

На правах рукописи



Глазков Александр Сергеевич

АППАРАТНЫЕ СРЕДСТВА ПОВЫШЕНИЯ
НАДЕЖНОСТИ КОНТРОЛЯ ОБРАЩЕНИЙ К
ДАННЫМ ВО ВНЕШНЕЙ ПАМЯТИ ЭВМ

05.13.05 – Элементы и устройства вычислительной техники и
систем управления,

05.13.19 – Методы и системы защиты информации,
информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание учёной степени
кандидата технических наук

КУРСК – 2012

Работа выполнена в Юго-Западном государственном университете.

Научный руководитель: доктор технических наук, профессор,
Типикин Александр Петрович

Официальные оппоненты: *Фисун Александр Павлович*
доктор технических наук, профессор,
филиал «Радиочастотный центр
Центрального федерального округа»
(г. Орел),
заместитель директора.

Фисенко Виктор Евгеньевич
кандидат технических наук, доцент,
«Государственный университет –
учебно-научно-производственный
комплекс» (г. Орел),
доцент кафедры «Информационные
системы».

Ведущая организация: Тульский государственный
университет

Защита состоится 16 марта 2012 г. в 14:00 часов в конференц-зале на заседании
диссертационного совета Д 212.105.02 при Юго-Западном государственном
университете по адресу: 305040, г. Курск, ул. 50 лет Октября, 94.

С диссертацией можно ознакомиться в библиотеке Юго-Западного
государственного университета по адресу: 305040, г. Курск, ул. 50 лет Октября, 94.

Автореферат разослан 14 февраля 2012 г.

Ученый секретарь
диссертационного совета Д 212.105.02



Е.А. Титенко

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность работы. Контроль обращений к данным во внешней памяти выполняется в современных ЭВМ на программном уровне. Надежность работы известной системы ограничения несанкционированного доступа (СОНД) недостаточна, так как коды атрибутов доступа к файлам могут модифицироваться деструктивными программами или в результате сбоев, а деструктивные программы, кроме этого, могут получать прямой доступ к секторам данных, минуя СОНД.

Надежность и быстродействие СОНД можно существенно повысить, если ее дополнить аппаратным уровнем контроля обращений к секторам файлов в контроллере накопителя информации. С помощью специализированного устройства контроля и ограничения доступа (УКОД) организуется долговременное хранение на аппаратном уровне кодов атрибутов доступа к секторам данных, обнаруживаются случаи обхода деструктивными программами основной программной СОНД, своевременно предотвращаются атаки на файловую систему и повышается надежность хранения файлов вплоть до полного закрытия любых видов доступа без ведома легитимного пользователя, в том числе из-за случайных обращений, вызванных сбоями и отказами ЭВМ или ошибками пользователя.

Известны два основных способа введения УКОД в состав накопителя информации: 1) включение УКОД между интерфейсным шлейфом и разъемом контроллера накопителя; 2) встраивание УКОД непосредственно в контроллер. По первому способу коды атрибутов доступа к секторам долговременно хранятся в накопителе в специальном ограниченном по доступу файле, а в рабочем режиме ЭВМ переписываются в оперативную память интерфейсного УКОД и используются для контроля обращений к секторам данных. По второму способу коды атрибутов постоянно хранятся в накопителе в специальном поле сектора записи как служебные данные, а при обращении к сектору вначале считывается код его атрибута и сразу же по нему производится контроль команды ЭВМ и принимается решение о запрещении или разрешении задаваемых командой операций контроллера над полем данных сектора.

Интерфейсное УКОД эффективно при контроле обращений к секторам в современных накопителях на жестких магнитных дисках (ЖМД). Однако в связи с существенным увеличением емкости памяти перспективных накопителей выявлены следующие недостатки интерфейсного УКОД: 1) непомерное возрастание требуемой емкости встроенной в УКОД оперативной памяти; 2) невозможность по той же причине увеличения числа типов атрибутов доступа; 3) принципиальная невозможность использования его для контроля обращений при хищении накопителя информации. Они могут быть преодолены, если в перспективных накопителях большой емкости перейти ко второму способу введения УКОД и реализовать его в составе блоков контроллера накопителя, как встраиваемое УКОД.

На аппаратном уровне с помощью встраиваемого УКОД сравнительно просто физически заблокировать возможность программно-управляемой модификации кодов атрибутов доступа к секторам в основном режиме обмена данными между ЭВМ и накопителем и тем самым достичь высокой достоверности контроля обращений. В то же время для снижения трудоемкости и стоимости модификации

атрибутов доступа к секторам целесообразно использовать стандартные интерфейсы и монитор ЭВМ, а для автоматизации ввода кодов атрибутов в УКОД создать специализированное управляющее программное обеспечение. Поэтому в эпизодических режимах модификации атрибутов потребуются снимать в УКОД физическую блокировку их программно-управляемого изменения, а вероятность правильного функционирования УКОД повышать дополнительными аппаратными средствами.

Кроме того, из-за высокой стоимости информации, похищаемой совместно с конструктивным модулем накопителя большой емкости, требуется создание специальной программно-аппаратной подсистемы, позволяющей закрывать доступ к данным, накопленным во внешней памяти ЭВМ. Встраиваемое в контроллер УКОД, похищаемое в составе накопителя, имеет принципиальную возможность во взаимодействии со специальными программными и идентифицирующими средствами, хранящимися на внешнем флэш-носителе только у легитимного пользователя ЭВМ, проконтролировать обращения к секторам данных в похищенном носителе.

В связи с вышеизложенным актуальной является **научно-техническая задача** повышения надежности аппаратного контроля обращений и ограничения доступа к секторам данных накопителя информации.

Объектом исследования является специализированное устройство контроля и ограничения доступа к информации, накопленной во внешней памяти ЭВМ.

Предметом исследования являются алгоритмы и схемы устройства, встраиваемого в контроллер накопителя информации для повышения надежности работы системы контроля и ограничения доступа к секторам файлов.

Диссертационная работа выполнена в совместной научно-исследовательской лаборатории Центра информационных технологий в проектировании РАН и Юго-Западного государственного университета: «Информационные распознающие телекоммуникационные интеллектуальные системы».

Целью работы является повышение надежности контроля обращений и ограничения доступа к секторам данных накопителя информации путем разработки методов, алгоритмов и устройства контроля и ограничения доступа к секторам файлов на аппаратном уровне контроллера.

Для достижения поставленной цели в работе решены следующие **основные задачи**:

1. Анализ известных методов и аппаратных средств повышения надежности работы системы ограничения доступа к информации, накопленной во внешней памяти ЭВМ.
2. Разработка способа встраивания в контроллер накопителя устройства контроля и ограничения доступа (УКОД) к секторам файлов для повышения надежности и скорости работы системы контроля и ограничения доступа.
3. Разработка способа и функциональной организации программно-аппаратных средств извлечения метаданных описания разделов накопителя информации.

4. Разработка архитектуры программно-аппаратной пользовательской системы контроля и ограничения доступа к информации, накопленной во внешней памяти ЭВМ. Определение требований к специализированным аппаратным и программным средствам системы контроля.

