УДК 004.056.53

Ю. В. ЛЫКОВ, канд. техн. наук, О. А. СЯГАЕВА

АНАЛИЗ ИСТОЧНИКОВ ПЭМИ В СОВРЕМЕННЫХ ПЭВМ

Введение

Развитие современного информационного общества связано с широким распространением персональных электронно-вычислительных машин (ПЭВМ), построением глобальной информационной сети и подключением к ней большого количества пользователей. Эти достижения выдвинули на передний план деятельность, связанную с производством, потреблением, передачей и хранением информации, но в то же время стали одной из главных причин образования опасных каналов утечки информации.

Источниками образования технических каналов утечки информации являются физические преобразователи. Любой электронный элемент при определенных условиях может стать источником образования канала утечки информации.

Одним из наиболее опасных каналов утечки информации в информационных системах является побочное электромагнитное излучение (ПЭМИ), создаваемое техническими средствами, например ПЭВМ и линиями связи. Принимая и декодируя эти излучения, можно получить сведения об информации, обрабатываемой в данном техническом средстве.

Оценочно, по каналу ПЭМИ может быть перехвачено не более 1 – 2 % данных, хранимых и обрабатываемых на персональных электронно-вычислительных машинах и других технических средствах передачи информации (ТСПИ) [1]. На первый взгляд, может показаться, что этот канал действительно менее опасен, чем, например, акустический, по которому может произойти утечка до 100 % речевой информации, циркулирующей в помещении. Однако в настоящее время практически вся информация, содержащая государственную тайну или коммерческие секреты, проходит этап обработки на персональных электронно-вычислительных машинах. Специфика канала ПЭМИ такова, что те самые два процента информации, уязвимые для технических средств перехвата, – это данные, вводимые с клавиатуры ПЭВМ или отображаемые на мониторе. То есть значительная часть сведений, подлежащих защите, может оказаться перехваченной злоумышленником.

Наиболее опасными устройствами вычислительной техники, с точки зрения утечки информации по ПЭМИ, являются мониторы ПЭВМ, клавиатура, принтеры, проводные линии связи. Например, с монитора можно снять информацию с помощью специальной аппаратуры на расстоянии до 500 – 1500 *м*, с принтеров – до 100 – 150 *м* [2]. Поэтому, если устройство вычислительной техники используется для обработки конфиденциальной информации, оно в целом и все его составные части должны в обязательном порядке проходить проверку на наличие в них ПЭМИ и соответствие обнаруженных излучений существующим нормам.

Постановка задачи

Проблема выявления устройств ПЭВМ, от которых возможна утечка информации через ПЭМИ, становится все более актуальной. Поскольку весь спектр ПЭМИ персональной электронно-вычислительной машины состоит из бесконечного множества гармонических составляющих, это значительно увеличивает затраты времени на их выявление и измерение. В составе практически каждой современной ПЭВМ есть как устройства, выполняющие вспомогательные функции, по которым не передаются сигналы, содержащие конфиденциальную информацию (неинформативные ПЭМИ), так и потенциально-опасные устройства, по которым непосредственно передаются сигналы, содержащие секретные данные (потенциально-опасные излучения). Выявление таких потенциально-опасных устройств, из которых возможна утечка информации, является важной задачей. Это позволит значительно сократить время тестирование ПЭВМ, на которой предполагается обработка конфиденциальной информации.

Кроме того, в связи с постоянно обновляющейся номенклатурой цифрового электронного оборудования, интерфейсов передачи данных, используемых протоколов, анализ ПЭВМ на наличие потенциально опасных устройств необходимо проводить периодически.

Цель работы – выявление потенциально-опасных устройств обработки информации в составе современных ПЭВМ.

Основные положения

Побочные электромагнитные излучения, генерируемые электронными устройствами, обусловлены протеканием токов в их электрических цепях. Спектр ПЭМИ цифрового электронного оборудования представляет собой совокупность гармонических составляющих в некотором диапазоне частот. Например, спектр частот ПЭМИ ПЭВМ представлен колебаниями в достаточно широком диапазоне: от единиц мегагерц до нескольких гигагерц. Диаграмма направленности побочного электромагнитного излучения ПЭВМ не имеет ярко выраженного максимума: взаиморасположение составных частей ПЭВМ (монитор, системный блок, проводники, соединяющие отдельные модули) отличается большим количеством вариантов. Поляризация излучений ПЭВМ, как правило, линейная и определяется так же, как и диаграмма направленности, – взаиморасположением соединительных проводов и отдельных блоков. Следует отметить, что именно соединительные провода, а точнее, их плохая или совсем отсутствующая экранировка, являются главным фактором возникновения ПЭМИ [3].

С точки зрения реальной утечки информации, не все составляющие спектра ПЭМИ потенциально опасны. Весь спектр можно разделить на потенциально информативные и неинформативные излучения. Совокупность составляющих спектра ПЭМИ, порождаемая протеканием токов в цепях, по которым передаются содержащие конфиденциальную информацию сигналы, называют потенциально-информативными излучениями (потенциально-информативными ПЭМИ) [4].

Практически в каждом цифровом устройстве существуют цепи, выполняющие вспомогательные функции, по которым не передают сигналы, содержащие закрытую информацию. Излучения, порождаемые протеканием токов в таких цепях, безопасны в смысле утечки информации. Для таких излучений вполне подходит термин – неинформативные излучения (неинформативные ПЭМИ). С точки зрения защиты информации, неинформативные излучения могут быть очень полезными, появляясь, в случае совпадения диапазона частот, в виде помехи приему информативных ПЭМИ.

