

На правах рукописи

Таныгин Максим Олегович

УСТРОЙСТВО КОНТРОЛЯ ОБРАЩЕНИЙ
И ПРОЦЕДУР ДОСТУПА К СЕКТОРАМ
ЖЁСТКОГО МАГНИТНОГО ДИСКА

Специальность 05.13.05 – Элементы и устройства
вычислительной техники и систем управления

Автореферат
диссертации на соискание учёной степени
кандидата технических наук

КУРСК – 2007

Работа выполнена в ГОУ ВПО
«Курский государственный технический университет»
на кафедре вычислительной техники
в совместной научно–исследовательской лаборатории
Центра информационных технологий в проектировании РАН
и Курского государственного технического университета:
«Информационные распознающие телекоммуникационные
интеллектуальные системы»

Научный руководитель:	доктор технических наук, профессор Типикин А. П.
Официальные оппоненты:	доктор технических наук, профессор Довгаль В. М. кандидат технических наук Жуковский Д. В.
Ведущая организация:	Тульский государственный университет

Защита состоится 27 апреля 2007 г. в 16 часов на заседании диссертационного совета Д.212.105.02 в Курском государственном техническом университете (305040 г. Курск, ул. 50 лет Октября, д. 94, конференц–зал)

Отзывы на автореферат в двух экземплярах, заверенные печатью, направлять по указанному выше адресу на имя учёного секретаря диссертационного совета Д.212.105.02.

С диссертацией можно ознакомиться в библиотеке Курского государственного технического университета.

Автореферат разослан «___» _____ 2007 г.

Учёный секретарь диссертационного совета:

Титенко Е. А.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность работы. В современной вычислительной технике средства контроля обращений к информации, хранящейся в памяти ЭЦВМ, находят применение в системах различного назначения: управления базами данных, ограничения доступа к информации, мониторинга событий, определения нагрузок на узлы ЭЦВМ. Системные и пользовательские программы во время своей работы многократно обращаются к данным, большая часть которых хранится на жёстких магнитных дисках (ЖМД). В связи с этим совершенствование средств контроля обращений к ЖМД является важным направлением сокращения общих затрат времени при обработке данных и обеспечении целостности дискового информационного пространства.

Программная реализация большинства существующих систем контроля обращений к диску имеет два основных недостатка. Во-первых, необходимы дополнительные затраты процессорного времени на анализ каждого обращения к файлам, и, во-вторых, отсутствует возможность контролировать обращения к отдельным секторам файлов. В существующих системах указанные недостатки устраняются за счёт выполнения части операций по контролю обращений к данным специальными аппаратными средствами. При этом некоторые из таких устройств по адресам контролируемых областей диска, записанных в их памяти, лишь фиксируют факт обращения к секторам и передают информацию об этом на уровень программных средств, где осуществляется её анализ. Другие известные устройства выполняют анализ такой информации без участия программного обеспечения.

Основным недостатком используемых аппаратных средств является снижение их обнаруживающей способности из-за программной доступности кодов атрибутов контролируемых областей диска, которые могут быть изменены либо в результате сбоя в работе системы контроля обращений, либо в результате ошибочного или преднамеренного искажения. Это влечёт за собой дополнительные временные затраты на обеспечение достоверности контроля. Устранение указанного недостатка определяет необходимость поиска новых подходов и создания инструментальных средств для организации подсистемы контроля обращений к кодам атрибутов контролируемых областей данных ЖМД.

Таким образом, актуальной является научно-техническая задача повышения скорости выполнения и обнаруживающей способности процедур контроля обращений к секторам файлов путём их переноса с программного на аппаратный уровень.

Объект исследования: система контроля обращения к данным, хранящимся на ЖМД.

Предмет исследования: процедуры контроля обращений к секторам файлов ЖМД, а также структурная организация специализированных устройств, их реализующих.

Цель работы: создание способов, аппаратно–ориентированных процедур и быстродействующего устройства контроля обращений к секторам ЖМД, позволяющих повысить обнаруживающую способность и скорость выполнения процедур контроля обращений к файлам ЭЦВМ. Для достижения поставленной цели необходимо решить следующие задачи:

- 1) анализ современных методов и систем контроля обращений к данным, выбор направления исследования;
- 2) создание способа контроля обращений к файлам на основе аппаратной проверки атрибутов секторов ЖМД;
- 3) разработка архитектуры системы контроля обращений (СКО), распределение функций между устройством контроля обращений к секторам (УКОС) и программными компонентами СКО;
- 4) разработка процедур взаимодействия УКОС с управляющим программным обеспечением (УПО) и средств контроля процедур доступа к служебным данным УКОС;
- 5) исследование путём математического моделирования на ЭЦВМ процесса функционирования УКОС и эффективности его применения;
- 6) разработка алгоритмов работы и структурно – функциональной организации УКОС.

Методы исследования базируются на современных достижениях теории математического моделирования, теории случайных процессов, теории вероятностей, теории проектирования ЭЦВМ и теории автоматов.

Научная новизна работы состоит в следующем.

1. На основе аппаратной проверки команд, записываемых в порты контроллера жёсткого магнитного диска, созданы два способа аппаратного контроля обращений и процедур доступа к секторам файлов, хранящихся на ЖМД, которые различаются организацией долговременного хранения кодов их атрибутов и позволяют повысить обнаруживающую способность устройства контроля обращений к секторам (УКОС), исключить несанкционированные запись и чтение контролируемых секторов, и ограничить доступ к секторам диска.
2. Разработаны аппаратно–ориентированные процедуры и функциональные узлы УКОС для проверки команд управляющего программного обеспечения (УПО), отличающиеся тем, что содержимое ключевых кодовых полей команд, проверяемых в УКОС формируется путём последовательных преобразований случайных чисел, и позволяющие организовать контроль процедур доступа к служебным данным УКОС с целью повышения вероятности заданной установки атрибутов секторов.
3. Синтезированы алгоритм функционирования, структурные и функциональные схемы интерфейсного УКОС, ориентированные на ускорение анализа кодов атрибутов секторов за счёт конвейерного выполнения операций по выборке из ОЗУ, позволяющие повысить быстродействие и обнаруживающую способ-

ность УКОС, снизить создаваемые им временные задержки до величины, на три порядка меньшей, чем время доступа к данным ЖМД, а также блокировать исполнение контроллером ЖМД заданного пользователем списка команд ЭЦВМ.

4. На основе аппарата цепей Маркова и метода вложенных подграфов созданы вероятностные математические модели процедур контроля обращений к секторам данных и процессов информационного обмена между УКОС и УПО, позволившие выбрать приемлемые для практической реализации значения параметров УКОС, а также обосновать достигаемые показатели обнаруживающей способности разработанных средств аппаратного контроля.