5. Разработка метода, алгоритмов и аппаратных средств повышения надежности работы УКОД в режиме программно-управляемой модификации атрибутов доступа к секторам.

6. Разработка алгоритмов функционирования, структурных и функциональных схем встраиваемого УКОД. Определение достигнутой степени повышения надежности работы УКОД.

Научная новизна и положения, выносимые на защиту:

1. Аппаратно-ориентированный способ контроля обращений к данным во внешней памяти, основанный на хранении кодов атрибутов в служебных полях в конце заголовка каждого сектора накопителя информации, что позволяет по сравнению с интерфейсным УКОД существенно снизить объем оперативной памяти и осуществлять контроль чтения/записи полей данных при поиске секторов в режиме реального времени (п.2 паспорта 05.13.05).

2. Способ извлечения метаданных из магнитного жесткого диска, позволяющий снизить вероятность несанкционированного считывания данных при хищении накопителя информации (п.13 паспорта 05.13.19).

3. Организация аппаратно-программных специализированных средств ограничения доступа, отличающаяся введением портативной памяти и разграничением хранения критически важной информации (загрузочный код, таблица описания разделов, ключевые записи метаданных файловой системы) для доступа к данным, что позволяет повысить надежность контроля обращений к внешней памяти ЭВМ (п.4 паспорта 05.13.05).

4. Метод, алгоритмы и аппаратные средства УКОД проверки подлинности команд ЭВМ, отличающиеся применением алгоритмов скремблирования исходной кодовой последовательности и позволяющие снизить вероятность несанкционированного изменения кодов атрибутов доступа к секторам и тем самым повысить достоверность контроля обращений к секторам файлов (п.13 паспорта 05.13.19).

5. Алгоритмы функционирования, структурные и функциональные схемы встраиваемого УКОД, основанные на разработанных методах, отличающиеся конвейерной организацией процедур анализа считываемых из накопителя кодов атрибутов доступа к секторам и блокирования операций чтения/записи их полей данных, и позволяющие повысить надежность работы системы контроля и ограничения несанкционированного доступа в современных ЭВМ (п.4 паспорта 05.13.05).

Практическая ценность результатов работы заключается в следующем:

1. Разработаны схема размещения устройства контроля и ограничения доступа (УКОД) в контроллере накопителя на жестких магнитных дисках (НЖМД) без изменения его схем и без вмешательства в алгоритмы его работы, позволяющая по сравнению с интерфейсным УОД уменьшить объем оперативной памяти в 10^3 раз и необходимость больших затрат времени на перезапись кодов атрибутов секторов

из накопителя в УОД и обратно, а также использовать аппаратные средства УКОД для предотвращения несанкционированного доступа к секторам данных. Разработана архитектура программно-аппаратной системы контроля и ограничения доступа.

2. Произведена оценка скорости выполнения операций контроля устройством УКОД, которая определяется затратами времени на анализ атрибута доступа и принятие решения о блокировании управляющих стробов в режиме чтения, сниженными до 7,5 нс на сектор.

3. Разработанный метод программно-аппаратной проверки подлинности команд ЭВМ в режиме программно-управляемой модификации кодов атрибутов доступа к секторам позволяет снизить вероятность несанкционированного изменения атрибутов до $2,4 \times 10^{-7}$ за сеанс их модификации и тем самым повысить надежность работы системы контроля и ограничения доступа в 10^6 раз по сравнению с программной реализацией системы ограничения несанкционированного доступа (СОНД) и примерно в 10 раз по сравнению с известным интерфейсным УКОД.

4. Число файлов, пораженных деструктивными программами, может быть снижено в сто раз, если доля файлов, контролируемых устройством УКОД, составляет более 70%. Максимальная надежность их хранения может быть достигнута, если долю защищенных файлов повысить до 100%, а ошибочную попытку доступа пользователя, прошедшего авторизацию, разрешать с нарушением прав однократно только в режиме чтения.

5. Разработанный способ извлечения с носителя информации основных записей метаданных и защиты управляющего программного обеспечения позволяет снизить вероятность восстановления пользовательских данных злоумышленником и повысить достоверность контроля обращений к секторам файлов.

Реализация и внедрение. Результаты диссертационного исследования внедрены в ООО «Сайнер» с целью соблюдения режимов секретности и коммерческой тайны в компьютерной системе управления базой знаний, содержащей техническую и финансовую документацию по проектам компании, а также используются в учебном процессе кафедры ВТ Юго-Западного государственного университета в дисциплинах «Технические средства защиты и сжатия информации» и «Методы и средства защиты компьютерной информации», что подтверждается соответствующими актами.

Соответствие паспорту специальности. Содержание диссертации соответствует п.4 «Разработка научных подходов, методов, алгоритмов и программ, обеспечивающих надежность, контроль и диагностику функционирования элементов и устройств вычислительной техники и систем управления» паспорта специальности 05.13.05 – Элементы и устройства вычислительной техники и систем управления, а также п.13 «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности» паспорта специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Апробация работы. Основные положения диссертационной работы докладывались и получили положительную оценку на региональных, Российских и международных конференциях: I Всероссийская научно-техническая конференция «Информтех 2008» (Курск, 2008); Всероссийская научно-техническая конференция «Интеллект 2009» (Тула, 2009); Всероссийская научно-техническая конференция «Интеллект 2011» (Тула, 2011); IX Международная конференция «Распознавание 2010» (Курск, 2010); III ежегодная международная научно-практическая конференция «Перспективы развития информационных технологий» (Новосибирск, 2011); Международная научная конференция «Теоретические и практические аспекты научных исследований» (Украина, Киев, 2011), а также на научных семинарах кафедры вычислительной техники ЮЗГУ с 2007 по 2011 гг.

Публикации. По результатам диссертационной работы опубликовано 12 печатных работ, из них 3 в рецензируемых научных журналах и изданиях, 1 патент на изобретение (№2359317). Список основных публикаций приведен в конце автореферата.

Личный вклад автора. Все выносимые на защиту результаты получены автором лично. В работах, опубликованных в соавторстве и приведенных в конце автореферата, в [1,3,6,7,9] автором предложена и описана архитектура системы ограничения несанкционированного доступа; в работе [12] – структурно-функциональная организация устройства контроля и ограничения доступа и функциональная схема блока анализа команд; в работах [1,3,5,7,8,12] – метод проверки подлинности команд выдаваемых управляющим программным обеспечением устройству контроля и ограничения доступа; в работах [2,7] – метод извлечения метаданных устройства хранения данных; в работе [2] – технологическая схема извлечения метаданных устройства хранения данных; в работе [9] – способ повышения скорости выполнения критичных по времени операций устройством контроля и ограничения доступа к файлам; в работе [10] – математическое моделирование работы устройства контроля и ограничения доступа; в работе [4] доработана структурно-функциональная организация устройства проверки кодированных команд и хранения истории команд; в работе [11] – структура управляющего программного обеспечения системы контроля и ограничения доступа.

Объем и структура работы. Диссертационная работа состоит из введения, 4 глав, заключения, списка литературы из 89 источников и 5 приложений. Работа содержит 156 страниц машинописного текста, 41 рисунок, 4 таблиц.