Известно, что наибольшую опасность представляет излучение тех устройств, в которых защищаемая информация циркулирует в виде последовательного кода. Фактически, примерно с 1983 г. цепи с параллельным кодированием и разрядностью выше восьми не рассматриваются как опасные по каналу ПЭМИН [5].

Выявление устройств ПЭВМ с последовательным кодированием информативного сигнала

Главная особенность структуры ПЭВМ заключается в том, что все её устройства обмениваются информацией через системную шину (рис.1). К системной шине подключён центральный процессор (или несколько процессоров), оперативная, постоянная и кеш-память. Эти компоненты размещены на материнской плате (*mother board*). К материнской плате присоединяются платы (карты) внешних устройств: видеоадаптер, звуковая плата, сетевая плата и др.[6].

В зависимости от сложности устройств на этих платах могут располагаться другие специализированные процессоры: математический, графический и др.

С помощью кабелей к материнской плате подключены жёсткий диск, гибкий диск и устройство чтения оптических дисков:

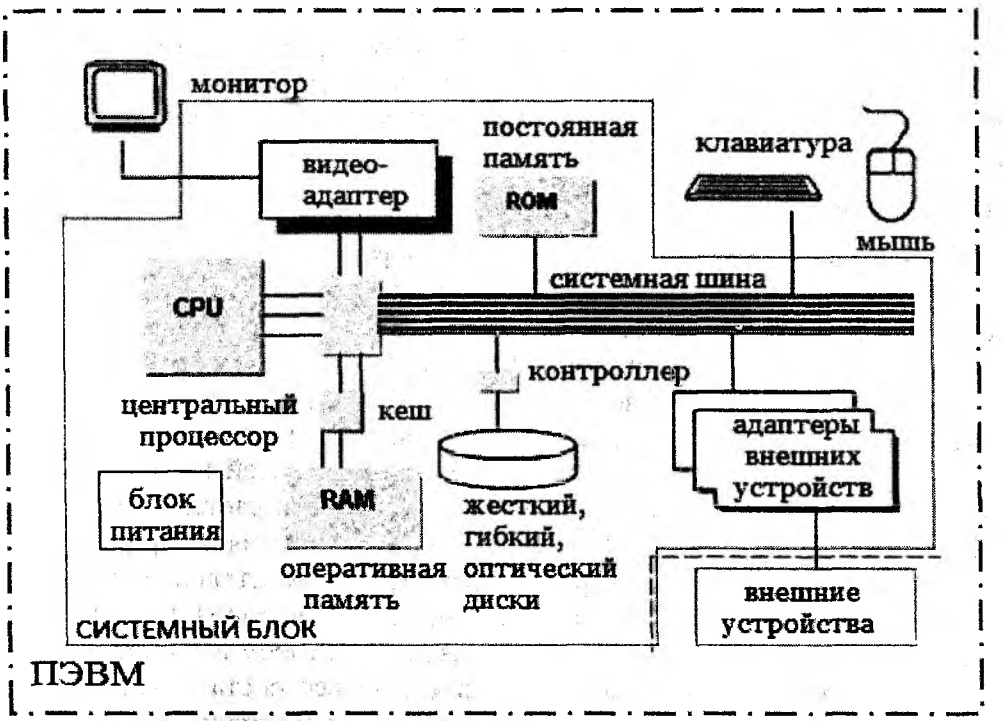


Рис. 1. Структура ПЭВМ

Все упомянутые компоненты располагаются в системном блоке. Остальные компонен ты, которые находятся вне системного блока, именуются внешними (периферийными) уст ройствами: монитор, клавиатура, мышь и другие манипуляторы, принтеры, устройств резервного копирования и архивации, сканеры, модемы и др.

В составе типовой ПЭВМ подпадают под понятие устройств с последовательным коди рованием [7]:

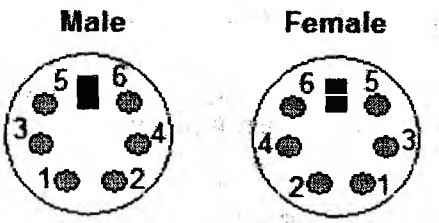
- видеоподсистема;
- накопители на жестком и гибком дисках, внешняя флэш-память;
- устройства *CD, CD-R, CD-RW, DVD, DVD-RW;*
- клавиатура;
- последовательный порт (*COM, USB*);
- принтеры.

Во всех перечисленных устройствах возможна обработка конфиденциальной информа ции. Рассмотрим эти устройства подробнее.

Анализ возможности возникновения ПЭМИ в клавиатуре

Традиционная клавиатура ПЭВМ представляет собой унифицированное устройств ввода со стандартным разъемом и последовательным интерфейсом связи с системной пла той. Существуют клавиатуры с интерфейсом *PS/2* и с интерфейсом *USB*.

Интерфейс *PS/2* используется в разъеме *Mini-Din* (рис. 2). Этот разъем состоит из шест контактов, из которых задействованы только четыре [8]:



1. *Data* (передаваемые данные)
2. *Not Implemented* (не используется)
3. *Not Implemented* (не используется)
4. *Ground* (Земля)
5. *VCC* (+5V) (Питание)
6. *Clock* (сигнал синхронизации передаваемых данных)
7. *Not Implemented*

Рис. 2. Цоколёвка разъема *Mini-Din*

При передаче от устройства к компьютеру используется следующий протокол. Устройство не начинает передачу, если *Clock* не находился в «1» по крайней мере 50 микросекунд. Устройство передает последовательно:

1. старт бит – всегда ноль;
2. 8 бит данных;
3. бит четности;
4. стоп бит – всегда единица.