Практическая ценность:

1. Разработана организация двух вариантов УКОС: встроенного в контроллер накопителя и в виде интерфейсного экрана, различающихся организацией долговременного хранения кодов атрибутов секторов ЖМД, и выполнено сравнение требуемых для их реализации затрат. Разработаны архитектура программно-аппаратной системы контроля обращений к секторам и проект реализации интерфейсного устройства контроля обращений.

2. Произведена оценка аппаратной сложности интерфейсного УКОС на основе ПЛИС (1014 слайсов, 265 блоков ввода-вывода и типовые микросхемы оперативных, постоянных и перепрограммируемых постоянных запоминающих устройств) и его быстродействия, (увеличение времени обращения к данным ЖМД при использовании разработанного устройства не превышает 0.1%).

3. Разработанное интерфейсное УКОС не требует изменения схем и конструкции контроллера жесткого диска и вводится в ЭЦВМ как переходная плата, вставляемая в его разъём, с использованием стандартных интерфейсов и системных программ типовых ЭЦВМ.

4. Созданные способы, процедуры и устройство контроля обращений к секторам могут быть применены в аппаратных системах контроля периферийных устройств ЭЦВМ, системах управления базами данных и в системах ограничения доступа к информации.

Реализация и внедрение. Результаты работы использованы и внедрены в ОКБ «Авиаавтоматика» (г. Курск), в Курском отделении Сберегательного банка РФ № 8596, а также в учебном процессе Курского государственного технического университета.

Апробация работы. Основные положения и результаты диссертационной работы докладывались и обсуждались на международных и российских научно-технических конференциях: МНТК «Распознавание-2005» (г. Курск, 2005 г.), 23 межвузовской научно-технической конференции студентов и аспирантов в области научных исследований «Молодёжь и XXI век» (Курск, 2005 г.), 2-м международном студенческом форуме (Белгород, 2004 г.), МНТК «Проблемы передачи и обработки информации в сетях и системах телекоммуникаций» (Рязань, 2004, 2005 гг.), а также на научных семинарах кафедры ВТ КурскГТУ.

Публикации. По материалам диссертации опубликовано 11 работ, в том числе 2 патента на изобретение, 4 статьи, 3 из которых – в журналах, входящих в перечень ВАК, 4 тезиса докладов и 1 депонированная рукопись.

Личный вклад соискателя в работах, опубликованных в соавторстве, состоит в следующем: в [3] – произведено математическое моделирование работы системы, контролирующей обращения к данным ЖМД; в [5, 11] – разработаны способ и процедуры проверки программных команд, выдаваемых устройству, и выполнен ряд математических экспериментов, позволивших получить численные характеристики вероятности исполнения устройством посторонних команд; в [6] – разработаны принципы работы и структурная организация интерфейсного устройства, контролирующего команды, записываемые в порты КЖД и предложен способ хранения атрибутов секторов в памяти устройства; в [7] – разработаны способ фиксации обращений к секторам накопителя информации и способ хранения атрибутов секторов в их заголовочных частях, разработана структурная организация блоков устройства ограничения доступа, их осуществляющих; в [9] – разработаны принципы функционирования компонентов программно – аппаратной системы, осуществляющих контроль обращений к данным ЖМД, и определены основные информационные потоки между ними; в [10] – разработана структурная организация контроллера ЖМД с дополнительной функцией контроля и обращений к отдельным секторам.

На защиту выносятся:

1. Способы аппаратного контроля обращений и процедур доступа к секторам файлов, хранящихся на ЖМД, основанные на переносе процедур контроля обращений с программного уровня ЭЦВМ на уровень контроллера жесткого магнитного диска и позволяющие повысить обнаруживающую способность УКОС, исключить несанкционированную запись и чтение контролируемых секторов и ограничить доступ к секторам диска.

2. Аппаратно–ориентированные процедуры и функциональные узлы УКОС для проверки команд УПО и основанные на них средства контроля процедур доступа к служебным данным УКОС, позволяющие снизить вероятность исполнения устройством команд, выданных иными, помимо УПО, программами и вероятность изменения атрибутов секторов без ведома пользователя.

3. Алгоритмы функционирования и структурно – функциональная организация интерфейсного УКОС, позволяющие за счёт конвейерного выполнения операций формирования адресов, чтения кодов атрибутов из ОЗУ и их анализа повысить быстродействие УКОС и его обнаруживающую способность, снизить создаваемые им временные задержки и блокировать исполнение контроллером жесткого магнитного диска команд ЭЦВМ.

4. Математические модели процедур контроля обращений к секторам ЖМД и процессов информационного обмена между УКОС и УПО, основанные на аппарате цепей Маркова и методе вложенных подграфов, позволившие выбрать приемлемые значения параметров УКОС и обосновать достигаемые показатели обнаруживающей способности разработанных средств аппаратного контроля.

Структура и объем работы. Диссертационная работа состоит из введения, 4 разделов и заключения, содержащих 133 страницы основного текста, 29 рисунков, список использованных источников из 101 наименования на 12 страницах, и 8 приложений на 25 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** показана актуальность темы диссертационной работы, сформулированы цели и задачи исследований, научная новизна, практическая ценность и результаты апробации работы, структура и объём диссертации.

В **первой главе** дана общая характеристика систем контроля обращений (СКО) к данным ЭЦВМ, и в частности систем, контролирующих обращения к ЖМД; приводятся основные принципы работы таких систем и требования, предъявляемые к ним. Отмечено, что при программной реализации СКО, каждое обращение требует затрат процессорного времени на выполнение операций по проверке атрибутов, что снижает производительность ЭЦВМ и скорость работы с диском. В этой связи наиболее предпочтительными с точки зрения повышения быстродействия, а также обнаруживающей способности являются аппаратные СКО, контролирующие обращения путём анализа атрибутов областей ЖМД. Известным аппаратным СКО присущи следующие недостатки:

- структурная организация тех из них, которые обеспечивают наибольшую достоверность контроля, не обеспечивает возможности быстрого и удобного изменения атрибутов секторов;
- контролируемые данные обычно описываются адресами контролируемых областей диска, что при большой фрагментации файлов требует существенных временных затрат для их анализа;
- используемые в известных системах для хранения атрибутов элементы энергонезависимой памяти имеют сравнительно большое время доступа к данным;
- программная доступность атрибутов данных снижает достоверность контроля.