Области возможного использования. Созданные способы, процедуры и устройство повышения надежности системы контроля и ограничения доступа к секторам могут быть применены в аппаратных системах контроля периферийных устройств ЭЦВМ, системах управления базами данных и в системах ограничения доступа к информации.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы, сформулированы цели и задачи работы, научная новизна и практическая ценность полученных результатов, представлена структура диссертации и основные положения, выносимые на защиту.

В первой главе приведены сведения о видах угроз для долговременно хранящихся в ЭВМ данных и средствах борьбы с ними. Программные средства ограничения доступа более распространены, чем аппаратные, однако они не дают гарантии предотвращения несанкционированного доступа к данным и своевременного его обнаружения. Проведен сравнительный анализ существующих аппаратных систем ограничения несанкционированного доступа (СОНД), работа большинства из которых основывается на шифровании защищаемых данных, что ограничивает доступ к ним только по чтению, не защищая их от повреждения со стороны деструктивных программ, что делает их неприменимыми в ЭВМ, где хранится ценная информация, существующая в одном экземпляре. Также рассмотрены аппаратные модули доверенной загрузки («Соболь», «Аккорд»), обеспечивающие контроль целостности технических и программных средств ЭВМ до загрузки операционной системы. Недостатком таких модулей является принципиальная невозможность закрытия доступа к похищаемому носителю информации, высокая аппаратная сложность и отсутствие контроля обращений к накопителю после загрузки операционной системы.

Надежную защиту могут гарантировать дополнительные аппаратные средства контроля, встраиваемые в систему контроля и ограничения доступа (СКОД) компьютера и используемые в качестве ядра безопасности системы ограничения доступа к данным ЭВМ.

Предложены меры по повышению надежности и скорости работы системы СКОД, к которым относятся: 1) ограничение доступа к информации, хранимой на внешнем носителе ЭВМ, целесообразно выполнять на основе присвоения отдельным секторам данных специальных атрибутов доступа; 2) контроль и ограничение доступа необходимо производить на аппаратном уровне; 3) управляющему программному обеспечению отводится только роль выдачи команд для установки/изменения атрибутов доступа секторов; 4) доступ к защищённым секторам и модификация атрибутов доступа может осуществляться только при наличии соответствующего разрешающего сигнала от легитимного пользователя; 5) для выполнения контроля обращений к секторам в реальном времени, а также для повышения надежности ограничения доступа к секторам файлов, устройство контроля и ограничения доступа необходимо встроить непосредственно в контроллер внешней памяти ЭВМ; 6) необходима аппаратная реализация проверки подлинности команд, выдаваемых управляющим программным обеспечением.

Во второй главе разработана архитектура программно-аппаратной СКОД, позволяющая без изменения существующих программных и технических средств ЭВМ, путем встраивания в контроллер НЖМД дополнительной микросхемы устройства УКОД и дополнения системного программного обеспечения ЭВМ утилитами и драйвером управления названным устройством с высокой вероятностью обнаружения средствами аппаратного контроля случаев обхода деструктивными программами имеющейся в ЭВМ программной системы ограничения доступа и повышения степени защиты файлов вплоть до полного закрытия доступа к ним без ведома легитимного пользователя и администратора (Рис. 1).

На аппаратном уровне достаточно просто физически заблокировать возможность программно-управляемой модификации кодов атрибутов доступа к секторам в основном режиме обмена данными между ЭВМ и НЖМД. Для хранения кода атрибута предлагается использовать служебное поле в конце заголовка каждого сектора ЖМД в отдельности. В режиме поиска сектора выполняются считывание и анализ его атрибута, а также контроль и принятие решения по защите до чтения/записи поля данных. Такой способ обеспечивает существенное уменьшение требуемого объема оперативной памяти устройства УКОД и достаточно надежное долговременное хранение кодов атрибутов.

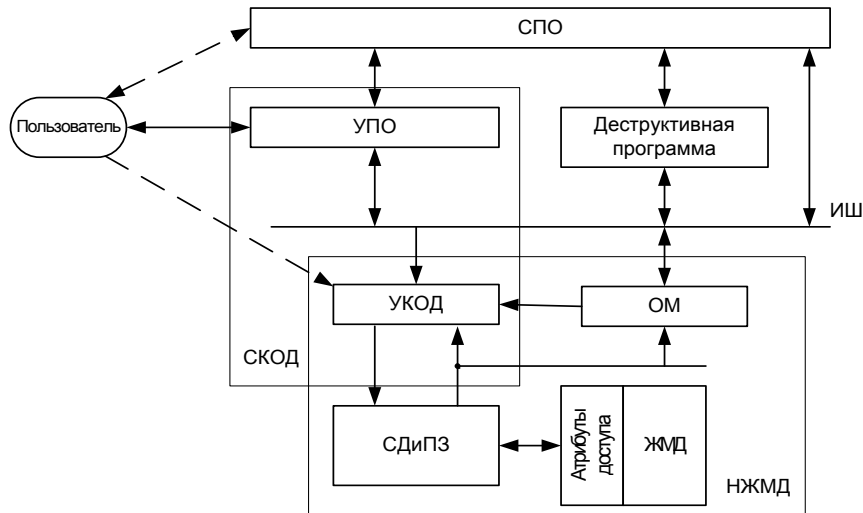


Рис. 1. Архитектура СКОД,

СПО – системное программное обеспечение; ОМ – однокристалльная микроЭВМ; СДиПЗ – сепаратор данных и предкомпенсация записи; ИШ – интерфейсная шина ЭВМ

Автоматизация преобразования файловых атрибутов в секторные и ввода их в УКОД выполняется специализированным управляющим программным обеспечением (УПО) (Рис. 1). К основным задачам УПО относятся: 1) получение команд от пользователя и трансляция их в команды, понятные аппаратной компоненте; 2) получение состояния аппаратной компоненты и представление этой информации в виде, удобном для восприятия пользователем; 3) контроль доступа к защищаемым секторам. УПО разделено на два подмножества: первое подмножество выполняется до начала работы основной ОС и предназначено для проведения процедуры подготовки и настройки СКОД, авторизации пользователя в СКОД; второе подмножество выполняется после загрузки основной ОС и предназначено для проведения процедур контроля, установки, снятия и модификации атрибутов доступа к файлам. Первое подмножество УПО выполняется до загрузки основной ОС и построено на базе более простой альтернативной ОС. Для хранения альтернативной ОС, первого подмножества УПО и дополнительных данных, необходимых для выполнения процедуры авторизации, используется портативный носитель информации, в качестве которого выбрано устройство флэш-памяти с интерфейсом подключения USB. Были разработаны способы защиты УПО от атак злоумышленников, в результате чего была повышена надежность управления СКОД.

Разработан способ извлечения метаданных из носителя НЖМД, позволяющий снизить вероятность восстановления пользовательских данных злоумышленником, получившим доступ к накопителю информации. Способ заключается в выполнении следующих операций: 1) извлечение основной загрузочной записи MBR; 2) извлечение структур описания вторичных разделов SMBR и сохранение адресов их секторов; 3) извлечение ключевых записей файловых систем и сохранение адресов их секторов; 4) сохранение серийного номера производителя ЖМД, хранящегося в его паспорте, для определения УПО именно того носителя, которому принадлежат извлекаемые метаданные.