Устройство устанавливает сигнал *Data,* когда *Clock* находится в логической единице. Контроллер на материнской плате читает данные, когда *Clock* находится в логическом нуле (рис. 3).

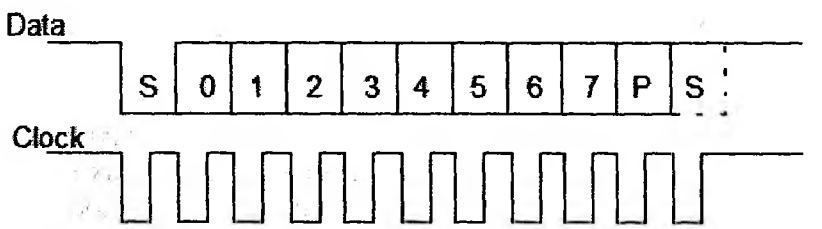


Рис. 3. Схема чтения данных контроллером

Частота сигнала *Clock* примерно 10 – 20 *кГц.* Время от фронта сигнала *Clock* до момента изменения сигнала *Data* не менее 5 микросекунд

Контроллер материнской платы сигнализирует устройству о невозможности приема, опустив сигнал *Clock* в логический ноль.

Для клавиатур характерна нестабильность тактовой частоты задающего генератора, поэтому она подвержена паразитной высокочастотной генерации. Следовательно, уровень излучения от клавиатуры может наблюдаться до частот 10 – 15 *МГц,* выше крайне редко. Спектр излучения клавиатуры линейчатый, сосредоточен в основном на частотах от единиц до сотен килогерц, с шагом 5 – 20 *кГц.* Поиск и измерение возможных опасных излучений сильно затруднены неинформативным ПЭМИ импульсных блоков питания системного блока (в диапазоне от единиц килогерц до первого десятка мегагерц) [9].

Интерфейс *USB* (*Universal Serial Bus* – Универсальный Последовательный Интерфейс) предназначен для подключения периферийных устройств к персональному компьютеру. Позволяет производить обмен информацией с периферийными устройствами на трех скоростях (спецификация *USB 2.0*):

- Низкая скорость (*Low Speed – LS*) – 1,5 *Мбит/с*;
- Полная скорость (*Full Speed – FS*) – 12 *Мбит/с*;
- Высокая скорость (*High Speed – HS*) – 480 *Мбит/с*.

Сигналы *USB* передаются по четырехпроводному кабелю, разъёмы которого схематично показаны на рис.4.

GND – цепь "корпуса" для питания периферийных устройств, *VBus* – +5V также для цепей питания. Шина *D+* предназначена для передачи данных, а шина *D* – для приема данных.

Кабель для поддержки полной скорости шины (*full-speed)* выполняется как витая пара, защищается экраном и может также использоваться для работы в режиме минимальной

скорости (*low-speed*). Кабель для работы только на минимальной скорости может быть любым и неэкранированным.

Шина *USB 2.0* является однонаправленной. То есть данные передаются либо в одну сторону, либо в другую (но не одновременно) по одной и той же витой паре:

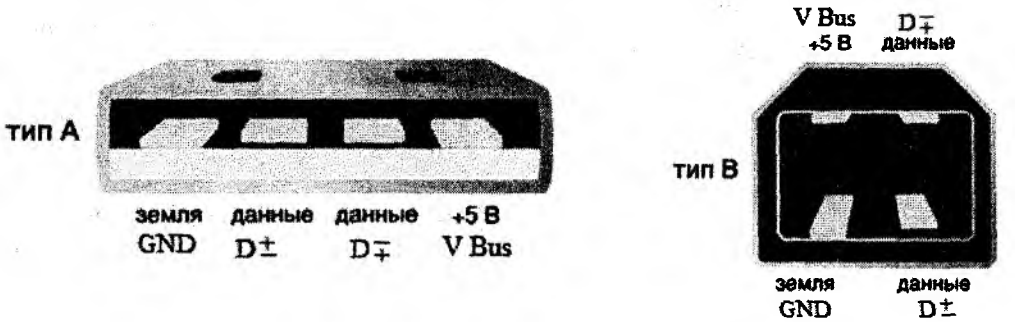


Рис. 4. Цоколёвка разъёмов USB

Рассмотренные интерфейсы передают информацию в последовательном коде, соответственно информация, вводимая клавиатурой в ПЭВМ потенциально, может быть перехвачена и декодирована злоумышленником.

Анализ возможности возникновения ПЭМИ в принтерах

В последнее время наибольшее распространение получили: матричные, струйные и лазерные принтеры.

Современные принтеры требуют высокоскоростной передачи данных по внешнему интерфейсу. Ранее производимые принтеры имеют параллельный интерфейс *Centronics* или более производительный *IEEE 1284*. Из последовательных интерфейсов в принтерах используется *RS-232C* для подключения к *COM*-порту. На сегодняшний день самым распространенным интерфейсом, используемым в принтерах, является *USB*.

Если используется порт по протоколу *USB 2.0*, то взаимообмен производится на произвольной частоте, которая может оказаться в диапазоне до 400 *МГц*. Эту частоту приходится определять непосредственными измерениями в кабелях интерфейса, так как проведение специальных исследований и последующих расчетов без знания этого значения невозможно.