Исходя из этого, для повышения быстродействия аппаратных СКО и снижения создаваемых ими задержек необходимо контролировать обращения к ЖМД по атрибутам отдельных секторов, а также максимально ускорить выполнение операций по выборке из банков памяти кодов атрибутов и их анализу. Для удобства управления такими системами и обеспечения возможности их гибкой настройки необходимо организовывать взаимодействие аппаратных компонентов СКО с системными и пользовательскими программами. Для повышения достоверности контроля необходимо реализовать в аппаратных компонентах СКО дополнительные механизмы обеспечения невозможности несанкционированного изменения атрибутов. Они включают в себя проверку устройством команд программного обеспечения и обязательный контроль программными компонентами СКО выполнения этих команд и применены в данной работе при разработке средств контроля процедур доступа к служебным данным устройства контроля обращений к секторам (УКОС).

Таким образом, решена первая задача данной диссертации.

Во **второй главе** описывается аппаратная реализация функций контроля обращений к секторам ЖМД. Разработаны основные принципы работы программно-аппаратной системы контроля обращений и её архитектура (рис. 1).



Рис. 1. Основные компоненты программно-аппаратной СКО

Вводятся четыре типа атрибутов: первый – обращения к сектору не контролируются; второй – контролируется запись в сектор; третий – контролируются любые обращения к сектору; четвёртый – доступ к сектору может быть закрыт по внешним управляющим сигналам разрешения/запрещения чтения и записи, подаваемым со специальной панели управления.

В материалах данной главы приводятся основные функции программной части СКО – так называемого управляющего программного обеспечения (УПО), и определены основные информационные потоки между ним и УКОС: от УПО в УКОС передаются команды модификации атрибутов секторов; от УКОС в УПО – информация о зафиксированных или предотвращённых попытках доступа к секторам диска, по которой программа УПО делает запись в журнал регистрации обращений к секторам (рис. 1).

Созданы два способа аппаратного контроля обращений. По первому способу коды атрибутов записываются на долговременное хранение непосредственно в заголовочные части секторов ЖМД в дополнительные служебные поля, имеющиеся у большинства моделей дисков, читаются вместе с заголовочными частями секторов и анализируются УКОС, выполненным в виде дополнительной микросхемы, размещённой на плате КЖМД как один из его узлов. Устройство контролирует внутренние управляющие сигналы контроллера и управляет его работой без вмешательства в алгоритмы работы остальных его узлов. При этом оно выполняет чтение, анализ и модификацию атрибутов во взаимодействии с остальной частью КЖМД.

Второй способ предусматривает хранение атрибутов в оперативной памяти УКОС, включаемого между интерфейсным шлейфом и разъёмом КЖМД, обработку устройством записываемых в порты КЖМД команд на доступ к секторам, чтение атрибутов адресуемых секторов из памяти, их анализ и фиксацию обращений к секторам. Кроме того, если поданы соответствующие внешние сигналы,

В компьютер на уровне контроллера жесткого магнитного диска (КЖМД) вводится дополнительное аппаратное средство – УКОС. Оно выполняет хранение, обработку и модификацию двоичных кодов атрибутов секторов данных ЖМД, и по ним, путём анализа потока команд, записываемых в порты КЖМД, контролирует обращения к секторам со стороны ЭЦВМ. На программном уровне атрибуты присваиваются файлу, а устройство анализирует атрибуты отдельных секторов. Для этого с помощью дополнительных программ по таблице размещения файлов определяются адреса секторов файлов и передаются в УКОС. На аппаратном уровне вво-

УКОС блокирует передачу в порты контролера команд на доступ к секторам. Основное отличие интерфейсного УКОС от встраиваемого заключается в увеличении аппаратных затрат на оперативное хранение кодов атрибутов секторов (в оперативной памяти УКОС) и расходов времени на организацию их долговременного хранения (сохранение на ЖМД).

Достоверность контроля обращений зависит от достоверности внутренних служебных данных УКОС, в том числе атрибутов секторов. В материалах данной главы описаны четыре аппаратно–ориентированные процедуры проверки команд программного обеспечения, позволяющие выполнять контроль обращений к служебным данным УКОС, в том числе к атрибутам секторов, в режимах их программно–управляемой модификации. Это снижает как вероятность исполнения устройством «ложных» модифицирующих команд, так и вероятность недопустимой установки атрибутов в результате сбоя в аппаратуре. Режим программно–управляемой модификации атрибутов определяется подачей в УКОС соответствующего внешнего сигнала с панели управления.

Процедура проверки ключевого слова команды и контроля целостности команды основана на введении в формат многословной составной команды (МСК), обрабатываемой устройством, дополнительного поля «Ключ». В момент запуска пользователем программы УПО, выдающей команды модификации атрибутов, та выдаёт УКОС нулевую команду «Старт», в состав поля «Ключ» которой введено дополнительное подполе А. Пусть S – содержимое поля «Ключ» очередной полученной УКОС команды, S_i – содержимое поля «Ключ» i -й (предыдущей) переданной на исполнение в УКОС команды. Полученная команда будет передана на исполнение, если выполнится равенство:

$$S = F(S_0^A, S_i) = F^{[i]}(S_0^A, S_1), \quad (1)$$

где F – выполненное устройством преобразование слова S_i в соответствии с содержимым S_0^A подполя А команды «Старт»; $F^{[i]}$ – выполненное i раз преобразование F ; S_1 – содержимое поля «Ключ» первой команды, переданной на исполнение в УКОС после команды «Старт». Рекуррентное преобразование F , в качестве которого был выбран циклический сдвиг на определяемое S_0^A число разрядов, выполняется идентично в устройстве и УПО. Дополнительно по контрольным битам, введённым в каждое слово МСК, проверяется её целостность.

Процедура сравнения ключевого поля с содержимым буфера истории команд (БИК) основана на введении в состав УКОС специального буфера, хранящего содержимое полей «Ключ» ранее переданных на исполнение МСК. При ёмкости буфера в r слов, где r – глубина истории команд, множество $\{\sigma\}^i$ слов, записанных в нём после передачи на исполнение i команд, определится как:

$$\{\sigma\}^i = \{F^{[i-j]}(S_0^A, S_1)\}, \quad j = 1 \dots r. \quad (2)$$

Содержимое поля «Ключ» S полученной УКОС команды, сравнивается с содержимым регистров БИК $\{\sigma\}^i$. Выполнение условия $S \in \{\sigma\}^i$ свидетельствует о том, что в устройстве были переданы на исполнение одна или несколько «ложных» команд, выданных иными, помимо УПО приложениями.

Процедура подсчёта числа исполненных команд заключается в сравнении по команде «Счёт» числа команд, переданных в УКОС на исполнение, с числом команд, выданных УПО. Данная команда выдаётся периодически во время выполнения программно–управляемой модификации атрибутов.

