\bigcup\limits_{g\in B_G}B_{\langle g\rangle\cap H}$ и $h_c(G\cap H)=\sum\limits_{g\in B_G}h_c(\langle g\rangle\cap H)$ выполнены тогда и только тогда, когда для любого $g\in B_G$ и любого $g'\in B_{\langle g\rangle\cap H}$ циклическая подгруппа $\langle g'\rangle$ максимальна во множестве $G\cap H$. ▷

Описание наследственного подмножества $\langle g\rangle\cap H$ циклической полугруппы $\langle g\rangle$ порядка n равносильно описанию c-базиса $(g^{t_1},\ldots,g^{t_r})$ множества $\langle g\rangle\cap H$. Эта задача сводится к задаче определения соответствующего подмножества наименьших натуральных чисел $\{t_1,\ldots,t_r\}$, названного множеством (H,g)-пороговых чисел (обозначается $\Pi(H,g)$).

Обозначим через C^g решетку всех циклических подполугрупп полугруппы $\langle g\rangle$ относительно теоретико-множественного включения.

Назовем порядком элемента g полугруппы G (обозначается ord$g$) наименьшее натуральное t такое, что $g^t=e$, где e — идемпотент.

Пусть N – множество натуральных чисел, $N_n=\{1,\ldots,n\}$, где $n\in N$. Рассмотрим на множестве N_{d+n-1} квазипорядок ρ_g: $t\rho_g\tau$ (иначе говоря, t не превышает τ в смысле квазипорядка ρ_g) $\Leftrightarrow\langle g^\tau\rangle\subseteq\langle g^t\rangle$.

Обозначим через $N_{d+n-1}/\cong$ фактормножество множества N_{d+n-1}, где $\tau\cong t$ для $\tau,t\in N_{d+n-1}$ тогда и только тогда, когда $\langle g^\tau\rangle=\langle g^t\rangle$. Через $[\tau]$ обозначим класс эквивалентности из $N_{d+n-1}/\cong$, содержащий элемент τ из N_{d+n-1}. Система представителей классов эквивалентности фактормножества $N_{d+n-1}/\cong$, состоящая из наименьших представителей классов эквивалентности относительно естественного порядка натуральных чисел, называется *каноническим трансверсалом* и обозначается $N_{d,n}$.

Теорема 1.7. а) Канонический трансверсал $N_{d,n}$ есть решётка по отношению ρ, антиизоморфная решетке C^g; ord$g$ и 1 суть соответственно максимальный и минимальный элементы решётки $(N_{d,n},\rho)$, и при $d>1$:

$N_{d,n} = \{1,\ldots,d\text{-}1,\min[d],\ldots,\min[d+n\text{-}1]\}$,
где $\min[\tau]=\min\{t\in\{d,\ldots,d+n\text{-}1\}: (t,n)=(\tau,n)\}$ при $\tau=d,\ldots,d+n\text{-}1$.

б) Если в полугруппе $\langle g\rangle$ имеется наследственный H-признак, то $\Pi(H,g)$ есть множество минимальных элементов t решётки $(N_{d,n},\rho)$ таких, что $g^t\in H$.▷

Следствие 1. Если полугруппа $\langle g\rangle$ имеет наследственный H-признак, то

$$\mathrm{pok}_g H = \begin{cases} \min\Pi(H,g), & \text{если } d>1 \text{ и } \min\Pi(H,g)<d, \\ \min\limits_{t\in\Pi(H,g)}(d+(t-d)\bmod r_t), & \text{если } \min\Pi(H,g)\geq d, \end{cases}$$

где $r_t=(t,n)$. ▷

Следствие 2. Циклическая полугруппа $\langle g\rangle$ имеет тривиальный наследственный H-признак тогда и только тогда, когда множество $\Pi(H,g)$ состоит из единственного числа, равного $\mathrm{ord}g$. ▷

Во **<u>второй главе</u>** исследуются наследственные признаки в группах подстановок, связанные со свойствами треугольно-ступенчатых подстановок.