Расчет объема извлекаемых метаданных V_{MD} может быть выполнен по формуле:

$$V_{MD} = V_{MBR} + n_{SMBR} \cdot V_{SMBR} + n_{FS} \cdot V_{FS} + (n_{SMBR} + n_{FS}) \cdot V_{SS} + V_{IDHDD}, \quad (1)$$

где V_{MBR} – объем, занимаемый MBR; n_{SMBR} – количество вторичных разделов; V_{SMBR} – объем, занимаемый SMBR; n_{FS} – количество разделов с файловыми системами (ФС); V_{FS} – объем, занимаемый служебными записями метаданных ФС; V_{SS} – размер адреса сектора; V_{IDHDD} – размер идентификатора НЖМД.

Результаты расчетов по формуле (1) для НЖМД, имеющего 3 расширенных раздела и 5 разделов NTFS, показали, что объем метаданных, извлекаемых с диска и переносимых на другой внешний портативный носитель, составляет около 140 Кбайт, что является несущественным по сравнению с емкостью современных портативных носителей информации на флэш-памяти.

На Рис. 2 представлена организация аппаратно-программных специализированных средств извлечения метаданных.



Рис. 2. Организация аппаратно-программных специализированных средств извлечения метаданных

Разработан метод повышения надежности работы СКОД путем применения специальных кодированных команд ЭВМ для устройства контроля (УКОД) во время программно-управляемой модификации атрибутов доступа. Для уменьшения вероятности исполнения УКОД ложных команд деструктивных программ в состав команды УПО вводится специальное поле «Ключ» (Рис. 3):

Код операции	«Ключ»
--------------	--------

Рис. 3. Формат команды

Программно-управляемая модификация атрибутов доступа легитимным пользователем начинается с отправки устройству дополнительной начальной команды «Старт». Поле «Ключ» этой команды «Старт» является кодовой последовательностью, содержащей коэффициенты полинома скремблирования (КПС), которые записываются в специальный регистр УКОД и используются в нем для преобразования полей «Ключ» следующих после команды «Старт» команд УПО. Команды, выдаваемые из УПО в устройство после команды «Старт», имеют формат поля «Ключ», представленный на Рис. 4.

А	В
Счет скремблированный	КЧЦК

Рис. 4. Формат поля «Ключ» команд УПО, следующих за командой «Старт»,
КЧЦК – контрольная часть циклического избыточного кода

Для кодирования и проверки команд в УПО используются следующие алгоритмы скремблирования и вычисления контрольной части циклического избыточного кода (КЧЦК).

Исходную n -разрядную скремблируемую последовательность представим двоичным вектором:

$$A = (a_0, a_1, \dots, a_k, \dots, a_{n-1}), a_k \in \{0,1\}.$$

Двоичные коэффициенты КПС также отобразим компонентами двоичного вектора:

$$D = (d_0, d_1, \dots, d_k, \dots, d_{n-1}), d_k \in \{0,1\}.$$

Деформированный промежуточный вектор кодированной последовательности B_j , получаемый на j -ом шаге скремблирования и используемый для формирования j -го бита b_j результирующей последовательности, представим в виде:

$$B_j = (b_0, b_1, \dots, b_{j-1}).$$

Значение j -го бита b_j результирующей последовательности $B_{j+1} = (b_0, b_1, \dots, b_{j-1}, b_j)$ вычисляется как:

$$b_j = \left(a_j + \sum_{k=0}^{j-1} b_k \cdot d_{j-k} \right) (\text{mod } 2), j = \overline{0, n-1}.$$

Обратное преобразование при дескремблировании выполняется аналогично. Если деформированный вектор представим в виде:

$$B_j = (b_0, b_1, \dots, b_{j-1}),$$

а в качестве результата будем накапливать последовательность вида:

$$C_j = (c_0, c_1, \dots, c_{j-1}),$$

то j -ый бит c_j вычисляется как:

$$c_j = \left(b_j + \sum_{k=0}^{j-1} b_k \cdot d_{j-k} \right) (\text{mod } 2), j = \overline{0, n-1}.$$

Данный принцип скремблирования и дескремблирования использован при формировании и проверке содержимого поля «Ключ» (Рис. 4).

Пусть S_i – содержимое поля «Ключ» следующей команды, выданной из УПО в УКОД. В СКОД выполняются следующие преобразования:

В УПО:

$$C_i^{(УПО)} = C_{i-1}^{(УПО)} + 1,$$

$$S_{Ai} = F_C(S_{A0}, C_i^{(УПО)}),$$

$$S_{Bi}^{(УПО)} = F_0(P^n, S_{Ai});$$

В УКОД:

$$C_i^{(DC)} = F_{DC}(S_{A0}, S_{Ai}),$$

$$S_{Bi}^{(УКОД)} = F_0(P^n, C_i^{(DC)});$$

где F_C, F_{DC}, F_0 – преобразования слова S_i ; $C_i^{(УПО)}$ – номер текущей команды УПО; S_{A0} – содержимое подполя А (коэффициенты полинома скремблирования) команды «Старт» S_0 ; S_{Ai} – содержимое подполя А (скремблированный номер текущей команды) поля «Ключ» команды S_i ; $S_{Bi}^{(УПО)}$ – содержимое подполя В поля «Ключ» команды S_i : КЧЦК, вычисленный в УПО по номеру $C_i^{(УПО)}$ текущей команды S_i ; P^n – полином степени n . В устройстве используется полином протокола CRC-5-USB: $P(x) = x^5 + x^2 + 1$; $C_i^{(DC)}$ – дескремблированный в УКОД номер текущей команды УПО S_i , подсчитанный в УПО и переданный в УКОД в скремблированном виде; $S_{Bi}^{(УКОД)}$ – КЧЦК, вычисленный в УКОД по дескремблированному номеру $C_i^{(DC)}$ текущей команды S_i .

Выданная команда исполнится, если для S_i будут верными при $i > 1$ следующие равенства:

$$\begin{cases} S_{Bi}^{(УПО)} = S_{Bi}^{(УКОД)}, \\ C_i^{(DC)} = C_{i-1}^{(УКОД)} + 1, \end{cases} \quad (2)$$

где $C_{i-1}^{(УКОД)}$ – номер команды, записанный в УКОД на $(i-1)$ шаге.

Номер команды, формируемый в УКОД на i -ом шаге, будет равен:

$$C_i^{(УКОД)} = \begin{cases} C_{i-1}^{(УКОД)} + 1, & \text{если } i > 1 \text{ и равенство (2) выполняется,} \\ C_{i-1}^{(УКОД)}, & \text{если } i > 1 \text{ и равенство (2) не выполняется,} \\ C_0, & \text{если } i = 1, \end{cases}$$

где C_0 – начальный номер последовательности команд, задаваемый в УПО.