Процедура буферизации команд и их дополнительной проверки подразумевает введение в состав УКОС дополнительной оперативной памяти, служащей буфером команд устройства (БКУ), передаваемых в устройство во время сеанса модификации атрибутов. Каждая МСК, полученная УКОС, проверяется по описанной выше алгоритмической схеме и в случае выполнения условия (1) записывается в БКУ. В буфере БКУ формируется очередь команд, исполняемых устройством после их проверки. В систему команд устройства вводится дополнительная команда «Финиш», получив которую, устройство прекращает запись команд в БКУ. После этого УПО проверяет содержимое БКУ. Для упрощения процедуры проверки, повышения её скорости и достоверности анализируется небольшое по объёму контрольное слово, формируемое устройством из записываемых в БКУ данных и сопоставляемое с контрольным словом, сформированным УПО по выданным в УКОС командам. Для формирования контрольного слова применён простой в аппаратной реализации алгоритм сложения по модулю 2. Проверка содержимого БКУ осуществляют не только однократно, после выдачи команды «Финиш», но и параллельно с заполнением БКУ, по специальной команде «Проверка БКУ». Команды из БКУ, исполняются УКОС только при получении специального разрешающего сигнала, подаваемого пользователем после окончательной проверки содержимого БКУ.

Таким образом, решены вторая, третья и четвёртая задачи диссертации.

В **третьей главе** рассматривается задача выбора приемлемых для аппаратной реализации значений параметров УКОС и обоснования показателей его обнаруживающей способности. Оценки выполнялись путём математического моделирования функционирования УКОС в составе СКО в двух основных режимах работы: в режиме модификации атрибутов и в обычном режиме контроля обращений к секторам. Основным показателем в режиме модификации атрибутов выбрана вероятность искажения их кодов за счёт исполнения УКОС «ложных» команд. Проанализированы три возможных варианта искажения.

При известном алгоритме преобразований F содержимого поля «Ключ» посторонней программе (ПП) необходимо для выдачи серии «ложных» команд подобрать содержимое поля «Ключ» S_i слова–инструкции предыдущей МСК, записанной в БКУ, и содержимое S_0^A подполя А команды «Старт», задающее вид преобразования F . Вероятность этого события $p_{\text{пдб}}$ определяется разрядностью поля «Ключ» и подполя А и составляет $p_{\text{пдб}} = 2^{-13} \times 2^{-4} \approx 10^{-5}$. В качестве хеш–функции, формирующей контрольное слово, выбрано побитовое суммирование по модулю 2 слов МСК, обозначенное ниже f_{\oplus} и \sum_{\oplus} , где первое – шестнадцатиразрядная сумма слов каждой МСК, второе – итоговая сумма кодов всех МСК. «Ложные» команды не будут обнаружены в случае совпадения двух контроль-

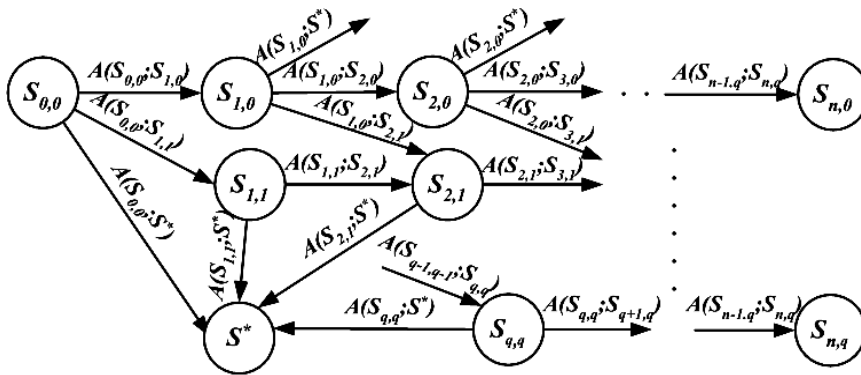
ных слов, одно из которых сформировано в устройстве из кодов «ложных» МСК, а другое – в УПО из кодов МСК, выданных после серии «ложных» команд:

$$\sum_{j=I+1}^W \oplus (f_{\oplus}(K_j^y)) = \sum_{j=1}^V \oplus (f_{\oplus}(K_j^{\text{пп}})), \quad (3)$$

где K_j^y – коды МСК УПО, $K_j^{\text{пп}}$ – коды «ложных» МСК, V – количество записанных в БКУ «ложных» МСК, I – номер команды УПО, после которой была выдана серия «ложных» МСК, W – общее количество выданных УПО команд.

Вероятность выполнения равенства (3) равна вероятности совпадения двух независимо формируемых 16-битовых слов $p_{\text{кс}} = 2^{-16} \approx 1,5 \cdot 10^{-5}$. Итоговая величина вероятности искажения кодов атрибутов за счёт исполнения УКОС команд, сформированных ПП при известном алгоритме F , равна произведению вероятностей $p_{\text{ис1}} = p_{\text{пдб}} \cdot p_{\text{кс}}$ и не превышает 10^{-9} .

При втором варианте искажения атрибутов «ложные» команды, передаваемые в УКОС, содержат в поле «Ключ» случайно сформированные коды. Случайный процесс подбора содержимого поля «Ключ» моделировался с использованием аппарата



марковских цепей (рис. 2). На рисунке: состояние $S_{i,j}$ соответствует записи в БКУ j «ложных» команд из выданных ПП i пробных; поглощающее состояние S^* соответствует обнаружению действий ПП за счёт случайного совпадения содержимого поля «Ключ» очередной

Рис. 2. Марковская цепь, имитирующая подбор содержимого поля «Ключ»

пробной МСК с содержимым БИК; $A(S'; S'')$ – вероятность перехода из состояния S' в состояние S'' ; q – максимальное число записанных в БКУ «ложных» команд.

Получены оценки значений вероятности $p_{\text{зап}}$ записи в БКУ хотя бы одной «ложной» команды, в результате анализа которых были найдены рекомендуемые величины параметров разрядности поля «Ключ» $k = 8 \dots 14$ и глубины истории команд $r = 10 \dots 15$, а также максимальное значение вероятности $p_{\text{зап}}$, равное $3 \cdot 10^{-2}$. Установлено, что вероятность $p_{\text{исп}}$ того, что одна или несколько «ложных» команд не будут обнаружены при подсчёте числа команд, определяется как произведение двух сомножителей $p_{\text{исп}} = (p_{\text{зап}})^2$, и при выбранных параметрах $k = 3$, $r = 12$ она не превысит 10^{-3} . Проверка содержимого БКУ по контрольному слову позволяет снизить вероятность искажения атрибутов, так как результирующая вероятность исполнения «ложных» команд $p_{\text{ис2}}$ равна произведению $p_{\text{ис2}} = p_{\text{исп}} \cdot p_{\text{кс}}$. При таком варианте искажения кодов атрибутов заранее не известны коды «ложных» команд, записанных в БКУ, поэтому слово в правой части равенства (3) формируется случайно и независимо от слова в левой. Следовательно, вероятность их совпадения равна показателю обнаруживающей способности хеширования $p_{\text{кс}} \approx$

$\approx 1,5 \cdot 10^{-5}$. При этих условиях вероятность необнаружения «ложных» команд и искажения атрибутов $p_{ис2} \approx 10^{-8}$.