Пусть $\Phi(X)$ – группа всех подстановок множества X, и подстановка $g\in\Phi(X)$ имеет цикловую структуру $C(g)$, записываемую таблицей чисел $C(g)=(l_1[q_1],\ldots,l_k[q_k])$, то есть g имеет q_i циклов длины l_i, $i=1,\ldots,k$.

Обозначим через $\mathrm{Part}(X)$ множество всех разбиений множества X на непустые блоки. Подстановка g однозначно определяет разбиение $\pi=(X_0,\ldots,X_{m-1})$ множества X на блоки, из элементов которых составлены циклы подстановки g. Это разбиение обозначим $\pi_c(g)$ и назовём g_c-**разбиением**. Рассмотрим $\pi_c(g)$ как монотонную функцию и обозначим g-подфункцию функции $\pi_c(g)$ через $\pi_g(t)$, т.е. $\pi_g(t)=\pi_c(g^t)$, $t=1,\ldots,n$.

Принадлежность элементов x и x' множества X одному блоку разбиения π обозначим $x\overset{\pi}{\cong}x'$. Разбиение π назовем ***g*-конгруэнцией**, а подстановку g назовем π-конгруэнтной, если из $x\overset{\pi}{\cong}x'$ следует $g(x)\overset{\pi}{\cong}g(x')$.

Для любого разбиения π из $\mathrm{Part}(X)$ множество всех π-конгруэнтных подстановок есть подгруппа полной симметрической группы $S(X)$ (обозначим эту подгруппу $S(X/\pi)$). Следовательно, $S(X/\pi)$ можно рассматривать как групповой признак в любой группе подстановок G множества X. Получим условия, при которых подстановка g является π-конгруэнтной.

Пусть Ω – конечное множество, Ω^* – множество слов в алфавите Ω, $l\in N$ и слово $\omega=(\omega_0,\omega_1,\ldots,\omega_{l-1})\in\Omega^l$. Длиной периода слова ω назовем наименьший делитель τ числа l такой, что $\tau<l$ и $\omega_i=\omega_{i+\tau}$ для $i=0,1,\ldots,l\text{-}\tau\text{-}1$, если такой существует. В противном случае длиной периода слова ω полагается l. Слова ω и ω' из Ω^* циклически эквивалентны, если они совпадают с точностью до циклического сдвига. Будем говорить, что слово ω имеет бесповторный период, если период слова ω есть бесповторная выборка из алфавита Ω. Слова ω и ω' называются совместимыми, если они имеют такие бесповторные периоды, которые либо циклически эквивалентны, либо не содержат общих элементов. Множество из двух и более слов совместимо, если любые два слова множества совместимы, а множество из одного слова с бесповторным периодом полагается совместимым.

Пусть g_c-разбиение $\pi_c(g)=(C_1,\ldots,C_r)$, где длина цикла C_j равна l_j, $j=1,\ldots,r$. Рассмотрим отображение $\omega_\pi: X \to Z/m$, где $\omega_\pi(x)$ для $x \in X$ есть номер блока разбиения π, содержащего x. Отображение ω_π индуцирует отображение $\omega_\pi^*: X^* \to Z/m^*$, где $\omega_\pi^*(x_1,x_2,\ldots)=(\omega_\pi(x_1),\omega_\pi(x_2),\ldots)$. Таким образом, $\omega_\pi^*(C_j)$ есть слово длины l_j в алфавите Z/m, $j \in \{1,\ldots,r\}$.

Теорема 2.1. Подстановка g является π-конгруэнтной тогда и только тогда, когда совместимо множество слов $\omega_\pi^*(C_j)$, $j=1,\ldots,r$.▷

Данный критерий позволяет получить ряд необходимых условий π-конгруэнтности подстановки g, выраженных через характеристики цикловой структуры подстановки g, разбиения π, и через частотные характеристики слов $\omega_\pi^*(C)$ для циклов C подстановки g. Проверка невыполнения этих условий для многих подстановок и разбиений требует существенно меньше вычислений, чем проверка условий критерия.

