СИСТЕМЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 004.056.53

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

КОНЦЕПЦИЯ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ ВИДЕОСИСТЕМ

Введение

С развитием технологий получения и обработки информации все больше актуализируются проблемы информационной безопасности. Поскольку успех работы механизмов безопасности реальной системы во многом зависит от индивидуальных особенностей ее построения, а также от условий эксплуатации, ни один из существующих традиционных методов защиты назвать универсальным нельзя.

С точки зрения утечки информации особую опасность представляют побочные электромагнитные излучения и наводки (ПЭМИН) средств вычислительной техники (СВТ), участвующих в процессе передачи, обработки и хранения конфиденциальной информации. Среди таких СВТ: мониторы персональных электронно-вычислительных машин (ПЭВМ), клавиатура, принтеры, проводные линии связи.

Опыт эксплуатации этих средств обработки информации показывает, что проблема обеспечения безопасности еще далека от своего решения, а предлагаемые производителями средства защиты сильно различаются как по решаемым задачам и используемым методам, так и по достигнутым результатам. Объективным критерием выбора средств защиты является соотношение их эффективности и стоимости. Все это и определяет сегодня актуальность проблемы построения защищенных систем обработки информации.

Постановка задачи

Несмотря на большое количество публикаций по вопросу построения защищенных информационных систем, к сожалению, до настоящего времени отсутствует единый подход к построению защищенной видеосистемы.

Учитывая всю сложность обеспечения максимальной защиты информации, обрабатываемой и передаваемой в компьютерных системах, для построения новой, более защищенной информационной системы, необходимо провести анализ уязвимостей в существующих, используемых для обработки конфиденциальной информации СВТ. Проведение такого анализа позволит выявить, обобщить, классифицировать причины и закономерности появления и существования уязвимостей СВТ.

Цель статьи – разработка концепции построения защищенной видеосистемы, основанной на использовании оптимизации структуры устройства обработки информации, а также изменении структуры данных выводимой видеоинформации.

Основные положения

Поскольку рассматривается угроза утечки информации, посредством ПЭМИН в средствах ПЭВМ, необходимо рассмотреть конструктивные особенности средств обработки информации, условия их размещения и эксплуатации, структуру и параметры полей, создаваемых их элементами.

В составе современной ПЭВМ есть устройства, выполняющие вспомогательные функции, по которым передаются сигналы, которые не содержат конфиденциальную информацию (неинформативные ПЭМИ), и потенциально-опасные устройства, по которым, непосредственно передаются сигналы, содержащие конфиденциальную информацию (потенциально-опасные излучения). Также известно, что наибольшую опасность представляет излучение тех устройств, в которых защищаемая информация циркулирует в виде последовательного кода [1].

Условия возникновения ПЭМИН такой ПЭВМ:

- большие значения паразитных индуктивностей и емкостей устройств ПЭВМ;

- наличие шлейфов, соединяющих элементы внутри ПЭВМ, по которым текут электрические токи информативных;

- большие длины совместного пробега соединительных линий технических средств передачи информации и посторонних проводников;

- неэкранированные (либо слабо экранированные) провода;

- элементная база с высоким уровнем излучения сигналов [2 – 3].

Наряду с определением понятия «защита информации» важным вопросом является классификация имеющихся способов и средств защиты, которые позволяют воспрепятствовать запрещенному (незаконному) ее использованию.

В настоящее время существуют традиционные методы защиты от ПЭМИН: зашумление, экранирование и фильтрация [1] (рис. 1). Наряду с достоинствами эти методы также имеют ряд недостатков.

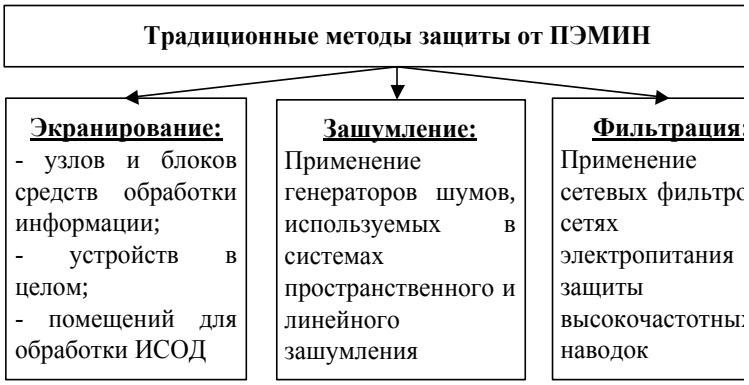


Рис. 1. Традиционные методы защиты от ПЭМИН

Достоинства и недостатки традиционных методов защиты от ПЭМИН.