Исследован третий возможный вариант искажения кодов атрибутов, когда ПП могут изменить файл задания МСК программы УПО (адреса секторов, атрибуты которых должны быть модифицированы), записывая в соответствующие порты УКОС собственные коды. Существует конечная вероятность того, что после окончания записи программой УПО в порт УКОС кода команды модификации атрибутов, в БКУ устройства она запишется с изменёнными словами файла задания. Подобные изменения обнаруживаются проверкой контрольного слова и контролем целостности команды. Вероятности модификации файла задания была определена путём математического моделирования процесса выдачи команд устройству. Кроме работы программ УПО и работы ПП в модели, также учтена работа системных процессов. Выдача устройству команд программами была представлена как случайный полумарковский процесс. Интервалы времени пребывания системы в состояниях «работает ПП» и «работает системный процесс» имитировались вложенными подграфами. В результате математических экспериментов установлено, что ожидаемый диапазон изменения вероятности модификации файла задания МСК $p_{мфз} \approx 0,015 \dots 0,15$. Вероятность модификации файлов заданий одной или более команд в группе проверяемых команд, подчиняется биномиальному закону и зависит от длины L этой группы. Получена следующая формула вероятности искажения атрибутов по данному типу действий ПП:

$$p_{ис3} = p_{кс} \cdot \sum_{i=1}^L [C_L^i \cdot (p_{мфз})^i \cdot (1 - p_{мфз})^{L-i} \cdot (p_{кл})^i], \quad (4)$$

где $p_{кл}$ – вероятность необнаружения модификации файла задания одной МСК системой контроля целостности команды ($p_{кл} = 2^{-8}$).

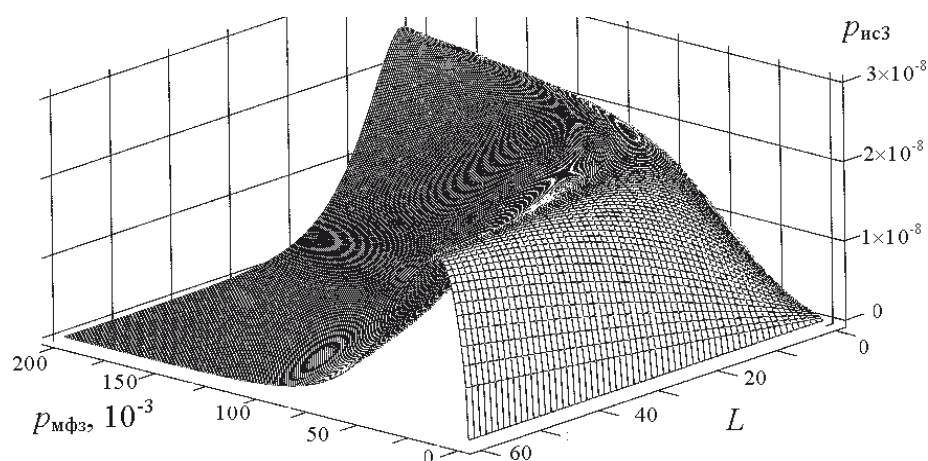


Рис. 3. Зависимость вероятности искажения атрибутов $p_{ис3}$ от длины группы проверяемых команд L и вероятности искажения файла задания $p_{мфз}$ одной МСК.

Из вычисленной по формуле (4) зависимости $p_{ис3} = f(L, p_{мфз})$ при $p_{кс} = 1,5 \cdot 10^{-5}$ и $p_{кл} = 2^{-8}$, приведённой на рис. 3, следует, что при достаточно частой подаче в устройство команды «Проверка БКУ» (при $L \leq 10$), вероятность искажения кодов атрибутов по данному типу попыток не превышает 10^{-8} .

Рассмотренные варианты искажения кодов атрибутов не являются взаимоисключающими. Поэтому результирующее значение оценки вероятности искажения кодов атрибутов может превысить найденные частные её значения по ка-

ждому из вариантов, и в худшем случае увеличиться до 10^{-7} на один сеанс модификации атрибутов пользователем.

В данной главе также приведено описание математической модели процесса функционирования УКОС в режиме контроля обращений к данным. Основное

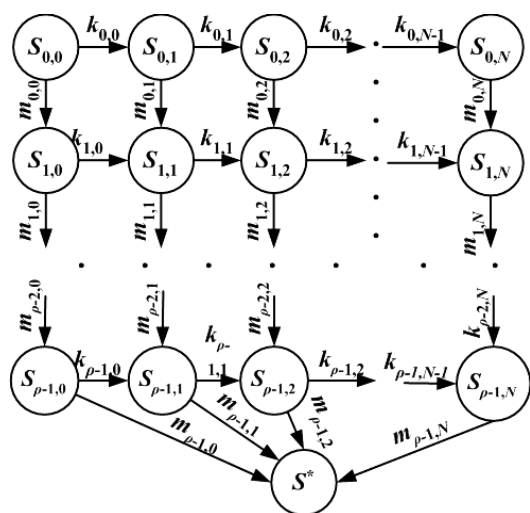


Рис. 4. Марковская цепь, имитирующая обращения к ЖМД

внимание при этом уделено исследованию возможности СКО обнаруживать и своевременно предотвращать деструктивные воздействия на файлы ЖМД, появившейся в результате аппаратной реализации процедуры контроля обращений к секторам. С помощью аппарата марковских цепей (рис. 4) выполнено математическое моделирование одного из вероятных вариантов деструктивного воздействия на ЖМД, заключающегося в серии попыток доступа к файлам, при котором обращения к неконтролируемым файлам случайно чередуются с обнаруженными обращениями к контролируемым. На рисунке: N – число неконтролируемых файлов, определяемое как

$N = N_{\phi} \cdot (1 - D)$; N_{ϕ} – общее число файлов диска; D – доля контролируемых файлов; r – пороговое число обращений к контролируемым файлам, после превышения которого они признаются деструктивным воздействием (введено для снижения вероятности «ложной тревоги» из-за ошибочных действий пользователя); состояние $S_{i,j}$ соответствует j обращениям к неконтролируемым файлам и i обращениям к контролируемым. Переходы из состояния $S_{i,j}$ при обращении к неконтролируемому и контролируемому файлу происходят с интенсивностями $k_{i,j}$ и $m_{i,j}$ соответственно. Поглощающее состояние S^* соответствует обнаружению деструктивного воздействия после обращения к r контролируемым файлам.

