

III Выводы

1. Актуальной по-прежнему является задача разработки, производства и сертификации недорогих эффективных отечественных ГШ.
2. В рамках решения этой задачи в Университете внутренних дел был разработан и исследован опытный образец ГШ радиодиапазона (0.05-1500 МГц).
3. Разработанный ГШ по базовым техническим характеристикам не уступает, а по ряду из них (нижняя и верхняя границы диапазона защищаемых частот, масса и габариты, цена) превосходит известные ГШ.
4. ГШ имеет более широкие возможности по защите от ПЭМИН переносных средств ЭВТ. Он может найти применение в целях метрологического обеспечения системы ТЗИ, а также в «атакующих» целях (подавление РМ, средств связи и управляемых радиовзрывателей).
5. Целесообразны дальнейшие совместные исследования разработанного ГШ с заинтересованными потребителями в направлениях: оценка качества шумовой помехи; исследование других типов антенных систем; оценка возможности защиты от ПЭМИН и подавления конкретных образцов техники и др.

Литература: 1. Каталог МАСКОМ. Специальная техника защиты информации, М., 1998. 2. Иванов В.П., Сак В.В. Маскировка информационных излучений средств вычислительной техники/ Защита информации. Конфидент, №1, 1998. 3. Емельянов С.Л., Марков С.И., Гаврюков В.Ф. Выбор и практическое применение генераторов шума/ Бизнес и безопасность, №4, 1998. 4. Безопасность излучений и наводок от средств ЭВТ. Домыслы и реальность/ Зарубежная радиоэлектроника, №12, 1989. 5. Провозин О.П., Солдатенко Г.Т. Деякі аспекти створення персонального комп'ютера для обробки інформації з обмеженим доступом/ Бизнес и безопасность, №6, 1998. 6. Емельянов С.Л. и др. Некоторые аспекты маскировки информационных излучений персональных компьютеров/ Бизнес и безопасность, №4, 1999. 7. Маркус Г. Кун, Росс Дж. Андерсон. Программный Темпест: скрытая передача данных с помощью электромагнитных излучений/ По материалам Интернет. 8. Величко О.М. Метрологічне забезпечення, стандартизація та сертифікація засобів ТЗИ в Україні/ Доповідь на ювілейній НТК, Київ, 1998.

УДК 537.611.3 : 537.613

МАГНИТООПТИЧЕСКИЕ СРЕДСТВА ДЛЯ РЕШЕНИЯ ЗАДАЧ ЗАЩИТЫ ИНФОРМАЦИИ, ЗАПИСАННОЙ НА МАГНИТНЫХ НОСИТЕЛЯХ

Юрий Агалиди, Сергей Левый

Национальный технический университет Украины «КПИ»

Аннотация: Рассмотрены области применения магнитооптических средств на основе плёнок висмутосодержащих феррогранатов для решения задач технической защиты информации: контроль уничтожения информации; контроль несанкционированных записей; исследования подлинности сигналограмм; кодирование и идентификация носителей; восстановление частично уничтоженной информации. Приведены структурные схемы реализации соответствующих устройств и некоторые результаты экспериментальных исследований.

Summary: Application of magneto optic means based on the bismuth containing ferrogarnet films is offered for the solution of the tasks of technical protection of information, such as the information destruction control, the illegal record control, the record authenticity research, the carriers coding and identification, the reconstruction of partially destroyed information. The block schemes of the appropriate instruments and some experimental results are shown.

Ключевые слова: Магнитная сигналограмма; техническая защита информации; эффект Фарадея; магнитооптическая визуализация.

Носители магнитной записи - магнитные ленты, жесткие и гибкие магнитные диски — по-прежнему остаются наиболее распространенным типом носителей информации в мире. Интерес к носителям магнитной записи во многом определяется тем, что, несмотря на наличие альтернативных носителей (оптические диски, флэш-память и др.), они обладают рядом существенных преимуществ и, очевидно, будут применяться еще достаточно долго.

Исходя из вышесказанного, актуальным становится раздел технической защиты информации (ТЗИ), который занимается защитой информации, записанной на магнитных носителях. Этот раздел ТЗИ на сегодняшний день недостаточно разработан как с точки зрения технико-методической базы, так и с точки зрения правовой.

Для решения вопросов ТЗИ, записанной на магнитных носителях, сегодня в основном используют методы и средства, относящиеся к кодированию информации (например, различные ключи к ЭВМ) на программном, и реже - аппаратном уровне. При этом практически никак не используется то, что информация на магнитном носителе представляет собой магнитную сигналограмму, в которой временному распределению амплитуд исходного сигнала соответствует пространственное распределение амплитуд остаточной намагниченности. Традиционный подход к анализу магнитных сигналограмм с помощью магнитопорошковых фигур приводит к уничтожению магнитного носителя, требует больших временных затрат и дорогостоящего визуализирующего материала. Поэтому это направление исследований ТЗИ практически не развивалось.