Программное моделирование описанных процедур контроля показало, что выбранный метод скремблирования обеспечивает корректное кодирование/декодирование данных и исключает появление дубликатов среди скремблированных последовательностей. Разработанный метод кодирования команд позволил снизить вероятность несанкционированной модификации атрибутов доступа в интервале времени между командами «Старт» и «Финиш» до $2,4 \times 10^{-7}$.

В третьей главе производится оценка основных параметров надежности работы системы контроля и ограничения доступа. Интенсивность отказов всех комплектующих элементов устройства контроля и ограничения доступа (УКОД) равна $4,26 \times 10^{-7}$ 1/ч и соответствует вычисленной величине вероятности незамеченной несанкционированной модификации атрибутов доступа к секторам ЖМД при вскрытых алгоритмах преобразований ключевой информации, равной $2,4 \times 10^{-7}$ за сеанс их программно-управляемой модификации. Тем самым, надежность работы создаваемой аппаратной системы контроля и ограничения доступа повышена в 10^6 раз по сравнению с существующей ее программной реализацией и примерно в 10 раз по сравнению с известным интерфейсным УКОД.

Выполнено математическое моделирование функционирования УКОД цепью Маркова в режиме контроля и ограничения доступа. Найденная в результате моделирования зависимость количества пораженных файлов (N_{II}) от относительной доли контролируемых файлов (D) и порога (ρ) обнаружения деструктивных программ (ДП) представлена на Рис. 5, где порог ρ соответствует поглощающему состоянию цепи Маркова, наступающему в случае обращения ДП к ρ файлам.

В результате математического моделирования установлено, что число файлов, пораженных деструктивными программами, может быть снижено в сто раз, если доля файлов, контролируемых устройством УКОД, составляет более 70%. Максимальная надежность их хранения может быть достигнута, если долю защищенных файлов повысить до 100%, а ошибочную попытку доступа пользователя, прошедшего авторизацию, разрешать однократно только в режиме чтения.

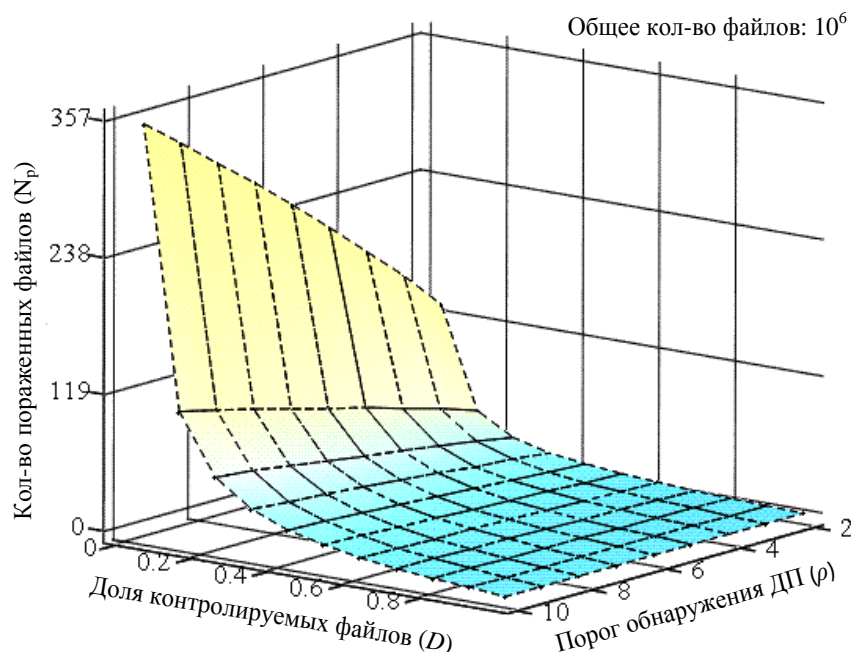


Рис. 5. Зависимость числа пораженных файлов (N_{II}) от относительной доли контролируемых файлов (D) и порога обнаружения ДП (ρ)

Четвертая глава посвящена разработке структурной и функциональной организации устройства аппаратного контроля и ограничения доступа (УКОД). Определены основные функции устройства УКОД, встраиваемого в контроллер

внешнего накопителя информации. Разработаны алгоритм работы, структурные и функциональные схемы УКОД и всех его блоков.

Структурная схема размещения устройства УКОД в контроллере носителя информации на ЖМД показана на Рис. 6.

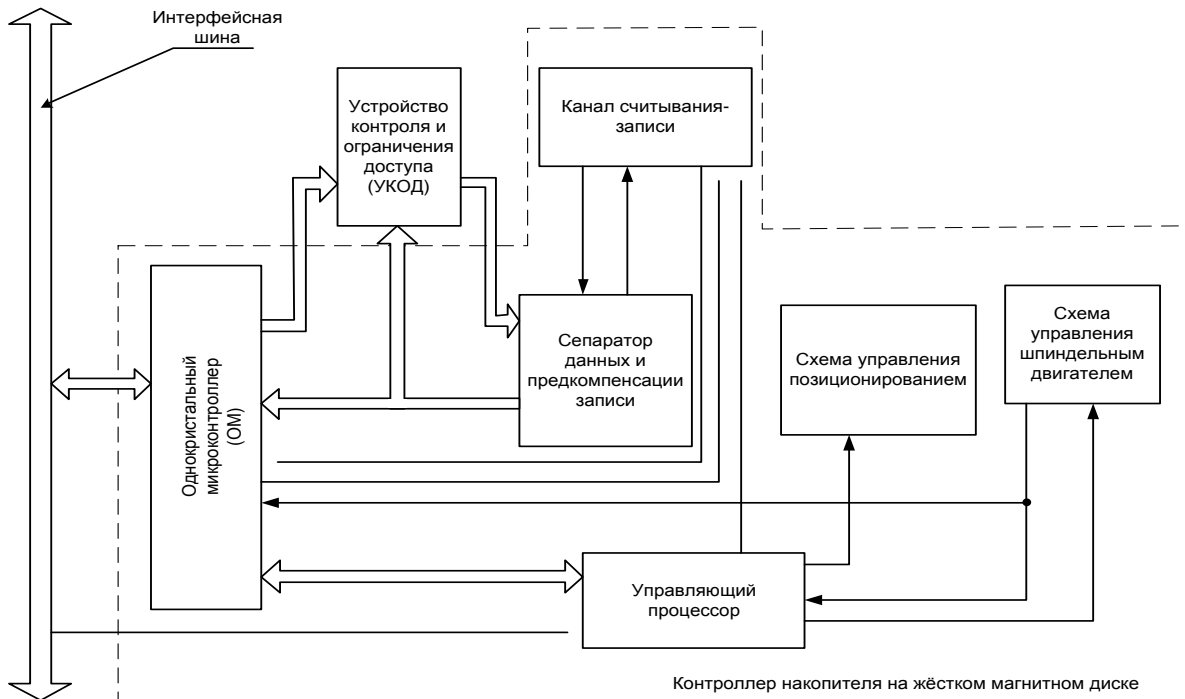


Рис. 6. Схема размещения устройства контроля в контроллере носителя информации на жестких магнитных дисках (ЖМД)

Устройство УКОД подключается к внутренним линиям контроллера жесткого диска таким образом, чтобы иметь возможность выполнения описанных выше процедур контроля и управления процессом обращения к секторам носителя информации без вмешательства в алгоритмы работы остальных частей контроллера ЖМД.