Рис. 5. Принцип работы матричного принтера

В *матричном принтере* изображение формируется в параллельном коде, который поступает на печатающую головку, представляющую собой набор иголок, приводимых в действие электромагнитами (рис. 5). Головка располагается на каретке, движущейся по направляющим поперёк листа бумаги. При этом иголки в заданной последовательности наносят удары по бумаге через красящую ленту [10].

В разное время выпускались принтеры с 9, 12, 14, 18, 24 и 36, 48 иголками в головке. В настоящее время 9-игольчатые матричные принтеры занимают большую часть рынка.

Казалось бы, что передача информации на печатающую головку матричного принтера происходит по параллельному интерфейсу, поэтому перехваченная информация не представляет интерес для злоумышленника. Однако перехваченное сообщение при передаче семантического текста не будет случайным. Для расшифровки в сообщении каждого символа и всего сообщения в целом по принятому сигналу можно будет выбрать наиболее вероятный набор символов алфавита, а затем их уточнять по соседним символам в слове (предложении) и по

семантике текста. Таким образом, возможен перехват и расшифровка ПЭМИ матричного принтера.

В *лазерных принтерах* основным является фотопроводящий элемент (фотобарабан), который представляет собой металлический цилиндр, покрытый тонкой пленкой фоточувствительного полупроводника. Поверхность такого цилиндра можно зарядить положительным или отрицательным зарядом, который сохраняется до тех пор, пока барабан не освещен. Если какую-либо часть барабана экспонировать, покрытие приобретает проводимость и заряд стекает с освещенного участка, образуя незаряженную зону. На рис. 6 представлены конструкция и принцип работы лазерного принтера [11].

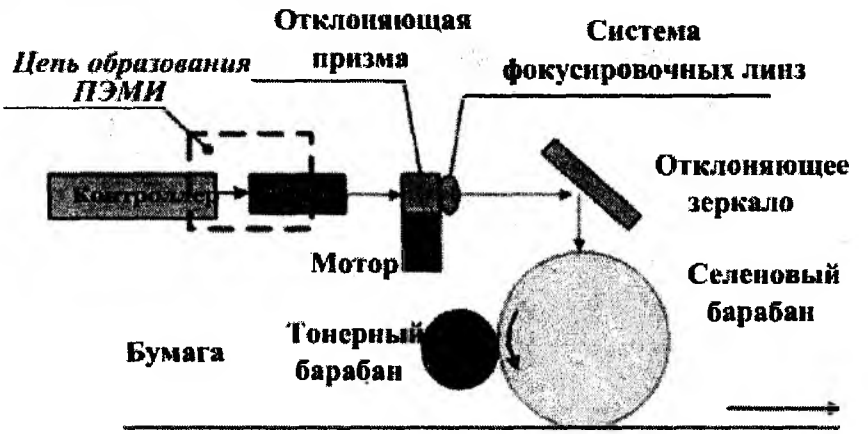


Рис. 6. Конструкция и принцип работы лазерного принтера

Для получения точечного изображения в принтере лазер включается и выключается при помощи управляющего микроконтроллера. Вращающееся зеркало разворачивает луч в виде строки скрытого изображения на поверхности фотобарабана. После формирования строки специальный шаговый двигатель поворачивает барабан для формирования следующей.

В лазерных принтерах сигнал на узел печати (лазерный диод) поступает в последовательном коде. Соответственно цепь, соединяющая внутренний контроллер с лазером, является наиболее уязвимым местом образования информативных ПЭМИ. Также опасность представляет собой и цепь протекания сигнала от персонального компьютера по *USB* интерфейсу на контроллер (рис. 7).

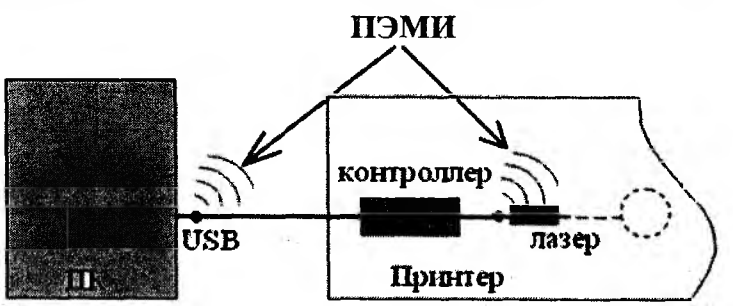


Рис. 7. Цепь протекания информативного сигнала в лазерном принтере

В *струйных принтерах* сигнал от внутреннего контролера на печатающую головку поступает в параллельном коде, разрядность которого соответствует количеству сопел, число которых в современных принтерах может достигать несколько сотен. Единственным уязвимым местом является интерфейсный кабель. Однако передача в принтер информации, выводимой на печать, по интерфейсному кабелю происходит только в начале печати в достаточно короткий интервал времени, что значительно затрудняет поиск частот ПЭМИ и их дальнейший перехват.

Проведенный анализ конструкций и принципов работы принтеров позволяет сделать вывод о том, что утечка информации по каналу ПЭМИ возможна только в лазерном и в некоторых матричных принтерах.

Анализ возможности возникновения ПЭМИ в мониторах ПЭВМ

Основным устройством вывода визуальной информации в ПЭВМ является монитор. Наиболее распространены мониторы двух типов: на основе электронно-лучевой трубки (ЭЛТ) и плоские жидкокристаллические (ЖК).