Все эти недостатки отсутствуют в методе визуализации магнитных полей рассеяния, который основан на использовании магнитооптических кристаллических пленок феррогранатов, работающих на эффекте Фарадея [1].

На наш взгляд, существует следующий ряд областей применения магнитооптики при решении задач ТЗИ:

1. Магнитооптический контроль уничтожения информации с магнитных носителей.
2. Магнитооптический контроль несанкционированных записей на магнитных носителях.
3. Магнитооптические исследования подлинности магнитных сигналограмм.
4. Магнитооптическое кодирование и идентификация магнитных носителей.
5. Магнитооптическое восстановление частично уничтоженной (запорченной) информации.

Рассмотрим более подробно каждую из перечисленных областей.

I Магнитооптический контроль уничтожения информации с магнитных носителей

Достаточно остро стоит проблема уничтожения конфиденциальной информации (стирания с магнитных носителей), без уничтожения самого носителя. Степень уничтожения информации существенно зависит от применяемой аппаратуры и методов стирания, и в ряде случаев не является достаточной. Так, применение штатных средств стирания — аппаратуры магнитной записи — для размагничивания сигналограммы и последующее применение штатных средств воспроизведения для контроля качества стирания, в ряде случаев, может привести к ошибочным выводам о полноте уничтожения информации. Наиболее вероятными причинами возникновения остаточной (нестёртой) информации могут являться:

- засорение, нарушение регулировки, либо дефекты магнитной головки стирания, приводящие к стиранию записи не по всей ширине дорожки записи;
- поперечные перемещения магнитного носителя в лентопротяжных механизмах, не имеющих магнитной головки стирания (схема “запись по записи”, применяемая в ряде диктофонов, автоответчиков и бортовых регистраторов) (рисунок 1);
- несовпадение форматов записи и стирания (рисунок 2).

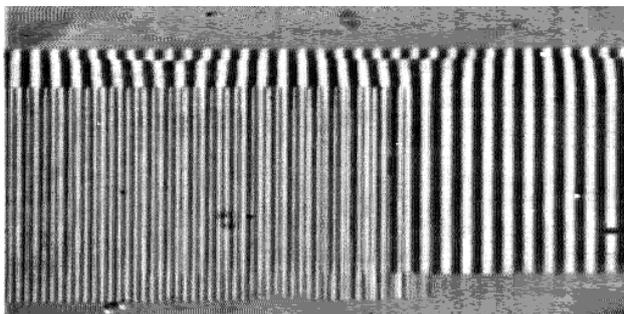


Рисунок 1

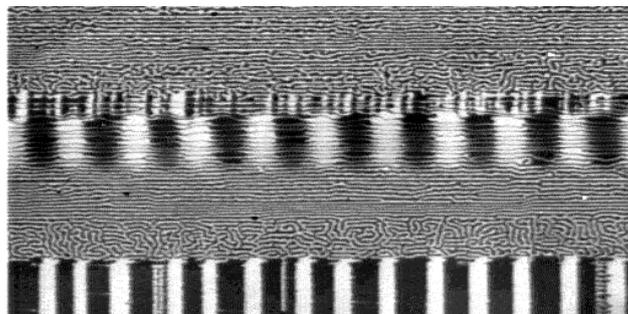


Рисунок 2

Магнитооптика в виде датчика контроля остаточной информации подобного рода, максимально использует свое назначение, так может чувствовать и отображать двумерные магнитные поля рассеяния на уровне шумов магнитного носителя с пространственным разрешением менее 1мкм [2].

Структурная схема контрольно-измерительной аппаратуры (КИА) для реализации контроля качества уничтожения информации представлена на рисунок 3.