Модифицированный формат сектора накопителя на жестком магнитном диске представлен на Рис. 7. Обращение к секторам контролируется устройством (УКОД) путем проверки кода атрибута доступа.

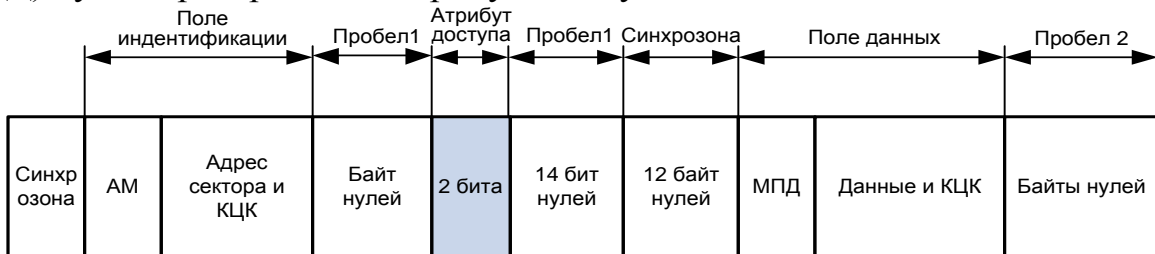


Рис. 7. Формат сектора накопителя на жестких магнитных дисках (НЖМД),
АМ – адресный маркер, МПД – маркер поля данных, КЦК – контрольно-циклический код

Код атрибута доступа записывается в конце заголовка сектора (Рис. 7) и обрабатывается устройством контроля и ограничения доступа.

В известном интерфейсном устройстве ограничения доступа ёмкость оперативной памяти равна: $V_{OЗУ} = V_{ЖМД} / 2024$, где $V_{ЖМД}$ – емкость ЖМД. Таким

образом, для контроля всех данных хранящихся на ЖМД емкостью 2 ТБ потребуется оперативная память емкостью 1 ГБ, что в 10^3 раз больше емкости оперативной памяти (512 КБ) используемой в разработанном устройстве.

Разработан обобщенный алгоритм работы устройства УКОД (Рис. 8) в режиме контроля и ограничения доступа:

1. Проверить, выполняется ли запись в регистр команд 1F7h. Если да, то перейти к п.2, если нет – перейти к п. 1.
2. Проверить содержимое регистра 1F7h. Если происходит авторизация пользователя (1F7h[7:0] = 4Ch), то перейти к п.3, иначе перейти к п.5.
3. По переданной паре «идентификатор-пароль» считать из ППЗУ УКОД учетную запись пользователя. Если учетная запись не найдена, присвоить текущему пользователю права «обычный пользователь» и перейти к п.5, иначе перейти к п.4.
4. По считанной учетной записи определить тип текущего пользователя (пользователь СКОД/администратор СКОД) и применить соответствующие права. Перейти к п.5.
5. Проверить содержимое регистров адреса 1F3h, 1F4h, 1F5h и 1F6h. Если происходит обращение к загрузочному сектору (1F3h[7:0] = 00000001b, 1F6h[7:0] = XXXX0000b, 1F3h[7:0] = 00000000b, 1F4h[7:0] = 00000000b), то перейти к п.6, если нет – перейти к п.7.
6. Считать данные MBR из внутреннего ОЗУ УКОД и передать по линии RD в ОМ. Перейти к п.7.
7. Проверить содержимое регистра команд 1F7h. Если происходит запись метаданных с внешнего портативного накопителя пользователя в УКОД (1F7h[7:0] = 46h), то перейти к п.8, иначе перейти к п.9.
8. Записать во внутреннее ОЗУ УКОД данные с линии RD от ОМ и перейти к п.9.
9. Проверить содержимое регистра команд 1F7h. Если происходит считывание/запись с/в ЖМД (1F7h[7:0] = 4Eh/4Fh), то перейти к п.10, иначе перейти к п.21.
10. Активировать схему чтения данных с линии RD и перейти к п.11.
11. Выделить из потока считываемых данных идентификатор текущего сектора, код атрибута доступа, если он присутствует, сформировать флаг о завершении поиска позиции атрибута доступа. Перейти к п.12.
12. Передать считанный идентификатор сектора в схему сравнения адреса и перейти к п.13.
13. Сравнить считанный идентификатор с идентификатором, хранящимся в группе регистров портов. Если идентификаторы совпадают, то перейти к п.14, иначе перейти к п.11.
14. Если происходит модификация атрибутов доступа, то перейти к п.15, иначе перейти к п.17.
15. Активировать схему записи атрибута доступа и перейти к п.16.
16. Выдать на линию WD код атрибута доступа, хранящийся в группе триггеров флагов и перейти к п.17.
17. Активировать подсистему блокирования стробов записи/чтения и перейти к п.18.
18. Если происходит модификация атрибута доступа, то перейти к п.19, иначе перейти к п.20.

19. Активировать строб записи WG и перейти к п.21.
20. Проанализировать права текущего пользователя, выполняемую операцию и считанный код атрибута доступа и принять решение об блокировании/разблокировании соответствующего строга (RG\WG). Перейти к п.21.
21. Проверить содержимое регистра команд 1F7h. Если запрашивается слово состояния УКОД ($1F7h[7:0] = 44h$), то перейти к п.22, иначе перейти к п.23.
22. Сформировать и передать по линии RD в ОМ слово состояния УКОД. Перейти к п.23.
23. Проверить содержимое регистра команд 1F7h. Если происходит модификация атрибутов доступа ($1F7h[7:0] = 48h/49h/4Ah/4Bh$), то сформировать код атрибута доступа, соответствующий коду пришедшей команды, сохранить его в группе триггеров флагов и перейти к п.24.
24. Активировать блок анализа команд и перейти к п.25.
25. Проверить подлинность команды модификации атрибута доступа по дополнительному кодовому полю. Если команда подлинна, то перейти к п.10, иначе сформировать и передать по линии RD в ОМ слово состояния УКОД и перейти к п.1.