Для обычных *мониторов на основе ЭЛТ* сигналы передаются в аналоговом VGA (Video Graphics Array) интерфейсе. Такой монитор содержит электронно-лучевую трубку с видеоусилителями сигналов яркости лучей, генераторы развёрток, блок питания и схемы управления этими узлами [12]. Функциональная схема ЭЛТ монитора показана на рис. 8.

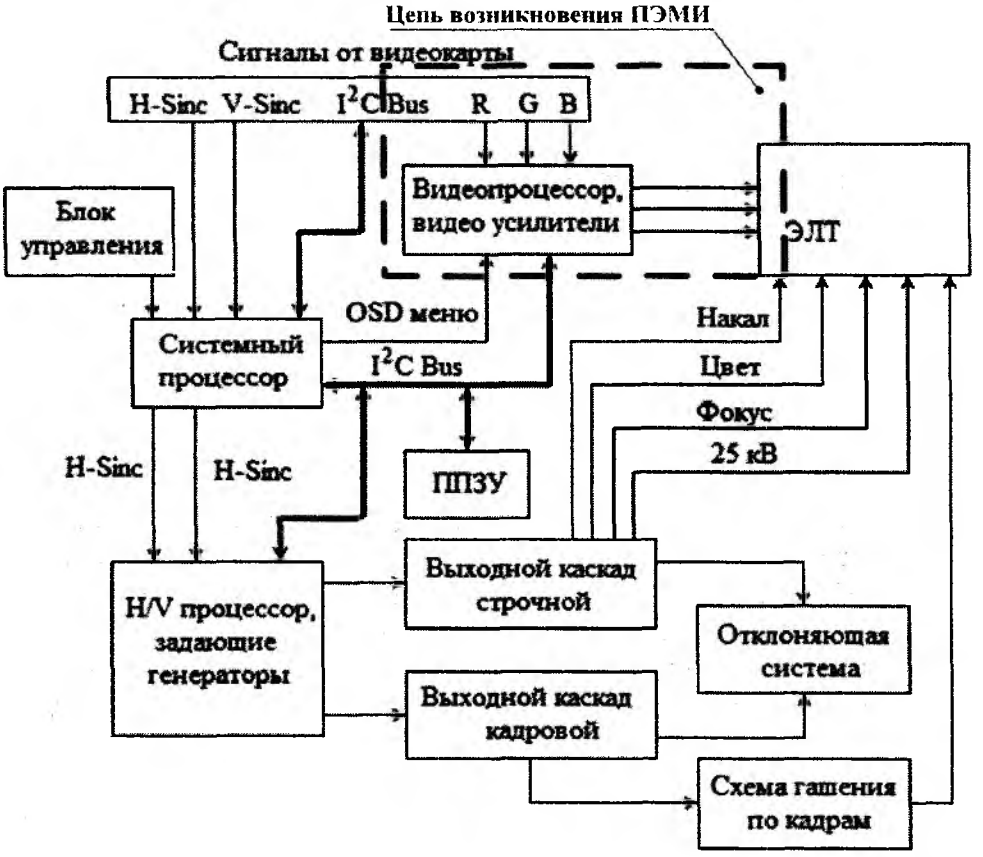


Рис. 8. Функциональная схема ЭЛТ монитора

Для передачи изображения на ЭЛТ-монитор используются сигналы интенсивности для каждого из трех основных цветов – RGB (Red – красный, Green – зеленый, Blue –синий), а также сигналы для управления ходом электронного луча – так называемые сигналы синхронизации горизонтальной (H) и вертикальной (V) разверток.

При суммировании сигналов с трех каналов в пространстве с помощью случайной антенны получается сигнал яркости. В общем случае такой сигнал достаточно просто декодировать злоумышленнику даже, когда в пространство излучается сигнал только от одного из RGB канала. При этом теряется только информации о цвете выводимого на экран изображения или текста.

Рассмотрим следующий тип мониторов – *ЖК мониторы*. Такой монитор представляет собой набор параллельных стеклянных пластин, между которыми расположены поляризаторы, прозрачные адресные электроды и жидкие кристаллы. Молекулы жидких кристаллов под воздействием электричества могут изменять свою ориентацию и вследствие этого изменять свойства светового луча проходящего сквозь них. На задней панели дисплея расположена лампа равномерной подсветки. Управляющая электроника построчно подает напряжение на определенные электроды, изменяя прозрачность соответствующих ячеек жидких кристаллов.

В результате создается изображение на экране ЖК монитора [13]. Структурная схема ЖК монитора представлена на рис. 9.