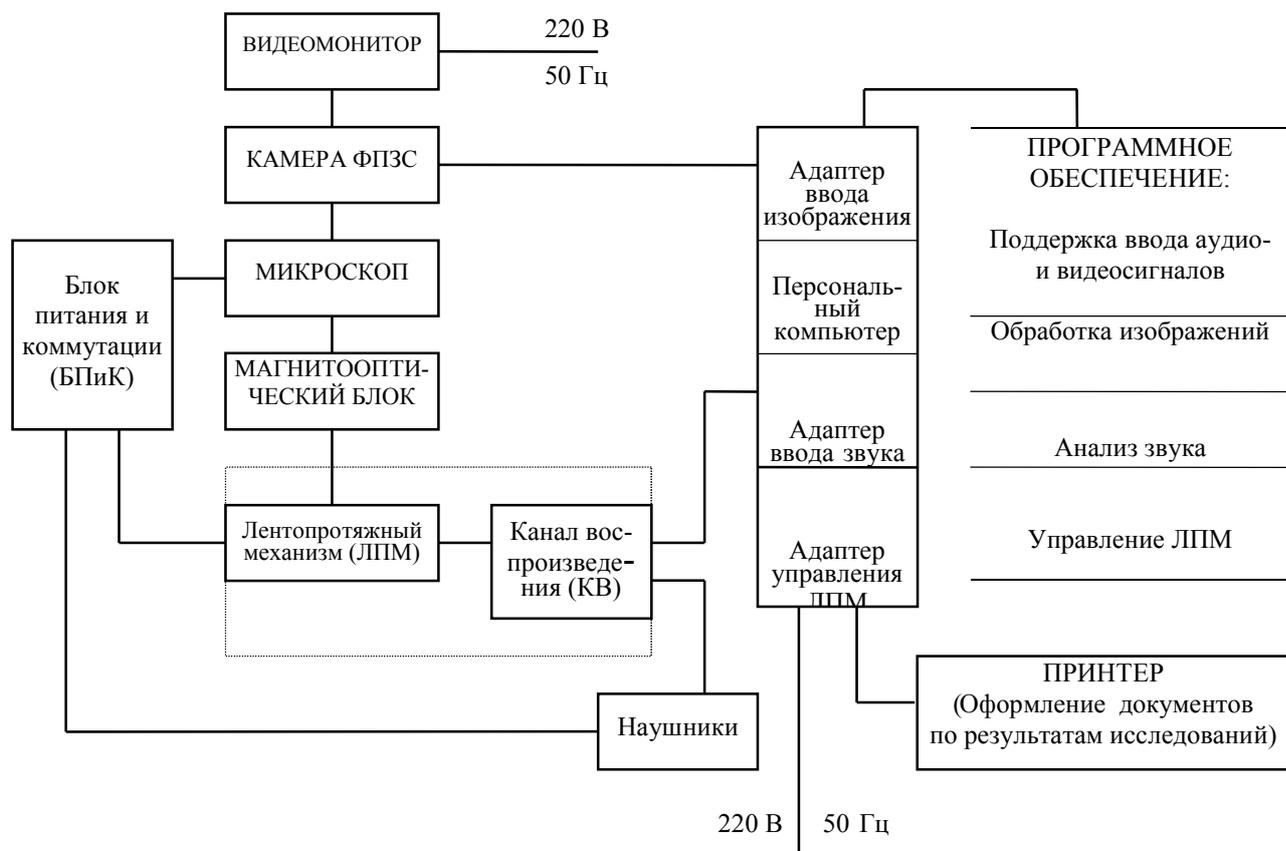


Рисунок 3 - Структурная схема контрольно-измерительной аппаратуры для контроля за уничтожением информации с магнитных носителей

Основным элементом КИА является магнитооптический визуализатор магнитооптического блока (МОБ), с помощью которого поле рассеяния магнитной сигналограммы преобразуется в световое распределение, где интенсивность света соответствует величине и положению в пространстве магнитных полей рассеяния. Считывание информации с магнитооптического кристалла (МОК) проводится поляризованным светом в поляризационном микроскопе с ограниченным спектральным составом.

Полученное при визуализации световое распределение проецируется через светофильтр СЗС-24 на позиционно-чувствительный элемент видеокамеры ФПЗС, телевизионный сигнал которой через адаптер ввода изображения поступает в ПК.

Для оперативного наблюдения визуализированной картины сигнал с видеокамеры также поступает на видеомонитор.

Визуализированная картина может наблюдаться оператором через бинокляр микроскопа.

Для смены кадров при визуализации с магнитной ленты, а также для звукового воспроизведения сигналов остаточной информации служит лентопротяжный механизм (ЛПМ) с усилителями каналов воспроизведения (УКВ). Управление ЛПМ осуществляется от компьютера через адаптер управления ЛПМ и блока питания и коммутации.

Ввод воспроизведенных звуковых сигналов в ПК осуществляется через плату адаптера ввода звука.

Прослушивание воспроизведенных сигналов осуществляется через наушники.

Питание МОБ, видеокамеры ФПЗС, ЛПМ, УКВ и осветителя микроскопа осуществляется от блока питания и коммутации.

Цифровая дообработка и анализ кадров визуализации и воспроизведения, а также управление ЛПМ, обработка и оформление результатов исследований осуществляется ПК с помощью специально разработанного программного обеспечения. Распечатка результатов исследований производится на принтере.