1. *Экранирование.*

Данный метод позволяет снизить уровень побочных электромагнитных излучений (информационных сигналов) СВТ на границе контролируемой зоны до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов; позволяет улучшить электромагнитную совместимость (ЭМС), при работе устройств обработки информации. Также посредством экранирования снижается вредное воздействие электромагнитного излучения (ЭМИ) на организм человека. Однако данный метод имеет ряд недостатков: электромагнитное экранирование помещений в широком диапазоне частот является сложной технической задачей, требует значительных материальных затрат, постоянного контроля и не всегда возможна по эстетическим и эргономическим соображениям; усложняется использование санкционированных средств связи в экранируемом помещении;

2. *Зашумление.*

Применяется для защиты информации, обрабатываемой СВТ любой категории, как по каналу утечки информации за счёт электромагнитных излучений, так и за счёт наводок на линии основных и вспомогательных технических средств и систем, при этом усложняется съем информации с помощью маломощных закладных подслушивающих устройств, установленных в «зашумляемом» помещении. К недостаткам зашумления можно отнести следующее: в одной точке пространства уровень излучения источника помех превышает уровень излучения компьютера, а в другой точке пространства или на другой частоте это может и не обеспечиваться, поэтому после установки источников шума необходимо проведение сложных измерений по всему периметру охраняемой зоны и для всех частот. Процедуру проверки необходимо повторять всякий раз, когда просто изменяется расположение компьютеров, а также при установке новых.

- данный метод предполагает использование достаточно мощного источника излучения (генератора шума), что вносит дополнительное вредное воздействие на здоровье человека;

- может внести помехи легитимным радиоэлектронным устройствам (например, системам телевидения, радио и т.п.);

- наличие маскирующего устройства свидетельствует о наличии конфиденциальной информации в данном помещении.

3. *Фильтрация.*

Обеспечивает защиту аппаратуры от внешних импульсных помех и защиту от наводок, создаваемых самой аппаратурой. Однако узкая направленность данного метода защиты (защита только от паразитных наводок), не позволяет комплексно подойти к вопросу обеспечения безопасности обрабатываемой техническими средствами информации.

Концепция построения защищенной видеосистемы

Защищенная система обработки информации для определенных условий эксплуатации должна обеспечивать безопасность (доступность, конфиденциальность и целостность) обрабатываемой информации и поддерживать свою работоспособность в условиях воздействия на нее заданного множества угроз.

В данной работе предложена концепция построения защищенной информационной системы, основанная на использовании оптимизации структуры устройства обработки информации, а также преобразования самой видеоинформации (рис.9).