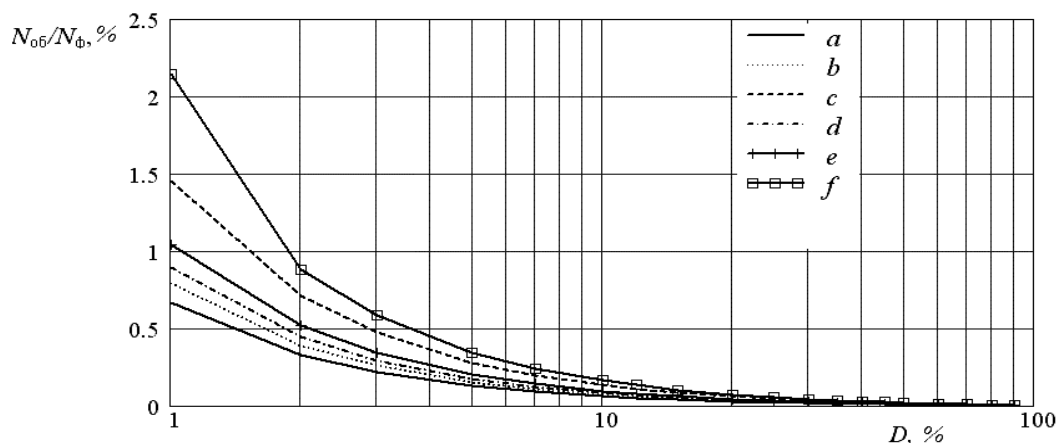


Рис. 5. Зависимость доли искажённых файлов $N_{об}/N_{\phi}$ от объёма контролируемых файлов D (данные по оси абсцисс приведены в логарифмическом масштабе) при:

- a) $U = 0,8, r = 5$; b) $U = 0,9, r = 5$; c) $U \approx 1, r = 5$;
- d) $U = 0,8, r = 7$; e) $U = 0,9, r = 7$; f) $U \approx 1, r = 7$;

U – значение вероятности обнаружения деструктивного воздействия.

В результате моделирования получены оценки (рис. 5) обнаруживающей способности СКО, в состав которой введено УКОС, которые показали, что при целесообразной доле аппаратно контролируемых файлов, равной 60%, и изменении величины вероятности обнаружения деструктивного воздействия в диапазоне 0,8...1, доля искажаемых файлов снижается за счёт своевременной приостановки воздействия до уровня 0,1% от общего числа файлов диска.

Таким образом, решена пятая задача диссертационного исследования.

В **четвёртой главе** разработан алгоритм функционирования интерфейсного УКОС. В соответствии с приведенными в предыдущих главах способами контроля обращений определены основные функции устройства и последовательность микроопераций блока управления. Синтезирована структурная схема устройства (рис. 6), разработаны функциональные схемы отдельных блоков устройства и схема подключения устройства к интерфейсам ЭЦВМ и КЖМД.

Функциональные блоки обмениваются данными по 16-разрядной внутренней шине ВШ[15:0]. Все блоки формируют сигналы для записи флагов условий в группе триггеров флагов (ГТФ) блока управления (БУ). Флаги записываются также по сигналам от таймера, отсчитывающего интервалы времени проведения процедуры модификации атрибутов. Кроме того, флаги записываются по внешним разрешающим сигналам, а также формируются из анализируемых слов, передаваемых по ВШ[15:0]. По этим флагам микропрограммное устройство управления вырабатывает управляющие сигналы для остальных блоков устройства. Формирователь слова вырабатывает 16-разрядное слово данных (слово состояния устройства, команды КЖМД и т. д.) и выдаёт его на ВШ[15:0].

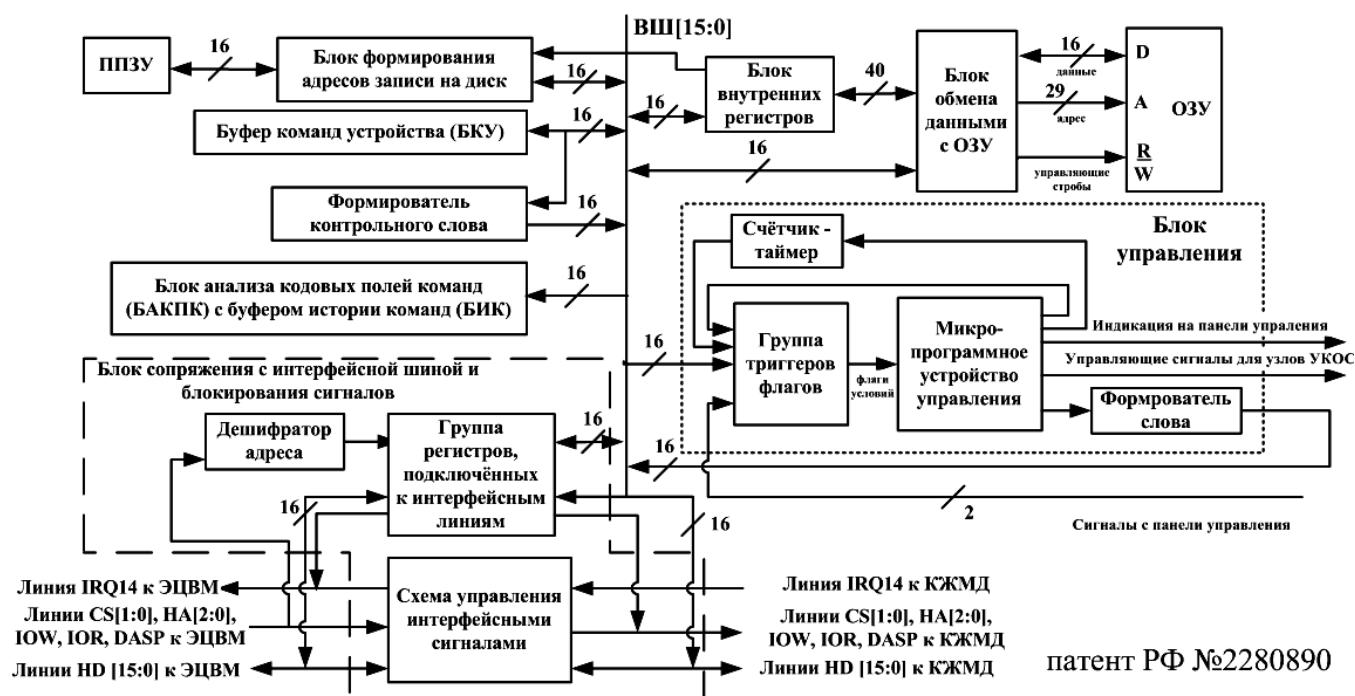


Рис. 6. Структурная схема интерфейсного УКОС

Назначение других блоков устройства (рис. 6):