II Магнитооптический контроль несанкционированных записей на магнитных носителях

Под “несанкционированными” подразумеваются скрытые (замаскированные) записи, не воспроизводимые стандартной аппаратурой воспроизведения. При этом маскирующая запись, не представляющая секретности, воспроизводится стандартными средствами и создаёт впечатление единственной записи на данном носителе.

Как правило, информация на магнитном носителе записывается по нескольким дорожкам, между которыми существуют междорожечные промежутки (достаточно большие, и в некоторых случаях равные размерам самой дорожки), где информация отсутствует. Геометрия записи информации на магнитную пленку определяется нормированным форматом, что позволяет воспроизводить ее на любом серийном магнитофоне данного типа (кассетный, катушечный, видеомагнитофон стандарта VHS и др.). Если информация каким-то способом будет записана в междорожечных промежутках, то стандартным магнитофоном она не будет воспроизводиться. Этот вариант несанкционированной записи проиллюстрирован на Рисунке 4. Два канала (а и б) соответствуют формату записи катушечного магнитофона, а между ними - несанкционированная запись (с).

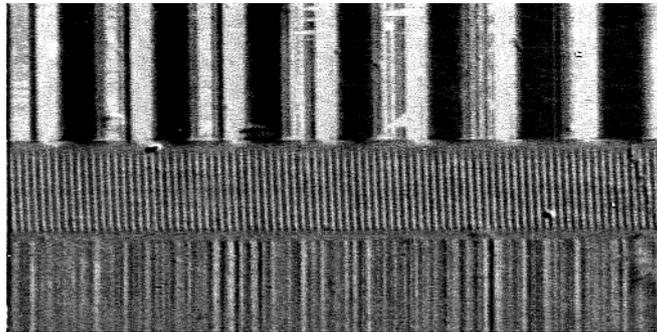


Рисунок 4

Несанкционированную запись можно записать также и внутри форматной дорожки более узкой головкой записи, при этом, с целью уменьшения взаимовлияния записей, узкую головку записи целесообразно наклонить. Авторами исследовался также и вариант продольной записи поверх наклонно-строчной – видеополы формата VHS. При просмотре (воспроизведении) кассеты с несанкционированной записью подобного типа наблюдается нарушение синхронизации некоторых строк изображения, однако с учётом низкого качества многих видеоматериалов пиратского и любительского производства подобный “дефект” может и не привлечь внимания контролирующих органов.

Все вышесказанное касается также и информации, которая записана на гибком магнитном диске в ПК.

Применение МОК позволит создать приборы контроля несанкционированных записей на магнитных носителях различного назначения, как для служб ТЗИ, так и для таможен, специализированных отделов на режимных предприятиях, а также в банковских организациях.

Для контроля несанкционированных записей на магнитных лентах пригодна аппаратура, описанная выше (рисунок 3). Аналогичный программно-аппаратный комплекс (ПАКАМС-М), расширенный в части исследований гибких магнитных дисков и магнитных карт, вместе с методиками был реализован для таможенной службы Украины.

Для контроля гибких магнитных дисков или для восстановления на них частично заперченной информации следует разработать аппаратуру, структурная схема которой представлена на рисунке 5.

Устройство работает следующим образом. Контролируемую или восстанавливаемую дискету устанавливают в магнитооптический блок, в котором к поверхности дискеты прижимается магнитооптический кристалл. Механическое перемещение дискеты по двум координатам для визуализации информации по всей поверхности дискеты осуществляется блоком механизмов, который управляется через блок питания, коммутации и управления от компьютера, имеющего адаптер управления и соответствующее программное обеспечение. Собственно визуализация магнитной сигналограммы информации, записанной на дискете, осуществляется с помощью поляризационно-оптического блока благодаря эффекту Фарадея в магнитооптическом кристалле. Визуализированная картина с помощью ФПЗС видеокамеры через видеоадаптер поступает в персональный компьютер, где дополнительно обрабатывается, сшивается, при необходимости восстанавливается заперченная информация и с помощью специальной программы записывается на новый гибкий магнитный диск,



Рисунок 5 - Структурная схема магнитооптического программно-аппаратного устройства для решения задач ТЗИ, записанной на гибких магнитных дисках

находящийся в дисковом компьютере. При отыскании несанкционированной записи происходит изучение формата записи и при его нарушении делается вывод о несанкционированной записи.