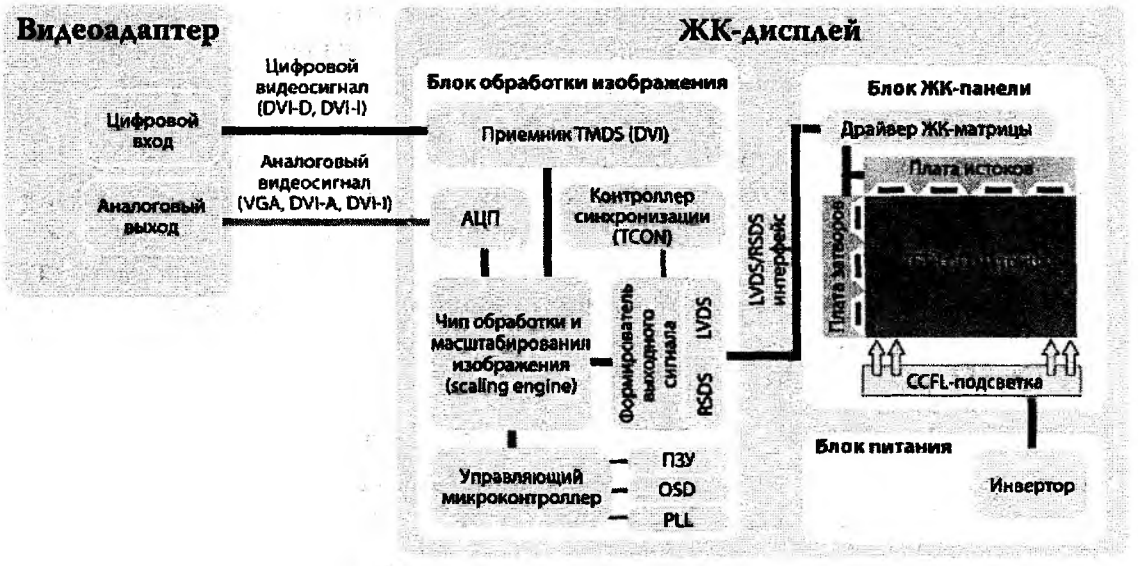


Рис. 9. Схема функциональных блоков ЖК монитора

В *ЖК* мониторах, как правило, применяются два типа интерфейса аналоговый *VGA* и цифровой *DVI* (*Digital Visual Interface*).

В основе протокола DVI находится предложенная Silicon Image технология быстродействующего последовательного интерфейса PanelLink, использующего метод разностных сигналов с минимизацией переходов – Transition Minimised Differential Signalling (TMDS). Фактически, данный стандарт объединяет три подвида: только аналоговый DVI-A, передающий аналоговый сигнал в формате VGA, чисто цифровой DVI-D и совмещенный DVI-I, объединяющий DVI-A и DVI-D в одном разъеме. Виды разъемов DVI представлены на рис. 10 [14].

Рис. 10. Виды разъемов DVI

Поскольку в DVI-A и DVI-I интерфейсах для совместимости с интерфейсом VGA видеоинформация продублирована в аналоговом виде то она, так же, как и у ЭЛТ-мониторов может быть перехвачена злоумышленником. Перехват информации, передаваемой по интерфейсу DVI-D, возможен лишь при условии, что ПЭМИ будут образоваться только в одном из трех цифровых RGB каналов.

Проведенный анализ мониторов ПЭВМ показал, что существует потенциальная возможность перехвата информации, выводимой на экран монитора.

Анализ возможности возникновения ПЭМИ в накопителях информации

Накопители на магнитных носителях, с точки зрения специалиста в области специальных исследований, должны разделяться, как минимум, на две части каждый – интерфейс связи между накопителем и системной шиной и цепь между узлом записи/считывания и внутренним контроллером. Для накопителя на жестком диске наиболее распространены интер-

зи между накопителем и системной шиной и цепь между узлом записи/считывания и внутренним контроллером. Для накопителя на жестком диске наиболее распространены интерфейсы: параллельный – *IDE* (минимум 32-разрядный) и последовательный – *SATA*. Для накопителя на дискете – последовательный, с тактовой частотой 250 *кГц* [15]. Цепи записи имеют последовательный код и их тактовые частоты и длительности импульсов постоянны только для дискет. Оптические диски разных моделей по интерфейсу, обычно – параллельные, по узлам считывания/записи – последовательные.

Наибольший интерес для злоумышленника представляет съём информации с жесткого диска. Однако перехват сопровождается помеховыми сигналами от того же диска, вызванными обращениями к нему системных служб операционной системы и запущенным программным обеспечением. Кроме того источник ПЭМИ – головка чтения/записи, находится внутри двойного экрана образованного корпусом жесткого диска и корпусом системного блока. Поэтому жесткие диски можно считать относительно защищёнными, в плане утечки информации через ПЭМИ, устройствами.

Экспериментальное исследование потенциально – опасных устройств ПЭВМ

В данной работе используется косвенный метод оценки защищенности информации, обрабатываемой ПЭВМ от возможной ее утечки за счет ПЭМИ. Он не использует проведение фактического обнаружения сигнала и основывается на применении в информационных излучающих цепях ПЭВМ тестовых сигналов в виде периодической последовательности информационных импульсов.

Для исследования ПЭМИ использовалась методика, описанная в [16]. Состав оборудования представлен на рис. 11 и включает в себя:

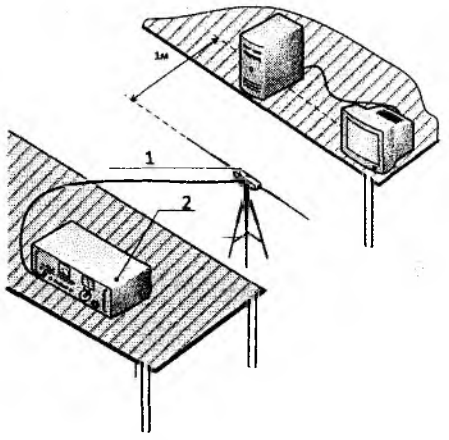


Рис. 11. Общий вид измерительной установки

1) антенны *DP3* (300 – 1000 *МГц*), *DP1* (80 – 300 *МГц*), рамочная антенна КВ-диапазона;

2) селективные микровольтметры *SMV 8.5*, *STV 303*.

Для того чтобы определить наиболее вероятный источник ПЭМИ в видеотракте ПЭВМ (рис. 12), проведены его экспериментальные исследования.