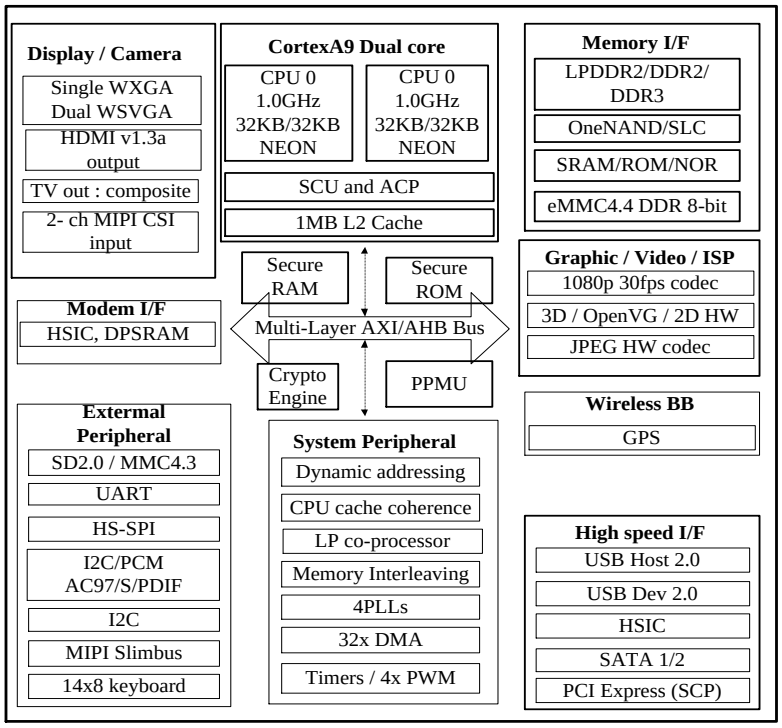


Рис. 2. Схема устройства платформы системы планшета на чипе фирмы Samsung — S5PV310 Exynos 4210 (в основе — ARM Cortex-A9)

Основным положением предложенной концепции является использование, в качестве средства обработки конфиденциальной информации, ПЭВМ, построенную на основе SoC (System on chip) – архитектуры.

Сегодня существует несколько видов архитектур, на которых строятся SoC. Одними из наиболее распространённых, сегодня являются устройства на основе RISK (APM) архитектуры (рис. 2) и CISK (x86-архитектуры) [4].

Благодаря своему конструктивному исполнению (большинство основных устройств расположены на одном кристалле) и маломощной элементной базе устройства, на основе SoC-архитектуры, обеспечивают следующие преимущества при работе с конфиденциальной информацией:

- отсутствие длинных шлейфов внутри устройства основе SoC-архитектуры, по которым циркулируют токи, несущие конфиденциальную информацию;
- использование в данных устройствах маломощной элементной базы с низким уровнем информативных сигналов.

Рассмотрим положения разработанной концепции.

Структурная оптимизация устройства обработки конфиденциальной информации

Особенностями данного положения концепции являются:

1. Использование оптических интерфейсных линий:
   - оптические каналы связи не порождают ПЭМИН;
   - обеспечивают высокую скорость передачи данных;
   - не подвержены воздействию электромагнитных помех.

2. Изменение конструкции устройства обработки информации подразумевает:

- уменьшение длин совместного пробега соединительных линий СВТ и посторонних проводников;

- использование маломощной элементной базы в конструкции устройства обработки конфиденциальной информации;

3. Использование фильтров в сигнальных цепях.

При передаче информации от видеокарты на монитор, с помощью фильтра низких частот из всего спектра сигнала, поступающего на монитор, можно блокировать спектральную составляющую ПЭМИН (рис.3).

На рис. 4 изображено прохождение сигнала через фильтр.

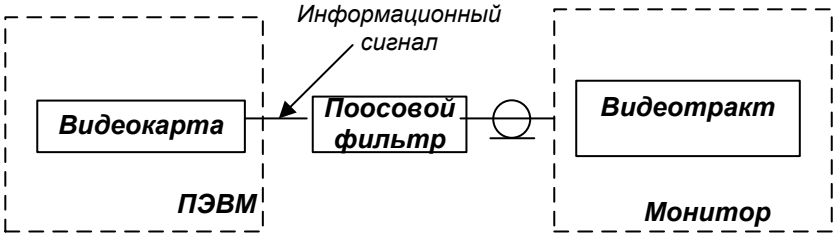


Рис. 3. Применение фильтра в сигнальных цепях

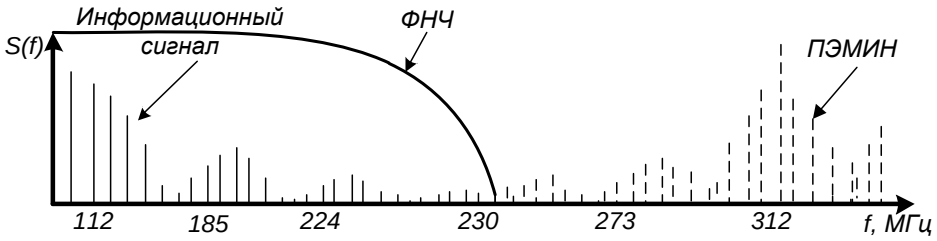


Рис. 4. Фильтрация сигнала

4. Гальваническая развязка в системе питания.