III Магнитооптические исследования подлинности магнитных сигналограмм

Если сложный и важный технический объект, управляемый аппаратурой, где информация об управлении записана на магнитный носитель, терпит аварию, то важно знать, была ли зарегистрированная информация целостным оригиналом или она была изменена путем монтажа, а также на каком аппарате была смонтирована и записана магнитная сигналограмма. Так как с помощью МО инструментальных средств можно визуализировать магнитную сигналограмму и образмерить формат записи, то это с достаточной степенью вероятности позволяет нам ответить на поставленные вопросы. В виде примеров представлены импульсы переходных процессов аппарата магнитной записи (рисунок 6), присущие только оригиналу, и трассы, обусловленные шихтованностью магнитопровода головки записи (рисунок 7), позволяющие идентифицировать аппарат магнитной записи.

Структурная схема устройства для реализации поставленной задачи аналогична структурной схеме КИА, представленной на рисунок 3. Аналогичный программно-аппаратный комплекс (ПАКАМС-К1) вместе с методиками был реализован для криминалистической службы МВД Украины.

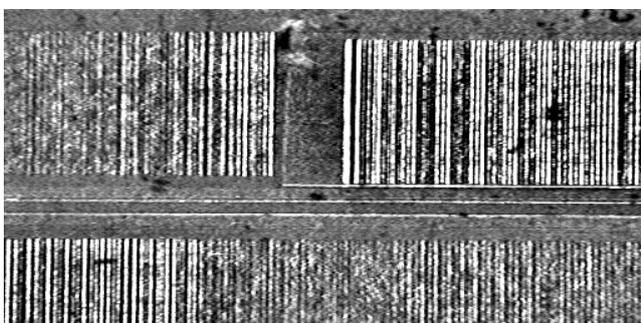


Рисунок 6

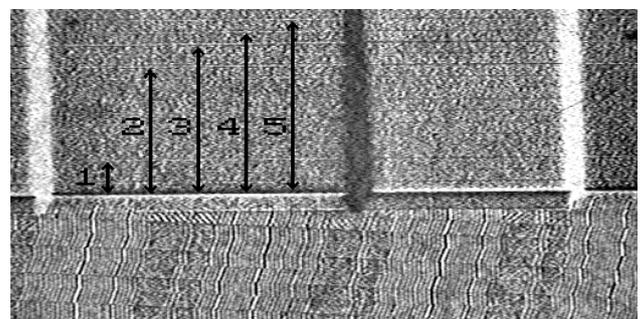


Рисунок 7

IV Магнитооптическое кодирование и идентификация магнитных носителей

Одной из важнейших задач при решении проблем ТЗИ является задача защиты от несанкционированного доступа к информации, а также от несанкционированного доступа к системам, использующим запись информации - особенно к стратегически важным системам.

Как вариант решения этой проблемы может служить магнитное кодирование магнитных носителей информации с использованием магнитооптической визуализации.

В вычислительной технике существуют методы защиты информации от доступа к ней и копирования. Одним из таких методов защиты является нанесение не копируемой метки. Известно два основных способа формирования таких меток:

1. Нанесение метки с использованием контроллера диска.
2. Нанесение физической метки.

К недостаткам первого метода можно отнести то, что практически все варианты его реализации читаются и копируются современными программными способами, такими как Disk Explorer или программно-аппаратными средствами Option Board и др.

Нанесение физической метки просто и эффективно защищает от копирования и практически не дает возможности скопировать информацию средствами контроллера дисководов.

Однако аппаратная реализация этого метода имеет свои недостатки:

1. Физическое повреждение поверхности диска, что делает ограниченным его дальнейшее использование.
2. Необходимость определения конкретного места расположения метки.
3. Сложность контроля процесса нанесения метки.

Вместо изложенных способов предлагается метод нанесения магнитной метки с помощью термомагнитной записи в заданное место информационного пространства специализированным устройством с контролем места нанесения метки магнитооптическим визуализатором.

Этот метод соединяет преимущества обоих вышеизложенных методов и характеризуется:

1. Отсутствием физических повреждений на поверхности носителя.
2. Возможностью нанесения метки любого вида и размера в любой предварительно выбранной области информационного пространства диска.
3. Большой возможностью вариантов размещения метки на логическом пространстве диска и возможностью применения дополнительно других методов защиты.
4. Отсутствием возможности копирования всеми известными средствами копирования.
5. Невозможностью нанесения такой метки без применения специализированных устройств.
6. Надежностью метода - не зависимо от того, что принцип защиты известен.
7. Возможностью использования устройства нанесения меток для восстановления заперченной информации на дискетах.
8. Невозможностью чтения метки без применения специализированных средств.

К недостаткам метода можно отнести:

1. Разработку специальной электронной схемы, которая будет устанавливаемой в ПК.
2. Необходимость защиты от несанкционированного доступа к специальной электронной схеме.