Пусть $\overline{\pi_c}(g)=(\overline{C}_1,\ldots,\overline{C}_h)$ – разбиение множества циклов подстановки g на классы π-эквивалентных циклов, то есть $\overline{\pi_c}(g) \in \mathrm{Part}(\pi_c(g))$, и τ_j - длина периода слова $\omega_\pi^*(C)$ для любого цикла C из класса $\overline{C}_j$, $j=1,\ldots,h$. Пусть также $\lambda: N_r \to N_h$ – сюръекция, определяемая тем, что цикл $C_j \in \overline{C}_{\lambda(j)}$, $j=1,\ldots,r$. Пусть q_{ij} – частота номера i в слове $\omega_\pi^*(C_j)$, $i=0,\ldots,m\text{-}1$, $j=1,\ldots,r$, и равенство $M(q_{0,j},\ldots,q_{m-1,j})=(0[k_0],\ldots,(m\text{-}1)[k_{m-1}])$ означает, что в слове $\omega_\pi^*(C_j)$ номер 0 содержится k_0 раз, …, номер m-1 содержится k_{m-1} раз.

Утверждение 2.1. Если подстановка g является π-конгруэнтной, то:

1) $\pi_c(g) \le \overline{\pi_c}(g) \le \overline{\pi}$ и выполнены свойства:

а) $k \le h \le r$, и имеется сюръекция $\varepsilon: N_h \to N_k$, определяемая тем, что $\overline{C}_j \in X'_{\varepsilon(j)}$, $j=1,\ldots,h$, и композиция сюръекций $\lambda\varepsilon: N_r \to N_k$, определяемая тем, что цикл C_j принадлежит блоку $X'_{\lambda\varepsilon(j)}$ разбиения $\overline{\pi}$, $j=1,\ldots,r$;

б) $l_j \le \left|\overline{C}_{\lambda(j)}\right| \le b_{\lambda\varepsilon(j)} \cdot m_{\lambda\varepsilon(j)}$, $j=1,\ldots,r$;

с) $\left|\overline{C}_j\right|$ делится на $b_{\varepsilon(j)}$, $j=1,\ldots,h$;

2) $\tau_1+\ldots+\tau_h=m$, откуда следует, что $d_1+\ldots+d_h \ge m$, где d_j - наибольший общий делитель длин всех циклов из класса $\overline{C}_j$, $j=1,\ldots,h$;

3) для частот q_{ij} выполнены свойства:

а) $M(q_{0,j},\ldots,q_{m-1,j})=(0[m\text{-}\tau_j], \frac{l_j}{\tau_j}[\tau_j])$, $j=1,\ldots,r$;

б) все ненулевые числа набора $(q_{i,1},\ldots,q_{i,r})$ прямо пропорциональны длинам соответствующих циклов $l_1,\ldots,l_r$, $i=0,\ldots,m\text{-}1$.▷

Обозначим $B^{i_1,\ldots,i_s}_{\alpha_1,\ldots,\alpha_s}$ множество всех наборов из X^n, у которых значение компонент с номерами $i_1,\ldots,i_s$ фиксировано и равно $\alpha_1,\ldots,\alpha_s$ соответственно. При любом фиксированном наборе $\{i_1,\ldots,i_s\}$ система множеств

$\{B^{i_1,\ldots,i_s}_{\alpha_1,\ldots,\alpha_s},(\alpha_1,\ldots,\alpha_s)\in X^s\}$ образует множество блоков разбиения множества X^n, обозначим это разбиение $R(i_1,\ldots,i_s)$.

Пусть $T_\Delta(s,n)$ - множество треугольно-ступенчатых преобразований, у которых первые s координатных функций зависят от $x_1,\ldots,x_s$.

Утверждение 2.6. Подстановка g множества X^n принадлежит $T_\Delta(s,n)$ тогда и только тогда, когда g является $R(1,\ldots,s)$-конгруэнтной. ▷

В **третьей главе** исследуется задача описания линейной подполугруппы в полугруппе преобразований векторного пространства над конечным полем, возникающая при анализе многих криптосистем защиты информации, обрабатываемой в дискретном виде.