Для исключения утечки информации по цепям питания применяют разделительные трансформаторы, помехоподавляющие фильтры и мотор-генераторы. При малых потребляемых токах применяют помехоподавляющие фильтры. При больших – разделительные трансформаторы и мотор-генераторы [5].

Разделительные трансформаторы должны обеспечивать развязку первичной и вторичной цепей по сигналам наводки. Это означает, что во вторичную цепь трансформатора не должны проникать наводки, появляющиеся в цепи первичной обмотки. Проникновение наводок во вторичную обмотку объясняется наличием нежелательных резистивных и емкостных цепей связи между обмотками.

Для уменьшения связи обмоток по сигналам наводок часто применяется внутренний экран, выполняемый в виде заземленной прокладки или фольги, укладываемой между первичной и вторичной обмотками.

Для исключения просачивания информационных сигналов в цепи электропитания используются фильтры нижних частот. Помехоподавляющие фильтры позволяют снизить помехи от внешних и от внутренних источников помех.

Помехоподавляющие фильтры позволяют оптимизировать схемотехнические и конструкторские решения с целью минимизации или полного устранения паразитных генераций и побочных излучений, снизить восприимчивость аппаратуры к внешним электромагнитным полям и импульсным сигналам, устранить возможные каналы утечки информации. Повышается надежность аппаратуры.

К достоинствам мотор-генераторов (умформеров) можно отнести их способность осуществлять:

- гальваническую развязку входной и выходной цепей;
- получение на выходе почти идеального синусоидального напряжения, без шумов, связанных с работой других потребителей сети;
- простоту устройства и его обслуживания;
- устойчивость к радиации;
- возможность получения на выходе трехфазного напряжения без существенного усложнения конструкции;
- фильтрация бросков тока при резком изменении нагрузки или кратковременном отключении питающего напряжения за счет инерции ротора;
- высокий КПД преобразования, достигающий 97 – 98%.

Однако мотор-генераторы имеют ряд недостатков:

- сравнительно низкий ресурс из-за наличия движущихся частей;
- высокая масса и стоимость за счет материалоёмкости конструкции;
- вибрация и шум;
- необходимость технического обслуживания (смазка подшипников, чистка коллекторов, замена щеток в коллекторных машинах).

Использование перечисленных средств позволяет полностью исключить утечку информации по цепям питания.

Изменение структуры потока данных выводимой видеоинформации

Данное положение разрабатываемой концепции включает следующие задачи:

1. Передача имитационного помехового сигнала параллельно с информационным.

Одним из наиболее эффективных методов препятствия перехвату информации по радиотехническому каналу является активная радиомаскировка [5]. Суть этого метода заключается в излучении защищенным устройством имитационного помехового сигнала, уровень которого превышает уровень ПЭМИ по всему диапазону (рис.5).

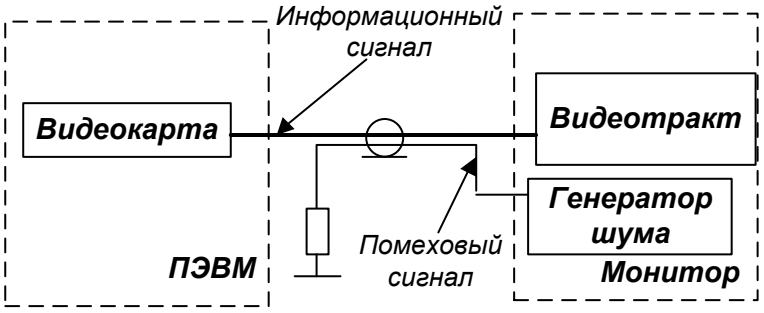


Рис.5. Передача имитационного помехового сигнала параллельно с информационным

2. Переход от последовательной передачи видеосигнала к параллельной.