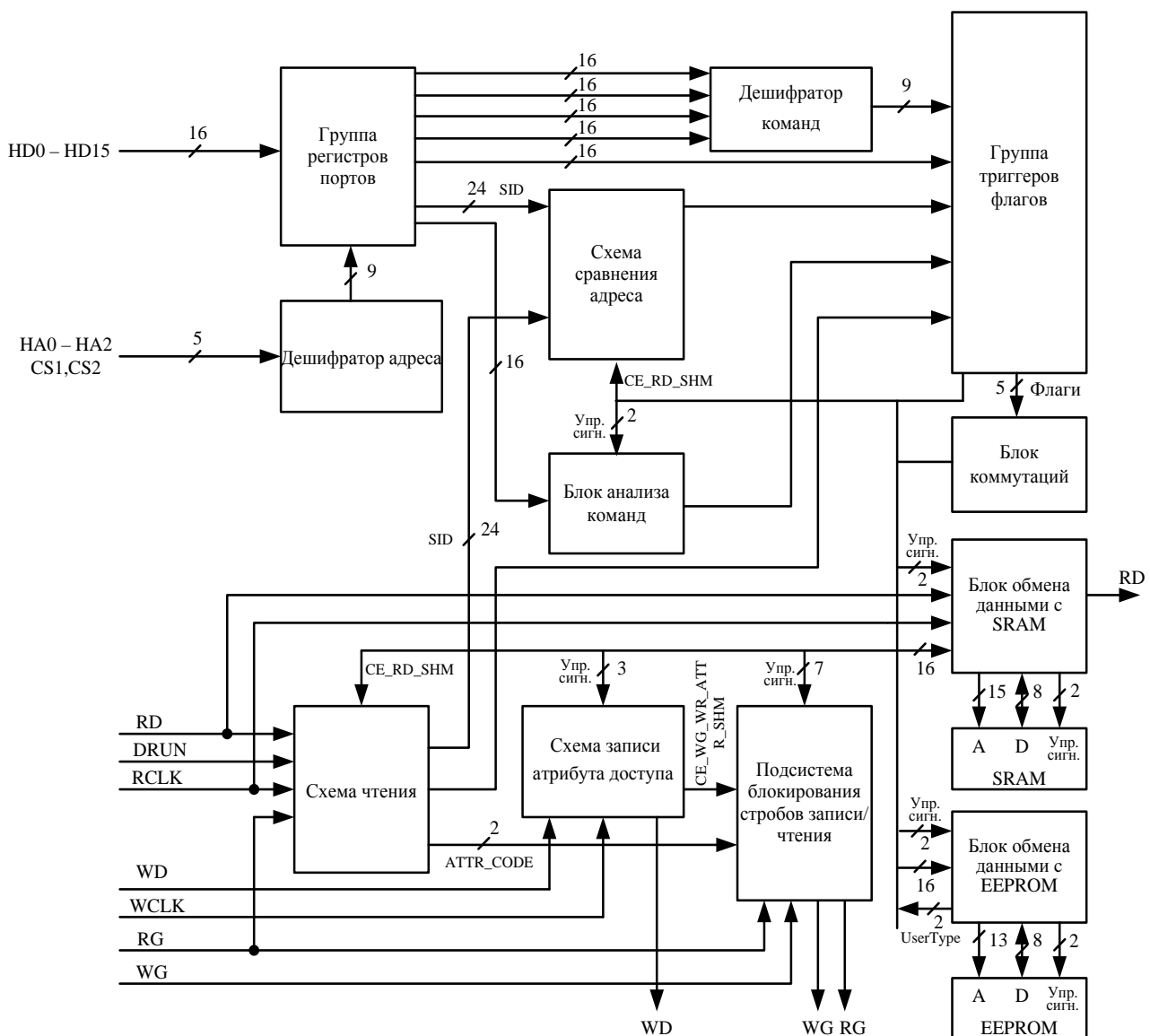


Рис. 8. Функциональная схема устройства контроля и ограничения доступа (УКОД)

Рассматриваемое устройство контроля и ограничения доступа (Рис. 8) выполняет следующие функции:

- чтение атрибута доступа из служебной зоны сектора и его анализ;
- модификация атрибута доступа к сектору;
- принятие решения о возможности доступа к полю данных сектора по считанному коду атрибута, виду выполняемой операции и типу пользователя;
- формирование для УПО слова текущего состояния, используемого в дальнейшем для построения отчета;
- формирование сигнала для пользователя о попытках доступа к контролируемым секторам;
- проверка подлинности команд УПО во время программно-управляемой модификации атрибутов доступа;
- авторизация пользователя СКОД и определение его прав;
- модификация учетных записей пользователей СКОД в ППЗУ устройства контроля;
- копирование с портативного носителя информации основных записей метаданных ЖМД во внутреннее ОЗУ устройства контроля;
- перехват запросов на доступ к основным записям метаданных ЖМД и перенаправление их во внутреннее ОЗУ устройства контроля.

Произведена оценка аппаратной сложности УКОД, содержащего 3 микросхемы: ПЛИС (Таблица 1), оперативную статическую память и перепрограммируемое постоянное запоминающее устройство.

Таблица 1

Использованные ресурсы ПЛИС CoolRunner-II XC2C38-TQ144

	Использовано	Доступно	Процент
Кол-во использованных макроячеек	352	384	92%
Кол-во использованных термов логич.произвед.	564	1344	42%
Кол-во использованных регистров	265	384	69%
Кол-во использованных контактов ввода/вывода	80	118	68%

Для повышения скорости анализа атрибута доступа и принятия решения о блокировании управляющих стробов в режиме контроля обращений к данным был произведен синтез наиболее важных функциональных схем.

Наиболее критичным по времени является анализ атрибута доступа. Он должен учитывать считанный схемой чтения код атрибута доступа, выполняемую контроллером ЖМД текущую операцию и полномочия зарегистрированного в СКОД пользователя. Обработав эти данные, схема анализа атрибута доступа должна выставить соответствующий флаг, разрешающий/запрещающий доступ к данным сектора ЖМД. Для уменьшения сложности и повышения скорости работы комбинационной схемы анализа атрибута доступа выполнен ее логический синтез. В результате получена следующая КНФ названной схемы анализа:

$$F_ACS_ALLOWED = (\bar{X}_2 \vee \bar{X}_5) \wedge (\bar{X}_2 \vee \bar{X}_6) \wedge (\bar{X}_1 \vee X_2 \vee X_3 \vee X_4 \vee \bar{X}_6) \wedge (\bar{X}_1 \vee X_2 \vee X_3 \vee \bar{X}_5 \vee \bar{X}_6),$$

где X_1 – признак операции чтения данных из сектора; X_2 – признак операции записи данных в сектор; X_3 – старший разряд типа учетной записи; X_4 – младший разряд

типа учетной записи; X_5 – старший разряд считанного атрибута доступа; X_6 – младший разряд считанного атрибута доступа.

Приведенное выражение КНФ показывает, что схема анализа атрибута доступа содержит три логических уровня. Это обеспечивает высокую скорость формирования сигнала открытия/закрытия доступа и при реализации схемы на современных ПЛИС позволяет снизить время принятия решения до $t_{\text{ПР}} = 7,5$ нс.

Атрибут доступа располагается в пробеле между адресным полем и полем данных (Рис. 7). Когда код атрибута будет считан схемой чтения, подсистема блокирования стробов чтения/записи должна успеть проанализировать входные данные и заблокировать соответствующий строб до того, как считывающая головка окажется над маркером поля данных (МПД). Позиции атрибута доступа и маркера поля данных разделяются пробелом и синхронизацией длиной 112 бит, которые будут пройдены считывающей головкой ЖМД за время $t_{\text{МПД}} = 373$ нс при тактовой частоте 300 МГц.

Таким образом, найденная выше величина времени $t_{\text{ПР}}$ принятия решения о блокировании управляющих стробов при выполнении операции чтения данных сектора значительно меньше времени $t_{\text{МПД}}$ прохождения считывающей головки ЖМД от позиции атрибута доступа до маркера поля данных, что позволяет гарантировать стабильность работы устройства УКОД в режиме контроля обращений к данным ЖМД и не снижать скорость обмена данными.