Преобразование g конечного множества X назовем k-циклическим, если в его графе имеется в точности k циклических точек, $0<k\le|X|$. Обозначим через $CYC(k;G)$ множество всех k-циклических преобразований из полугруппы G, где $G\le\Xi(X)$.

Утверждение 3.5. Для любой полугруппы G и для произвольного натурального числа k, где $0<k\le|X|$, множество $CYC(k;G)$ является наследственным. Для любого преобразования $g\in\Xi(X)$ циклическая полугруппа $\langle g\rangle$ есть подмножество одного из блоков разбиения $G=CYC(1;G)\cup\ldots\cup CYC(|X|;G)$. ▷

Рассмотрим граф преобразования g векторного пространства P^r. Для циклической вершины x графа Γ_g обозначим через $T_x(g)$ дерево подхода к вершине x, и через $n_{x,i}(g)$ — количество вершин на i-м уровне дерева $T_x(g)$, где i - целое неотрицательное число. Нулевым уровнем является корень дерева, т.е. $n_{x,0}=1$. Обозначим через $h(g)$ наибольшую из длин подходов в графе преобразования g.

Пусть $H(q|n)$ - множество преобразований g из $\Xi(P^r)$ таких, что величина $\sum_{i=0}^{k} n_{x,i}$ делится на q для любой циклической вершины x графа Γ_g и при любом $k=1,\ldots,h$.

Утверждение 3.6. Множество $H(q|n)$ является наследственным. ▷

Стабилизатором элемента x векторного пространства P^r в полугруппе преобразований G называется множество (полугруппа) преобразований g полугруппы G, относительно которых элемент x является неподвижным.

Обозначим через g_c ограничение преобразования g из $\Xi(P^r)$ на множество циклических точек преобразования g. Преобразование g из полугруппы G является унидоминантным (L-замкнутым сверху, $\overline{\sigma}$-стабильным, p-нормально неподвижным), если унидоминантна (L-замкнута сверху, $\overline{\sigma}$-стабильна, p-нормально неподвижна) подстановка g_c

Обозначим через $SGL(r,P)$ полную линейную подполугруппу полугруппы $\Xi(P^r)$. Назовём $SGL(r,P)$-признак **линейным признаком**.

В любой полугруппе преобразований пространства P^r признак $SGL(r,P)$ является полугрупповым.

Теорема 3.2. Справедливо включение:

$$SGL(r,P) \subseteq \Xi_\theta \cap \overline{C} \cap \Lambda^{[p\nu]}(P^r) \cap \Sigma(P^r) \cap H(q|n) \cap H_{cyc},$$

где θ — ноль пространства P^r и Ξ_θ — стабилизатор нуля в полугруппе $\Xi(P^r)$, множества $\overline{C}$, $\Lambda^{[p\nu]}(P^r)$ и $\Sigma(P^r)$ суть множества соответственно всех L-замкнутых сверху, p-нормально неподвижных и $\overline{\sigma}$-стабильных преобразований пространства P^r,

$$H_{cyc} = CYC(1;\Xi(P^r)) \cup CYC(q;\Xi(P^r)) \cup \ldots \cup CYC(q^r;\Xi(P^r)). \triangleright$$

Исследована линейная подполугруппа генератора $[d,k]$-самоусечения, построенного на основе линейного регистра связи (ЛРС) с обратной связью f, реализующего подстановку h пространства P^r. Если на выходе ЛРС ноль, то состояние x заменяется на $h^d(x)$, если единица – на $h^k(x)$. Продвижка σ ЛРС за один такт определяется формулой $\sigma = d \cdot (f(x) \oplus 1) + k \cdot f(x)$. Порождаемая генератором циклическая полугруппа есть $\langle h^\sigma(x) \rangle$.

Пусть генератор $[d,k]$-самоусечения имеет ненулевое начальное заполнение, а ЛРС имеет максимальный период.

Известно, что период T_r $[d,k]$-самоусеченной последовательности, порожденной ЛРС длины r, равен $T_r = \left\lfloor \frac{2}{3}\left(2^r - 1\right) \right\rfloor$, где $[d,k] = t \cdot [1,2] \bmod 2^r\text{-}1$ и НОД$(t, 2^r\text{-}1)=1$.