Одним из возможных вариантов использования предложенного метода кодирования может быть маркировка дискет, которые могут быть использованы только в ПК одного предприятия или организации. Работники этого предприятия могут работать с ПК только на маркированных дискетах. Ни списать с ПК, ни записать в него информацию с немаркированной дискеты они не смогут, при этом никакой информации о коде сотруднику для работы не надо. Такой подход существенно уменьшит вероятность занесения вируса при использовании программных продуктов или информации, записанной на "чужих" дискетах, а также ограничит несанкционированное распространение информации, которая принадлежит предприятию.

Предложенное кодирование должно осуществляться специализированной службой, и все коды должны храниться только в ней.

Магнитооптическое кодирование информации на гибких магнитных дисках может осуществляться на стенде, структурная схема которого представлена на рисунок 8.

Идеология магнитооптического кодирования ГМД заключается в следующем. Так как контроллер дисководов не позволяет записать на диске элемент записи длиной более двух тактовых интервалов, то наличие трех и более участков с совпадающим направлением намагниченности будет восприниматься контроллером диска как заперченная информация. С помощью стенда, структурная схема которого приведена на рисунок 5, термомагнитным способом с магнитооптической визуализацией можно записать "заперченную" информацию в

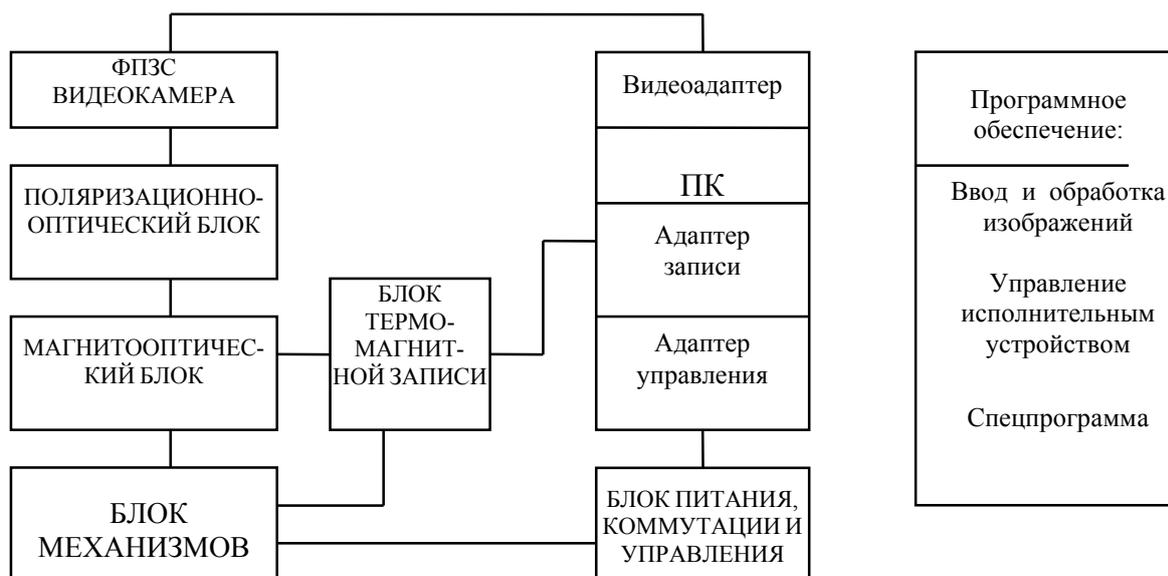


Рисунок 8 - Структурная схема стенда магнитооптического кодирования

любой предварительно выбранной области информационного пространства заранее отформатированной дискеты. Характером и местоположением таких меток, как ключом, производится кодирование информации на дискете. Кодирование и декодирование информации будет выполняться кодировщиком-декодировщиком, установленным в ПК между дисководом и контроллером дисковода.

Стенд работает аналогично программно-аппаратному комплексу, структурная схема которого приведена на рисунок 3, за исключением нанесения метки. Визуализируя нужную область информационного пространства дискеты, мы в то же время через магнитооптический кристалл (скажем, лазерным лучом, специально сфокусированным) нагреваем поверхность магнитного носителя до температуры Кюри и при остывании подаем импульсное магнитное поле, которое записывается в месте нагрева (рисунок 9). Весь стенд управляется и синхронизируется с помощью ПК.