ОСНОВНЫЕ ВЫВОДЫ И РЕЗУЛЬТАТЫ РАБОТЫ

1. Разработан аппаратно-ориентированный способ контроля обращений к данным во внешней памяти, основанный на хранении кодов атрибутов в служебных полях в конце заголовка каждого сектора накопителя информации, что позволяет по сравнению с интерфейсным УКОД уменьшить не менее чем в 10^3 раз требуемую емкость оперативной памяти и осуществлять контроль чтения/записи полей данных при поиске секторов в режиме реального времени.

2. Разработана архитектура программно-аппаратной СКОД, позволяющая, без изменения программных и технических средств ЭВМ путем встраивания в контроллер НЖМД микросхемы устройства контроля УКОД и дополнения системного программного обеспечения ЭВМ утилитами и драйвером управления названным устройством, предотвращать возможность обнаружения случаев обхода деструктивными программами имеющейся в ЭВМ программной системы ограничения доступа и повышения степени защиты файлов вплоть до полного закрытия доступа к ним без ведома легитимного пользователя и администратора.

3. Разработан способ извлечения метаданных из магнитного жесткого диска, позволяющий снизить вероятность несанкционированного считывания данных при хищении накопителя информации.

4. Синтезирована организация аппаратно-программных специализированных средств ограничения доступа, отличающаяся введением портативной памяти и разграничением хранения критически важной информации (загрузочный код, таблица описания разделов, ключевые записи метаданных файловой системы) для

доступа к данным, что позволяет повысить надежность контроля обращений к внешней памяти ЭВМ.

5. Разработан метод программно-аппаратной проверки подлинности команд ЭВМ в режиме программно-управляемой модификации кодов атрибутов доступа к секторам, позволяющий снизить вероятность несанкционированного изменения атрибутов до $2,4 \times 10^{-7}$ за сеанс их модификации и тем самым повысить надежность работы системы контроля и ограничения доступа в 10^6 раз по сравнению с существующей ее программной реализацией и примерно в 10 раз по сравнению с известным интерфейсным УКОД.

6. Проведено математическое моделирование работы устройства УКОД цепями Маркова, в результате которого было установлено, что число файлов, пораженных деструктивными программами, может быть снижено в сто раз, если доля файлов, контролируемых устройством УКОД, составляет более 70%. Максимальная надежность их хранения может быть достигнута, если долю защищенных файлов повысить до 100%, а ошибочную попытку доступа пользователя, прошедшего авторизацию, разрешать однократно только в режиме чтения.

7. Разработаны алгоритмы работы, структурные и функциональные схемы устройства контроля и ограничения доступа к секторам файлов, встраиваемого в контроллер накопителя и позволяющего предотвратить несанкционированный доступ к файлам и оперативно обнаруживать атаки деструктивных программ. Для повышения скорости анализа атрибута доступа к сектору выполнен логический синтез соответствующих комбинационных схем, в результате которого время принятия решения снижено до 7,5 нс, что в 50 раз менее времени доступа к полю данных сектора со стороны контроллера ЖМД. Разработанное устройство УКОД не вносит задержек при обмене данными с ЖМД и может быть применено в перспективных высокоскоростных накопителях информации.

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

Статьи в рецензируемых научных журналах и изданиях

1. Глазков, А.С. Организация пользовательской системы защиты информации, хранящейся на жестком магнитном диске [Текст] / А.С. Глазков, С.А. Муратов, А.П. Типикин // Телекоммуникации. М.: Изд-во «Наука и технологии», 2009. №10. С. 33–38.
2. Глазков, А.С. Метод и функциональная организация контроля обращений и закрытия доступа к секторам файлов при хищении накопителя информации [Текст] / А.С. Глазков, А.П. Типикин // Информационные технологии. М.: Изд-во «Новые технологии», 2010. №5. С. 25–30.
3. Глазков, А.С. Метод повышения надежности управления программно-аппаратной системой ограничения доступа [Текст] / А.С. Глазков, А.П. Типикин // Известия Курского государственного технического университета. Курск, 2010. № 1. С. 32–38.

Публикации в других изданиях

4. Глазков, А.С. Алгоритмы и технические средства аутентификации в системе ограничения доступа к информации на жестком диске [Текст] / А.С. Глазков, М.О.

Таныгин, С.А. Муратов // Методы и средства систем обработки информации: сборник научных статей, 2007. №4. С. 65–70.

5. Глазков, А.С. Метод установления доверительного канала обмена данными между программным обеспечением и аппаратным средством [Текст] / А.С Глазков, М.О Таныгин, С.А. Муратов // Современные информационные технологии в деятельности органов государственной власти (Информтех – 2008). Курск: изд-во КурскГТУ, 2008. С. 171–172.

6. Глазков, А.С. Аппаратная реализация ограничения доступа в пользовательской программно-аппаратной системе защиты информации [Текст] / А.С Глазков, М.О Таныгин, А.П Типикин // Современные информационные технологии в деятельности органов государственной власти (Информтех – 2008). Курск: изд-во КурскГТУ, 2008. С. 177–178.

7. Глазков, А.С. Устройство аппаратной поддержки системы ограничения доступа [Текст] // Интеллектуальные и информационные системы (Интеллект – 2009). Тула: изд-во ТулГТУ, 2009. С. 193–194.

8. Глазков, А.С. Метод закрытия доступа к секторам файлов при хищении накопителя информации [Текст] // Оптико-электронные приборы и устройства в системах распознавания образов, обработки изображений и символьной информации (Распознавание – 2010). Курск: изд-во КурскГТУ, 2010. С. 131–133.

9. Глазков, А.С. Повышение скорости аппаратных средств ограничения доступа к файлам носителя информации [Текст] // Перспективы развития информационных технологий. Новосибирск: изд-во НГТУ, 2011. С. 9–14.

10. Глазков, А.С. Математическое моделирование системы ограничения доступа к файлам жесткого магнитного диска [Текст] / А.С Глазков, А.П. Типикин // Теоретические и практические аспекты научных исследований. Украина, Киев: Изд-во ООО «Миранда», 2011. С. 97–100.

11. Глазков, А.С. Структура управляющего программного обеспечения системы контроля и ограничения доступа [Текст] / А.С Глазков, А.П. Типикин // Интеллектуальные и информационные системы (Интеллект – 2011). Тула: изд-во ТулГТУ, 2011. С. 114–115.

Патент

12. Патент 2359317 РФ, МПК⁷G 06 F 12/14. Устройство ограничения доступа к секторам жесткого диска [Текст] / А.С. Глазков, М. О. Таныгин, А. П. Типикин; заявитель и патентообладатель ГОУ ВПО Курский государственный технический университет. – № 2007117962/09; заявл. 14.05.2007; опубл. 20.06.2009, БИМП №17.



Подписано в печать 10.02.2012. Формат 60×84 1/16.

Печатных листов 1,0. Тираж 120 экз. Заказ _____.

Юго-Западный государственный университет.

305040, г. Курск, ул. 50 лет Октября, 94.