Утверждение 3.8. Если преобразование g пространства P^r реализует генератор [1,2]-самоусечения, то циклическая полугруппа $\langle g \rangle$ не имеет линейного признака. $\triangleright$

В **<u>четвертой главе</u>** исследованы наследственные признаки, связанные с неинъективностью полугрупповых преобразований, и использованы для разработки математических моделей протоколов аутентификации пользователей в информационных системах. Описана реализация разработанного протокола на базе технологии интеллектуальных карт.

Рассмотрим отношение эквивалентности $\overset{g}{\cong}$ на множестве X, индуцируемое преобразованием g множества X: $x \overset{g}{\cong} x'$ тогда и только тогда, когда $g(x)=g(x')$. Пусть $p(g)$ – разбиение множества X, индуцируемое отношением эквивалентности $\overset{g}{\cong}$. Известно, что если $h(g)$ — максимальная из длин подходов к циклам графа Γ_g полугруппового преобразования g, и n – наименьшее общее кратное длин всех циклов, то полугруппа $\langle g \rangle$ определяется соотношением $g^d = g^{d+n}$, где

$$d = \begin{cases} 1, & h(g) \le 1; \\ h(g), & h(g) > 1. \end{cases}$$

Теорема 4.1. Пусть циклическая полугруппа $\langle g \rangle$ определяется соотношением $g^d = g^{d+n}$, где $d>1$, тогда $p(g^t) < p(g^{t+1})$ для всех $t \in \{1,\ldots,d\text{-}1\}$ и $p(g^t) = p(g^{t+1})$ для любого $t \ge d$. $\triangleright$

Теорема позволяет каждому полугрупповому преобразованию g множества X поставить в соответствие цепь разбиений $(p(g),\ldots,p(g^d))$ из решетки Part(X), которую назовем **цепью g-разбиений**. Разбиение $p(g^d)$ назовем

максимальным g-разбиением и обозначим его $p_{\max}(g)$. Обозначим для произвольного разбиения $p\in\mathrm{Part}(X)$: $\Xi(p(g)\geq p)=\{g\in\Xi(X)\colon p(g)\geq p\}$; $\Xi^p=\{g\in\Xi(X)\colon p_{\max}(g)=p\}$.

Следствие. 1) $\Xi(p(g)\geq p)$ и Ξ^p суть наследственные признаки в полугруппе $\Xi(X)$ при любом разбиении $p\in\mathrm{Part}(X)$.

2) Если циклическая полугруппа $\langle h\rangle$ определяется соотношением $h^d=h^{d+n}$, где $d>1$, то $\mathrm{pok}_h\Xi(p(g)\geq p_{\max}(h))=d$. ▷

Математическая идея предлагаемого протокола аутентификации заключается в использовании обеими сторонами секретного полугруппового преобразования g векторного пространства P^r, где P – конечное поле порядка q. Циклическая полугруппа $\langle g\rangle$ определяется соотношением $g^d=g^{d+n}$, где $d>1$.

В ответ на запрос заявителя проверяющий отправляет заявителю случайно выбранный вектор x и получает от него вектор x', где $x'\neq x$. Аутентификация считается успешной, если $g^d(x)=g^d(x')$.

Корректность протокола обеспечивается существованием указанного вектора x', так как для любой ациклической вершины x вектор $g^d(x)$ является циклическим, поэтому найдется хотя бы один (например, циклический) вектор $x'\in P^r$ такой, что $x'\neq x$ и $g^d(x')=g^d(x)$.

Протокол работает эффективно, если заявитель генерирует вектор x' с невысокой трудоемкостью, а злоумышленник может угадать (при случайном выборе) значение x' с небольшой вероятностью, не превышающей заранее оговоренную допустимую границу.