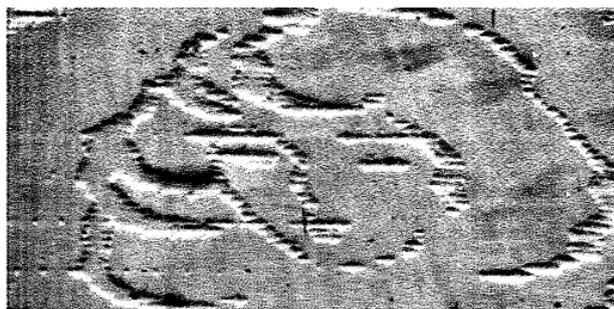


Рисунок 9

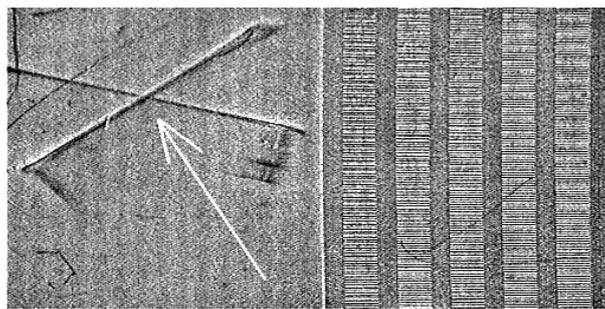


Рисунок 10

Возможно применение магнитооптики и для идентификации магнитного носителя информации. Идентификация возможна путем нанесения на поверхность дискеты, свободную от информации, магнитной метки в виде символа или числа (см. рисунок 10) с помощью магнитного карандаша или маркера. Таким образом, поверхность дискеты будет визуально чистой, но при наблюдении с помощью магнитооптического кристалла эта цифра или метка будет проявляться. Подобный подход оправдан в режимных отделах или первых отделах предприятий, где в использовании находятся дискеты с секретной информацией.

Структурная схема стенда для обнаружения идентификационных меток достаточно проста (см. рисунок 11).

Дискета устанавливается в магнитооптический визуализатор, где к ее поверхности прижимается магнитооптический кристалл, и есть возможность поворота дискеты. Затем, поворачивая дискету, находим место

с меткой, которая визуализируется под поляризационным микроскопом. Наблюдение визуализированной метки происходит с помощью ФПЗС видеокамеры на видеоконтрольном устройстве.

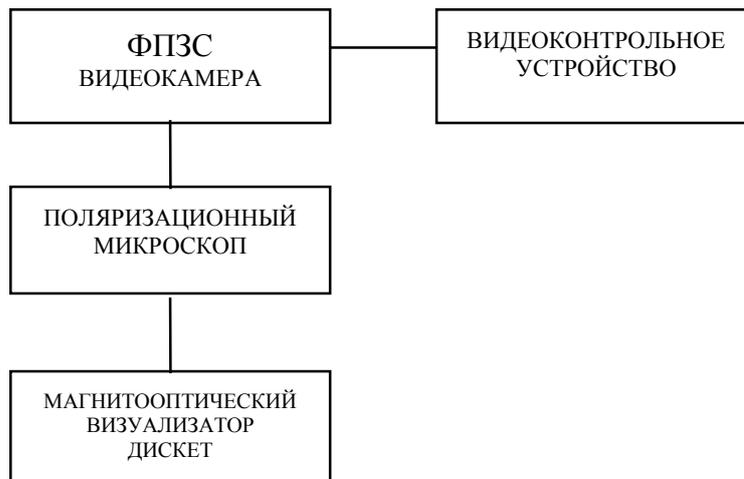


Рисунок 11 - Структурная схема стенда обнаружения кодированных меток на дискетах

V Магнитооптическое восстановление частично уничтоженной (запорченной) информации

В процессе хранения и использования информации нередки случаи её частичного или полного уничтожения в результате ошибок, халатности и экстремальных обстоятельств. При этом степень ущерба от потери информации иногда может быть очень высокой. Поэтому задача восстановления частично уничтоженной информации подчас бывает весьма актуальной.

Работа [3] посвящена восстановлению магнитооптическими средствами частично уничтоженной информации в случаях уничтожения значительной части ширины дорожки записи (рисунок 1; 2). Проведенные исследования показали возможность восстановления содержания речевого сообщения при остаточной ширине дорожки записи до 5мкм (менее 1% стандартной ширины дорожки аудиокассеты). Иными словами, восстановление речевого сообщения предыдущей и пред- предыдущей записи автоответчика (рисунок 1; 2) с технической точки зрения не составляет проблемы.

Весьма критичными к различного рода дефектам являются магнитные носители информации персональных компьютеров. Характер повреждения записи на дискете (группа магнитных трасс), подлежащей восстановлению магнитооптическими средствами, представлен на рисунок 12.