– блок внутренних регистров служит для временного хранения данных, полученных с интерфейсной шиной;

- блок обмена данными с ОЗУ, формирует адреса, по которым производится чтение или запись кодов атрибутов в ОЗУ; выполняет модификацию кодов атрибутов; формирует сигналы записи флагов в ГТФ, информирующие БУ о процессе обмена данными с ОЗУ и о типе прочитанных атрибутов;

- буфер БКУ хранит передаваемые в устройство команды модификации атрибутов, а формирователь контрольного слова формирует из их кодов контрольное слово, выдаваемое на ВШ[15:0];

- блок формирования адресов записи на диск формирует из записанных в ППЗУ данных (адреса начального сектора и требуемого количества секторов) адрес сектора ЖМД для записи (чтения) очередного 512 – байтового блока кодов атрибутов при их сохранении на ЖМД;

- блок сопряжения с интерфейсной шиной и блокирования сигналов контролирует передачу данных по линиям интерфейса IDE, а также определяет порядок выдачи данных из группы регистров, подключённых к интерфейсным линиям (РПИЛ), на линии HD[15:0], идущие к ЭЦВМ и КЖМД;

- регистры из группы РПИЛ по сигналам от дешифратора адреса выдают/принимают данные на линии HD[15:0], идущие к ЭЦВМ и КЖМД.

Одним из основных требований к интерфейсному УКОС в режиме контроля обращений является необходимость быстрого чтения атрибутов из ОЗУ и их анализа. Поскольку особенностью работы устройства является возможность чтения атрибутов только после появления на интерфейсных линиях, идущих от ЭЦВМ, последнего слова команды доступа к секторам, блоки УКОС сконфигурированы таким образом, чтобы сохранить все предыдущие слова данной команды во внутренних регистрах, сформировать адреса читаемых атрибутов и другие необходимые данные за наименьшее число тактов. Это достигается за счёт одновременного параллельного выполнения нескольких микроопераций независимыми узлами УКОС: блоком внутренних регистров, блоком обмена данными с ОЗУ, формирователем слова.

Блок обмена данными с ОЗУ может читать 8 двухбитных кодов атрибутов за один такт (рис. 6), тогда как в одной команде ЭЦВМ может быть адресовано до 256 секторов, что может потребовать для прочтения всех атрибутов до 32 тактов чтения. Поэтому данный блок построен так, чтобы в текущем одном такте чтения атрибутов конвейерно формировать адреса для следующего. Схема анализа считанных кодов введена в состав третьей ступени названного конвейера, что при подобранных соответствующим образом кодах атрибутов обеспечивает формирование флагов условий ГТФ параллельно с чтением атрибутов из ОЗУ. Всё это обеспечивает максимальную скорость выполнения операций контроля обращений к секторам ЖМД.

Описанные выше процедуры проверки устройством команд программного обеспечения, позволяющие выполнить контроль обращений к служебным данным УКОС, реализуются по специальным микропрограммам БУ и поддерживаются формирователем контрольного слова, буфером БКУ и блоком анализа кодовых полей команд, функциональная схема которого приведена на рис. 7.

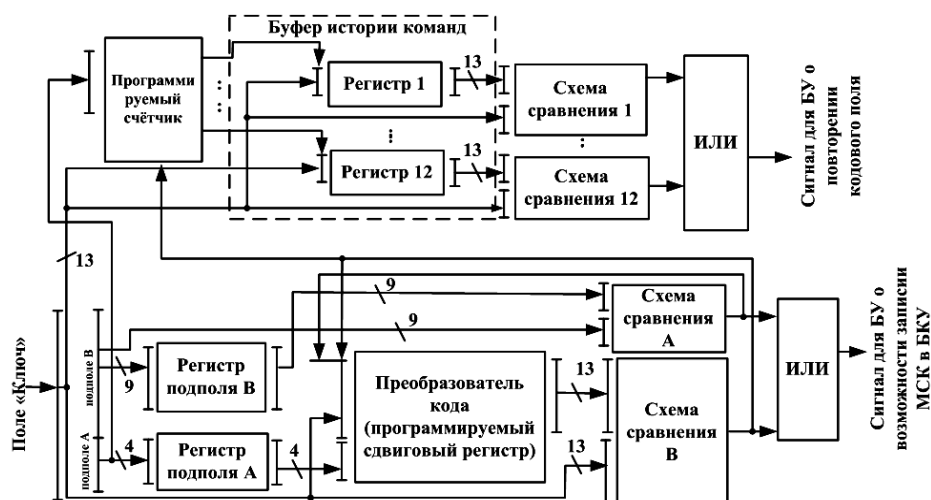


Рис. 7. Функциональная схема блока анализа кодовых полей команд

параметры записи содержимого ОЗУ на диск хранятся соответственно в дополнительных микросхемах ОЗУ, ПЗУ, ППЗУ. В соответствии с максимальной задержкой распространения сигнала в схеме УКОС, запрограммированной в ПЛИС, которая составила 17.9 нс, была выбрана тактовая частота работы устройства, равная 55 МГц. С учётом выбранной тактовой частоты были рассчитаны временные задержки, создаваемые УКОС при каждом обращении ЭЦВМ к диску. Они определены на основании анализа алгоритма работы УКОС, показавшего, что для сохранения поступившей команды во внутренних регистрах, чтения из ОЗУ кодов атрибутов заданных секторов и их анализа требуется $(\lfloor \mu/8 \rfloor + 20)$ тактов работы устройства, где μ – заданное в команде ЭЦВМ количество секторов, к которым производится обращение, $\lfloor \mu/8 \rfloor$ – целая часть результата деления μ на 8. При максимально возможном $\mu = 256$ задержка, создаваемая УКОС, составит около 1 мкс, что практически не отразится на времени доступа к данным ЖМД, которое имеет величину порядка миллисекунд.

Таким образом, решена шестая задача диссертационного исследования.