Семейство $E=\{g\}$ преобразований, отвечающих данным требованиям, имеет вид: $E=\{\delta\cdot\lambda\cdot\delta^{-1}\}$, где $\delta\colon P^r\to P^r$ — нелинейная биекция и $\lambda\colon P^r\to P^r$ — линейное полугрупповое преобразование с длиной наибольшего цикла l и максимальной длиной подхода h. Каждое преобразование из множества E является нелинейным и подобно преобразованию λ. Например, в качестве биекции δ при $r=64$ можно использовать алгоритм блочного шифрования DES, AES, ГОСТ-28147 и др. Тогда выбор секретного полугруппового преобразования g сводится к совместному выбору ключа блочного шифра участниками протокола. При неизменном преобразовании λ смена преобразования g равносильна смене ключа. Для любого натурального t верно: $g^t=\delta\cdot A^t\cdot\delta^{-1}$, что позволяет с невысокой сложностью вычислять g^t.

Пусть злоумышленник случайным образом угадывает вектор x', чтобы получить полномочия законного пользователя информационной системы. Если все векторы из $P^r\backslash\{x\}$ равновероятны, то вероятность P_x того, что $g^h(x')=g^h(x)$ при заданном векторе x и достаточно больших h оценивается величиной, обратной к числу циклических вершин графа Γ_g

Применение разработанного протокола аутентификации было осуществлено в рамках исследований особенностей использования технологии интеллектуальных карт при построении систем защиты информации. Была рассмотрена архитектура информационной системы из широкого класса, описано функционирование и взаимодействие элементов. Система

обеспечивает авторизованный доступ зарегистрированных пользователей к ресурсам, содержащимся в ней. Авторизация в системе выполняется на основе результатов выполнения аутентификации пользователя с системой.

Предложен вариант информационной системы, в которой пользователи аутентифицируются с системой по протоколу, разработанному в четвертой главе. При этом каждому пользователю выдается службой документов персональное секретное преобразование, реализованное в интеллектуальной карте.

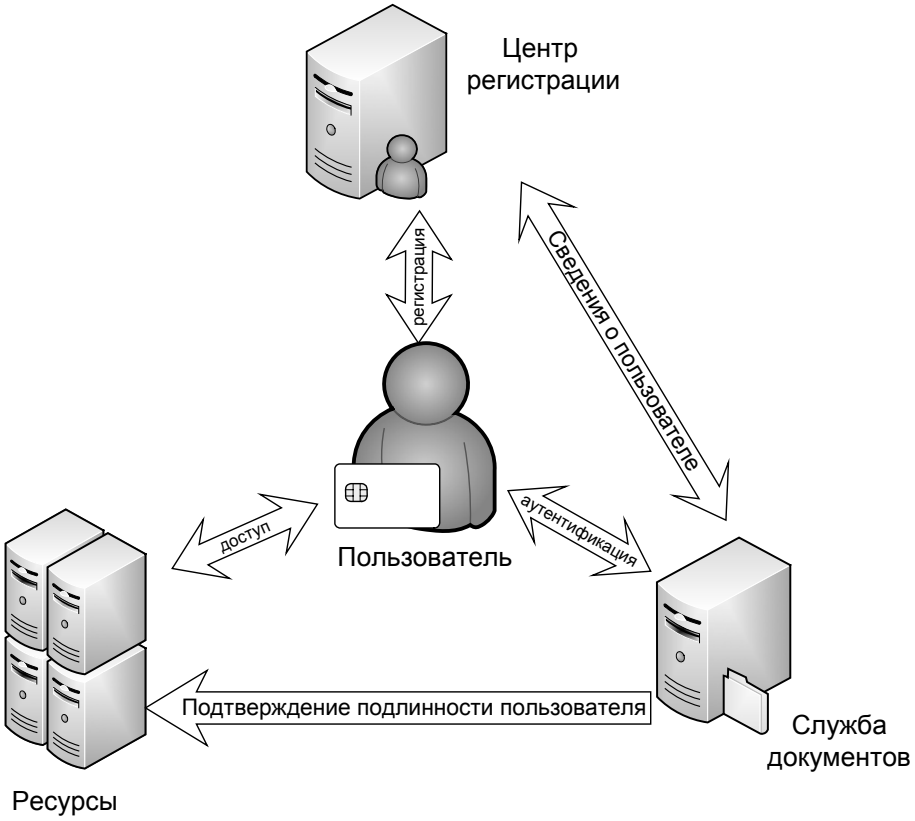

Рис.1. *Архитектура информационной системы*

Действия в протоколе аутентификации со стороны пользователя реализованы как приложение защищенного хранилища данных для смарт карт, отвечающих стандарту Java Card v.2.2.1. Приложение хранит данные в виде файлов и разграничивает доступ к ним с помощью отдельного модуля, отвечающего за выполнение протокола. Создан стенд, в котором интеллектуальная карта со встроенным приложением выполняет протокол аутентификации с терминалом, осуществляющим доступ к данным, хранимым на карте,