С помощью селективного микровольтметра *SMV – 8.5* выполнялся поиск сигналов, излученных всеми блоками видеотракта при включенном тестовом сигнале в диапазоне частот 110…600 *МГц*. Для исследования ПЭМИ отдельных блоков видеотракта ПК применялась следующая методика:

1. Измеряется общее излучение видеотракта при всех подключенных составляющих U_{Σ};
2. Измеряется уровень сигнала с отключенным монитором U';
3. Измеряется уровень сигнала с отключенным монитором и кабелем U''.

Далее рассчитываются уровни излучения отдельных составляющих видеотракта:

$$U_{\Sigma}{}^2 = U_{ву}{}^2 + U_{вк}{}^2 + U_a{}^2, \quad U_{ву} = \sqrt{U_{\Sigma}{}^2 - \left(U_{вк}{}^2 + U_a{}^2\right)},$$

$$U_{вк}{}^2 = (U')^2 - (U'')^2, \quad U_a = U'',$$

где U_{Σ} – уровень общего излучения видеотракта; $U_{ву}$ – уровень излучения видеоусилителя; $U_{вк}$ – уровень изучения видеокабеля; U_a – уровень сигнала видеоадаптера.

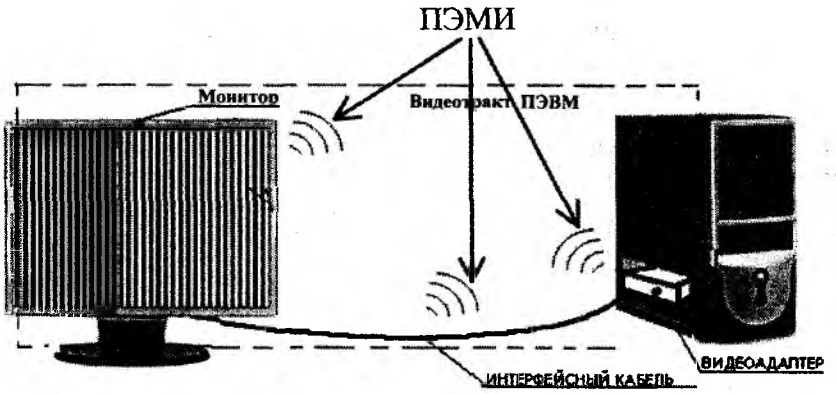


Рис. 12. Источники опасных сигналов в видеотракте ПЭВМ

Соотношение количества их ПЭМИ приблизительно одинаковое. Но по уровню излучений, монитор можно считать основным источником опасного сигнала. Результаты исследований занесены в табл. 1.

Таблица 1

Результаты экспериментального исследования ПЭМИ отдельных блоков ПЭВМ

Блок видеотракта	Модели монитора											
	Samsung 765MB (17",ЭЛТ)*		*LG 575* (15",ЭЛТ) *		*Samsung 940 NW*(19",ЖК) *		*LG W2242T* (22",ЖК)**		*Packard Bell A520* (15")*		*Packard Bell A727/P**	
	Напряжение на входе селективного микровольтметра, *мкВ*											
Частота, *МГц*	190	1142	140	220	133	168	174	390	130	292	118	426
Видеоадаптер U_a	1	1	0	0	1	0	0	0	0	0	0	0
Видеокабель $U_{вк}$	4,5	6,9	2	1,7	2	0	0	2,8	1	2,5	15,8	1,6
Видеоусилитель $U_{ву}$	27,8	39,2	7	6,8	2,6	5	6,5	0	100	13	8	8,8
Общее излучение U_{Σ}	28,2	39,8	7,244	7	3,98	5	6,45	2,8	100	13,3	17,7	8,91

Примечание: *подключение по аналоговому интерфейсу (*VGA*); ** – по цифровому интерфейсу (*DVI*).

Проведено подробное исследование видеотракта с монитором *Packard Bell A727/P* (17", ЭЛТ). Результаты сведены в табл. 2.

Таблица 2

Результаты исследования видеотракта с монитором *Packard Bell A727/P*

F, *МГц*	118	119	142	166	178	189	212	238	260	282	308	332	356	379	403	425	450	478	535
Uc, *мкВ*	46	11	51	23	2	25	4	19	3	3	3	3	13	11	22	27	3	2	8
Источник ПЭМИ	к	к	к	к	к	м	м	м	м	к	к	м	м	м	м	м	м	к	к

Примечание: к – основной источник ПЭМИ – видеокабель; м – основной источник ПЭМИ – видеоусилитель.

В работе проведен эксперимент по исследованию ПЭМИ лазерных и матричных принтеров (табл.3 – 4).

Таблица 3

ПЭМИ лазерного принтера *HP 1300*

Частота ПЭМИ, *МГц*	Напряжение сигнала + шум, *дБ*	Напряжение шума, *дБ*	Напряжение сигнала, *мкВ*
130	24	10	15
300	35	3	56
470	13	8	3
980	-3	-5	0,4

Таблица 4

Результаты экспериментального исследования матричного принтера *EPSON LX – 1050*

Частота ПЭМИ, *МГц*	Напряжение сигнала + шум, *дБ*	Напряжение шума, *дБ*	Напряжение сигнала, *мкВ*
148	53	34	40
166	37	25	27
292	59	22	54
675	30	24	18
900	28	13	24
970	20	14	14

Полученные результаты подтверждают наличие потенциально-опасных ПЭМИ принтеров.