В **заключении** приведены основные результаты диссертационного исследования. В **приложениях** приведены: структурная схема модулей УПО, результаты математических экспериментов, сведения об интерфейсе IDE, алгоритм работы УКОС, функциональные схемы его узлов, списки флагов условий микропрограммы и управляющих сигналов БУ, оценки аппаратной сложности и быстродействия УКОС при его реализации на ПЛИС, акты о внедрении.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

В диссертации решена актуальная научно–техническая задача разработки быстродействующих аппаратных средств контроля обращений к секторам жёсткого магнитного диска (ЖМД), обеспечения достоверности кодов атрибутов секторов и повышения обнаруживающей способности разработанных средств по сравнению с известными программными и аппаратными системами контроля обращений (СКО). Получены следующие результаты:

Выполнена оценка аппаратной сложности устройства, которая составила 1014 слайсов и 265 блоков ввода–вывода при реализации устройства на микросхеме ПЛИС xc2s300e–7–fg456 фирмы Xilinx. Коды атрибутов секторов, микропрограмма блока управления и

1. Созданы способы аппаратного контроля обращений и процедур доступа к секторам данных ЖМД, основанные на переносе функции проверки атрибутов файлов и их секторов с программного уровня ЭЦВМ на аппаратный уровень контроллера жёсткого магнитного диска (КЖМД), которые позволяют повысить быстродействие СКО, исключить в основных режимах обмена информацией с ЖМД возможность записи и чтения контролируемых файлов, своевременно обнаруживать деструктивные воздействия на данные, снижая при этом долю искажённых файлов до 0.1% от общего числа файлов диска.

2. Разработаны архитектурная организация СКО с аппаратным контролем обращений к секторам данных ЖМД, в состав которой включены аппаратное средство поддержки – устройство контроля обращений к секторам (УКОС), обслуживающее данное устройство управляющее программное обеспечение (УПО) и панель управления устройством; сформулированы принципы взаимодействия компонентов СКО друг с другом, дающие возможность управлять режимами работы УКОС, присваивать секторам задаваемые пользователем типы атрибутов, запрещать и разрешать исполнение устройством команд модификации атрибутов, организовывать оперативное и долговременное хранение кодов атрибутов, в реальном времени контролировать команды на доступ к секторам ЖМД и блокировать исполнение тех из них, которые запрещены атрибутами, передавать в УПО информацию об обращениях к контролируемым секторам.

3. Разработаны способ и процедуры организации взаимодействия УКОС и УПО, позволяющие обеспечить удобство и простоту управления УКОС; снизить трудоёмкость и стоимость модификации атрибутов секторов ЖМД за счёт использования стандартных интерфейсов ЭЦВМ; выполнять контроль процедур доступа к служебным данным УКОС, снизив за счёт этого величину вероятности искажения кодов атрибутов до 10^{-7} на один сеанс их модификации.

4. Выполнено математическое моделирование марковскими цепями с вложенными подграфами процессов функционирования УКОС в режиме информационного обмена с УПО и стандартном режиме обмена данными с ЖМД, позволившее обосновать достигаемые показатели его обнаруживающей способности, определить характеристики функций хеширования кодов команд и преобразования содержимого ключевых полей команд и выбрать целесообразные величины параметров УКОС: глубину истории команд ($r = 12$), длину ключевого поля команды УПО ($k = 13$), частоту проверки имитоприставки ($L \leq 10$).

5. Разработаны алгоритмы функционирования, структурные и функциональные схемы и проект реализации на ПЛИС вставляемого в разъём КЖМД интерфейсного УКОС с конвейерным выполнением операций формирования адресов, чтения из ОЗУ кодов атрибутов и их анализа, имеющего приемлемую для практической реализации аппаратную сложность (1014 слайсов и 265 блоков ввода-вывода ПЛИС и микросхемы ОЗУ, ПЗУ, ППЗУ), что позволило повысить быстродействие УКОС и снизить создаваемую им при работе с ЖМД задержку до величины около 1 мкс, что на три порядка меньше, чем среднее время доступа к диску.

СПИСОК ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ.

1. Таныгин, М.О. Анализ эффективности использования кодированных команд в программно – аппаратных системах [Текст] / М.О. Таныгин // Проблемы передачи и обработки информации в сетях и системах телекоммуникаций: Материалы 14-й Международной науч.–техн. конф. Рязань: РГРА, 2005. – С. 72 – 73.
2. Таныгин, М.О. Метод маркирования секторов жёсткого диска [Текст] / М.О. Таныгин // Образование, наука, производство: Сб. тез. докл. II Международного студенческого форума.– Белгород: БГТУ им. В.Г. Шухова, 2004.–С. 261.
3. Таныгин, М.О. Обнаружение вирусных атак с помощью аппаратной системы защиты файлов [Текст] / М.О. Таныгин, А.П. Типикин // Известия Курского государственного технического университета. – 2006.– №.2–С.119 – 123.
4. Таныгин, М.О. Обнаружение при программном управлении работой устройства команд, выданных посторонними программами [Текст] / М.О. Таныгин // Оптико – электронные приборы и устройства в системах распознавания образов, обработки изображений и символьной информации. Распознавание–2005: сб. матер. 7 Межд. конф. – Курск: КурскГТУ, 2005. – С. 202 – 203.
5. Таныгин, М.О. Программно – аппаратная система ограничения доступа к данным на жёстком магнитном диске и оценка её эффективности [Текст] / М.О. Таныгин, А.П. Типикин // № 1397 – В2005 от 31.10.05 в ВИНТИ.
6. Таныгин, М.О. Способ и устройство блокирования команд для ограничения доступа к записанным на носителе данным [Текст] / М.О. Таныгин, А.П. Типикин // Патент РФ № 2280890, МПК⁷ G 06 F 12/14. – № 2005101010/09; заявл. 2004.18.01; опубл. 2006.27.07, БИМП №21. – 1 с.
7. Таныгин, М.О. Способ и устройство ограничения доступа к записанным на носителе цифровым данным [Текст] / М.О. Таныгин, А.П. Типикин // Патент РФ № 2277720, МПК⁷ G 06 F 12/14, G 06 Q 90/00. – № 2004120012/09; заявл. 2004.30.06; опубл. 2006.10.06, БИМП №16. – 1 с.
8. Таныгин, М.О., Устройство ограничения доступа к информации в ЭЦВМ [Текст] / М.О. Таныгин // Проблемы передачи и обработки информации в сетях и системах телекоммуникаций: Материалы 13-й Межд. науч.– техн. конф. – Рязань: РГРА, 2004. – С. 174 – 175.
9. Типикин, А.П. Архитектура системы аппаратного ограничения доступа к информации на жестком диске ЭЦВМ [Текст] / А.П. Типикин, М.О. Таныгин // Телекоммуникации. – 2006. – №3. – С. 44 – 46.
10. Типикин, А.П. Маркирующий контроллер жёсткого диска [Текст] / А.П. Типикин, М.О. Таныгин // Известия ВУЗов. Приборостроение. – 2005. – Т.48, №2. – С.73 – 76.
11. Типикин, А.П. Методы аутентификации устройств защиты информации и управляющих программных средств [Текст] / А.П. Типикин, М.О. Таныгин // Телекоммуникации. – 2005. – №9. – С. 37 – 42.