В качестве блочного шифра, используемого как преобразование подобия δ при формировании g, используется алгоритм 3DES со 128-битовым ключом, реализованный в смарт карте аппаратно и являющийся частью её операционной системы.

В приложении реализована матрица λ размера 64×64, для которой вероятность угадывания злоумышленником вектора x' равна 2^{-32}.

ОСНОВНЫЕ ВЫВОДЫ И РЕЗУЛЬТАТЫ РАБОТЫ

1. Математический аппарат исследования признаков в конечных группах обобщен на конечные полугруппы. Исследование в полугруппах подмножеств элементов с заданным признаком моделирует в виде общей алгебраической задачи определение подмножеств слабых преобразований для криптосистем защиты информации, построенных с использованием полугрупповых преобразований. Признаки в полугруппах классифицированы в зависимости от алгебраических свойств множества $G \cap H$ на полугрупповые, групповые, наследственные, тривиальные.

2. Задача описания наследственного признака в полугруппе сведена к задачам описания признака во всех максимальных циклических подполугруппах полугруппы G. Сложность определения наследственного подмножества определяется числом максимальных циклических подполугрупп полугруппы G (c-шириной полугруппы G) и сложностью определения рассматриваемого наследственного признака H в циклических полугруппах.

3. Существенно более сложно по сравнению с группами описывается наследственный признак в циклической полугруппе. Описание признака в полугруппе $\langle g \rangle$ дано через характеристики определяющего соотношения, получены условия тривиальности признака.

4. В группах подстановок исследовано свойство π-конгруэнтности, то есть согласованности подстановок с заданным разбиением π основного множества, которое обобщает свойства треугольно-ступенчатых подстановок конечномерных векторных пространств.

5. Исследованы характеристики нового класса наследственных признаков π-конгруэнтности в группах подстановок. Доказан критерий π-конгруэнтности подстановок, показано, что вычислительная сложность определения π-конгруэнтности подстановок по порядку не меньше мощности основного множества подстановок. Получен ряд необходимых условий π-конгруэнтности подстановок, позволяющих в некоторых случаях определять тривиальность признака π-конгруэнтности с невысокой вычислительной сложностью.

6. Описание признака π-конгруэнтности использовано для описания свойств признака треугольно-ступенчатости в группах подстановок множества X^n, где X - конечное множество. Даны определяющие свойства треугольно-ступенчатых преобразований множества X^n, доказан критерий их обратимости. Полученные результаты исследования признака треугольно-ступенчатости являются существенными для оценки защищенности широкого класса криптосистем относительно методов последовательного опробования ключей.

7. Исследованы в полугруппе G преобразований векторного пространства над конечным полем полугрупповой линейный признак, важный для анализа многих криптосистем защиты информации, обрабатываемой в дискретном виде. Установлено, что линейная подполугруппа полугруппы преобразований G содержится в пересечении шести изученных наследственных подмножеств полугруппы G. Описание этих наследственных подмножеств циклической

полугруппы $\langle g \rangle$ определяется характеристиками графа преобразования g. Для случая групп данная оценка уточняет ранее известную оценку. Полученное уточнение расширяет класс криптосистем, для которых с использованием доказанного теоретико-множественного включения можно обосновать высокий уровень защиты информации относительно метода линеаризации.

8. Исследована линейная подполугруппа полугруппы генератора $[d,k]$-самоусечения с неравномерным движением, используемого при построении криптосистем защиты информации. Выделен широкий класс генераторов самоусечения с максимальным периодом и для него доказано, что линейный признак в полугруппе генератора отсутствует. Полученные результаты позволяют сделать вывод, что в выходной гамме генератора самоусечения из исследованного класса не имеется участков, линейно зависящих от знаков начального заполнения.