Результаты исследования ПЭМИ клавиатур ПЭВМ приведены в табл. 5-7.

Таблица 5

Результаты экспериментального исследования клавиатуры GEMBIRD

Частота ПЭМИ, *кГц*	Напряжение сигнала + шум, *дБмк*В	Напряжение шума, *дБмк*В	Напряжение сигнала, *мкВ*
123	20	7	9,7
156	16	9	5,6
175	26	12	19,5
203	32	15	39,4
231	8	6	1,5
258	18	14	6,2

Таблица 6

Результаты экспериментального исследования клавиатуры Fitper

Частота ПЭМИ, *кГц*	Напряжение сигнала + шум, *дБмкВ*	Напряжение шума, *дБмкВ*	Напряжение сигнала, *мкВ*
125	5	4	0,8
155	11	10	1,6
170	10	8	1,9
200	14	13	2,2
235	19	17	5,4
265	15	13	3,4
280	21	19	6,8
300	25	24	8
431	26	25	9

Таблица 7

Результаты экспериментального исследования клавиатуры Genius KB-06X2

Частота ПЭМИ, кГц	Напряжение сигнала + шум, дБмкВ	Напряжение шума, дБмкВ	Напряжение сигнала, мкВ
117	10	9	1,4
124	5	4	0,8
150	22	19	8,8
172	24	23	7,2
210	30	28	19,2
270	20	18	6
300	14	12	3
350	7	4	1,6
430	16	12	4,8
620	21	20,3	4,3
700	10	6	2,4

Полученный экспериментальный материал подтверждает наличие побочного излучения клавиатуры ПЭВМ. Клавиатуры с экранированным интерфейсным кабелем (например, Mitsumi KFK-EA4SA) ПЭМИ практически не имеют.

Выводы

В работе решается актуальная научно-прикладная задача выявления наиболее опасных источников ПЭМИ в ПЭВМ. Получены следующие результаты:

1. Выявлены наиболее опасные, с точки зрения утечки информации через ПЭМИ, устройства современных ПЭВМ, которыми являются мониторы, принтеры, клавиатура.

2. Экспериментально подтверждено наличие в выявленных устройствах побочных излучений.

3. Полученные результаты могут быть полезны для составления общей модели канала утечки информации через ПЭМИ, что позволит предварительно рассчитать зону защищенности на этапе строительства (реконструкции) объекта информационной деятельности, на котором обрабатывается информация с ограниченным доступом.

Список литературы: 1. *Wim van Eck, I. Neessen* and *P. Rijsdijk.* On the electromag-fields generated by video display units // Proc. symp. EMC. Zurich, March 1985. 2. *Волокитин, А.В., Маношкин, А.П., Солдатенков, А.В., Савченко, С.А., Петров, Ю.А.* Информационная безопасность государственных организаций и коммерческих фирм : Справочное пособие / под общей ред.Реймана Л.Д. – М. : НТЦ «ФИОРД-ИНФО», 2002. – 272с. 3. *Gorobets, N.N., Trivaylo,* A.V. Compromising emanations: overview and system analysis // Вісник Харк. нац. ун-ту ім. В.Н.Каразіна. Сер."Радіофізика та електроніка". № 883, вип. 15. – 2009. – С. 83-88. 4. *К вопросу* оценки уровня ПЭМИ цифрового электронного оборудования – режим доступа: http://kievsecurity.org.ua/box/7/K_voprosu_ocenki_urovnya_PEMI_cifrovogo_elektronnogo_oborudovaniya_p-5-.shtml 5. *Петраков,А. В.* Основы практической защиты информации : учеб.пособие. – М. : Радио и связь, 2001. – 368с 6. *Косарева, В.П., Королева, А.Ю.* Экономическая информатика и вычислительная техника. – М. : Финансы и статистика, 1996. 7. *Спесивцев, А., Вегнер, В., Крутяков, А., Серегин, В., Сидоров, В.* Защита информации в персональных ЭВМ. – М. : Радио и связь, МП "Веста", 1992. – 192 с. 8. *Гук, М.* Интерфейсы ПК : Справочник. – Спб. : ЗАО «Издательство Питер», 1999. – 416с. 9. *Пятачков, А.Г.* Защита информации, обрабатываемой вычислительной техникой, от утечки по техническим каналам. – М. : НП РЦИБ «Факел», 2007. 10 *Новиков, Ю., Черепанов, А.* Персональные компьютеры: аппаратура, системы, Интернет : учеб. курс. – СПб. : Питер, 2002. 11. *Михеева, Е.В.* Информационные технологии в профессиональной деятельности : учеб. пособие для сред. проф.образования. – М. : Изд. центр «Академия», 2004. 12. *Видеоадаптеры* и интерфейсы мониторов – режим доступа: http://www.sd-company.su/article/ computers/adapters_interfaces_monitors 13. *Обзор* технологий дисплеев на жидких кристаллах – режим доступа: http://itc. ua/articles/ obzor_tehnologij_displeev_na_zhidkih_kristallah_1457/.14. Цифровой Визуальный Интерфейс (Digital Visual Interface). – режим доступа: http://www.xserver.ru/ computer/computer/video/1/ 15. *Бузов, Г.А. , Калинин, С.В., Кондратьев, А.В.* Защита от утечки информации по техническим каналам. – 2005. – 416с. 16. *Зайцев, А.П., Шелупанов, А.А., Мещеряков, Р.В.* Технические средства и методы защиты информации. – М. : ООО «Изд-во Машиностроение», 2009. -508с.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 11.04.2012