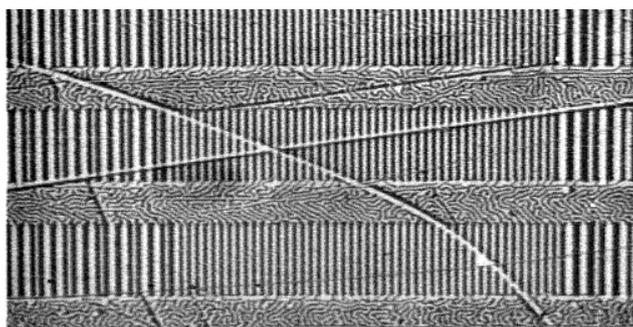


Рисунок 12

Очевидно, что несмотря на повреждения фрагментов дорожек записи, делающие невозможным считывание при помощи дисководов, физически информация сохранилась, и запись уверенно визуализируется магнитооптикой.

Для восстановления с гибких магнитных дисков частично запорченной информации возможно применять аппаратуру, структурная схема которой представлена на рисунок 5.

Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні

Все описанные технические средства на основе магнитооптики (за исключением системы магнитооптического кодирования) успешно прошли апробацию и подтвердили свою конкурентоспособность и эффективность при решении практических задач ТЗИ.

Литература: 1. Levy S.V., Ostrovsky A.S., Agalidi Yu.S. Magnetic field topographical survey by space-time light modulators. SPIE Proceedings Vol. 2108 (1993). 2. Левый С.В., Агалиди Ю.С., Вишневецкий В.Г. Магнитооптические средства технической защиты информации. ISSN 0021 – 3470, Радиоэлектроника, 1998, №8. 3. Левый С.В., Мачнев А.М., Агалиди Ю.С., Магера В.Н., Турбин Д.А. Применение магнитооптического преобразователя для восстановления сигнала по неформатным записям. ISSN 0021 – 3470, Радиоэлектроника, 2000, №5, стр.62-66.

УДК 621.314.68:621.382.3

МОДЕЛИРОВАНИЕ СЕТЕВОГО ПОМЕХОПОДАВЛЯЮЩЕГО ЗАЩИТНОГО ФИЛЬТРА

Владимир Пилинский, Владимир Первой, Мария Родионова, Антон Янушевский
Национальный технический университет Украины «КПИ»

Аннотация: Разработана модель помехоподавляющего защитного фильтра по несимметричному кондуктивному пути. Модель описывает трёхзвенный фильтр с затуханием не менее 60 дБ в диапазоне частот десятки килогерц – единицы гигагерц. Показано влияние регулярных и паразитных параметров компонентов на частотную зависимость затухания фильтров.

Summary: Common – mode model of protective RFI – filter is suggested. Three – links filter with attenuation more then 60dB in the frequency range 10 kHz ... 1GHz is analysed. Influence of regular and parasitic parameters of the filter components on filter attenuation is shown.

Ключевые слова: Помехоподавляющий защитный фильтр, моделирование, затухание, паразитные параметры, энергетическая сеть.

I Постановка задачи

Один из элементов системы, через который возможен несанкционированный доступ к конфиденциальной информации – силовые кабели энергообеспечения электронно-вычислительной аппаратуры, средств телекоммуникации, оргтехники и т.п.

Эффективным средством защиты от утечки информации по цепям электропитания могут быть помехоподавляющие фильтры (ППФ) [1], на которые возложена дополнительная задача. Решение этой задачи сводится к расширению диапазона частот в полосе подавления фильтров 150кГц ... 30МГц для ППФ общего применения [2] до единиц, десятков килогерц – сотен мегагерц, единиц гигагерц с затуханием не менее 60 дБ для фильтров, предназначенных для информационной защиты в силовых цепях.

Особенность проектирования таких фильтров состоит в необходимости учёта не только регулярных, но и всех паразитных параметров компонентов фильтра и даже элементов конструкции. Ниже, на модели несимметричного кондуктивного пути трёхзвенного фильтра показано влияние этих элементов. Очевидно, что если будет известно влияние паразитных параметров на затухание фильтра, то возможно отыскание путей управления их значениями, т.е. становится реальным обеспечение необходимого значения затухания в заданном диапазоне частот.

II.1 Модель фильтра

На основе анализа материалов различных источников и собственного опыта предложена модель фильтра для несимметричного пути распространения помехи или сигнала – в зависимости от основного назначения фильтра и направления потока энергии в представляющем интерес диапазоне частот (рисунок 1). В частности, также многозвенные фильтры описаны в [3] с указанием соответствия частотной характеристики затухания положениям документа TEMPEST specification, применяемым в США для электронных средств, оперирующих с конфиденциальной информацией.