9. Исследованы наследственные признаки, основанные на неинъективности полугрупповых преобразований. Эти признаки использованы для разработки математических моделей протоколов аутентификации пользователей в информационных системах. Обоснованы положительные свойства разработанных математических моделей протоколов: возможность обеспечения заданного уровня надежности за счет выбора параметров секретного преобразования, сравнительно невысокая вычислительная сложность реализации, удобство реализации на широком классе вычислительных платформ, в том числе, на интеллектуальных картах.

10. Разработанный протокол аутентификации пользователей применен при исследовании систем защиты информации на базе технологии интеллектуальных карт. Создано приложение интеллектуальной карты и реализован стенд, в котором выполняется протокол аутентификации карты терминалом. В карте протокол реализован в виде модуля, способного встраиваться во все интеллектуальные карты, отвечающие спецификации Java Card 2.2.1. Функционирование модуля отлажено и протестировано на микроконтроллере производства NXP. Характеристики секретного преобразования выбраны такими, что они предполагают удобную реализацию на выбранной вычислительной платформе.

Данная реализация протокола предъявляет низкие требования к вычислительным ресурсам, и предоставляет возможность использования стандартных, хорошо изученных алгоритмов шифрования.

Основные публикации по тема диссертации:

Основные положения диссертационной работы опубликованы в 10 печатных трудах, в том числе в 8 статьях в журналах, включенных ВАК РФ в перечень ведущих рецензируемых научных журналов и изданий:

1. *Н.В. Фомичёв*. Об аутентификации пользователей информационных систем. // Безопасность информационных технологий. – М.: МИФИ, – 2007, №2, – С. 50-52.

2. *Н.В Фомичев*. Признаки, определяемые Свойствами линейных полугрупповых преобразований. // Вестник МГУ леса. Лесной вестник. № 4. - М.: МГУ леса. – 2007. – С. 164-166.

3. *Н.В. Фомичев*. Признаки, определяемые свойствами треугольно-ступенчатных подстановок векторного пространства. // Вестник МГУ леса. Лесной вестник. № 4. - М.: МГУ леса. – 2007. – С. 166-167.

4. *Н.В. Фомичёв*. Свойства линейных признаков в полугруппах преобразований. // Обозрение прикладной и промышленной математики. – 2007. – т.14, в.5. - С. 941-942.

5. *Н.В. Фомичёв*. Признаки π-конгруэнтности в группах подстановок. // Обозрение прикладной и промышленной математики. – 2007. – т.14, в.3. - С. 568

6. *В.М. Фомичёв, Н.В. Фомичёв*. Исследование признаков элементов в конечных полугруппах и группах // Безопасность информационных технологий. - М.: МИФИ. – 2006, №1. – С. 97-100.

7. *В.М. Фомичёв, Н.В. Фомичёв*. Общая алгебраическая задача различения элементов конечных полугрупп и групп // Обозрение прикладной и промышленной математики. – 2006. – т.13, в.1. - С. 157-159.

8. *В.М. Фомичёв, Н.В. Фомичёв*. Вычислительные аспекты исследования признаков в полугруппах и в группах // Обозрение прикладной и промышленной математики. – 2006. – т.13, в.1. - С. 155-157.

9. *Н.В. Фомичёв*. Наследственные признаки в конечных полугруппах. // Математика и безопасность информационных технологий. Материалы конференции в МГУ им. Ломоносова 28-29 октября 2004 г. – М.: МЦНМО, 2005. – С. 194-197.

10.*В.М. Фомичёв, Н.В. Фомичёв*. Исследование наследственных признаков в конечных полугруппах и группах // Материалы докладов V Сибирской научной школы-семинара с международным участием "Компьютерная безопасность и криптография" - SIBECRYPT'06 в Шушенском 5-8 сентября 2006 г. – Томск: Вестник Томского гос. университета – 2006. - Приложение №17. - С. 81-86.