Наибольшую опасность представляет излучение тех устройств, в которых защищаемая информация циркулирует в виде последовательного кода [2]. А значит, для снижения информативности сигналов ПЭМИН и затруднения использования их при перехвате, необходимо осуществить с помощью специальных решений таких как:

- замена последовательного кода передаваемой информации параллельным;
- увеличение разрядности параллельных кодов.

2. Нарушение регулярности повторения выводимой информации.

Регулярность повторения выводимой от видеокарты на монитор конфиденциальной информации определяется числом повторения кадров за секунду и скоростью «пролистывания» документа и при несанкционированном съёме информации может обеспечить злоумышленнику возможность накопления информационного сигнала, что позволит существенно повысить отношение сигнал/шум. Регулярность вывода информации (кадров) для стандартного TFT- монитора составляет 60 *кадров/с*. Нарушив эту регулярность можно снизить дальность канала утечки информации.

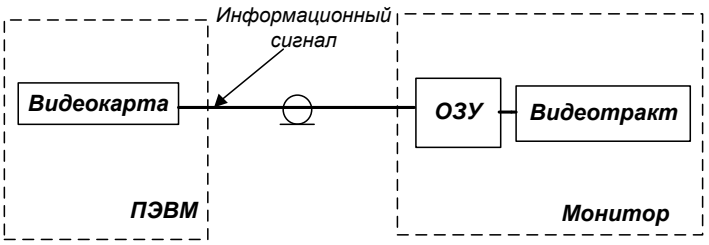
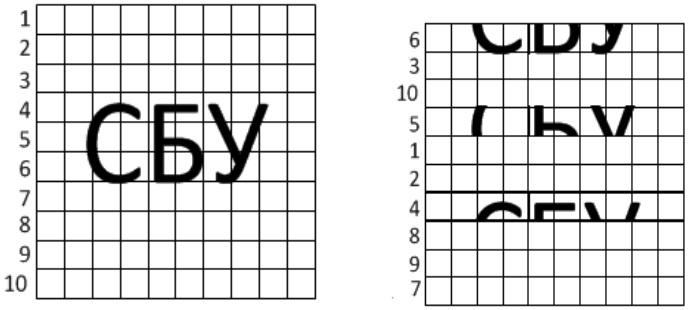


Рис. 6. Нарушение регулярности повторения выводимой информации

Для этого в мониторе должно находиться ОЗУ (рис. 6), в котором запоминается последний кадр и в последующем монитор считывает информацию уже не с видеокарты, а с собственного запоминающего устройства до тех пор, пока не изменится выводимое изображение. Видеокарта при этом передаёт статическое изображение только один раз.

3. Изменение очередности передачи строк выводимой информации.

Метод заключается в замене исходной последовательности строк выводимого изображения по определенному алгоритму, не известному злоумышленнику (рис.7). Такое преобразование усложнит расшифровку сообщения в случае его перехвата.



а *б*

Рис.7. Вывод изображения на монитор ПЭВМ:
а – передача 1-го кадра изображения на монитор с исходной последовательностью строк;
б – передача 2-го кадра изображения на монитор с новой последовательностью строк, зашифрованной по определенному алгоритму

4. Разработка специальных TEMPEST-шрифтов.

Идея таких шрифтов основана на том, что злоумышленнику доступны только высокочастотные компоненты видеосигнала. То есть, если удалить верхние 30 % преобразования Фурье сигнала, сворачивая его подходящим НЧ-фильтром (что незначительно скажется на качестве изображения на экране пользователя), то перехватываемая текстовая информация полностью исчезает с перехватывающего монитора, даже если антенна расположена вплотную к видеодисплею [6].

К особенностям таких шрифтов, позволяющим уменьшить уровень ПЭМИН (рис.8), относятся сглаженные, размытые края шрифта.

а *б*

Рис. 8. Шрифты: *а* – стандартный Times New Roman; *б* – TEMPEST

5. Криптографическое преобразование информации:

Под криптографической защитой информации понимается преобразование исходной информации, включающее её шифрование, создание имитированной вставки, или цифровой подписи.

Известны различные подходы к классификации методов криптографического преобразования информации. По виду воздействия на исходную информацию методы криптографического преобразования информации могут быть разделены на три группы: 1) шифрование; 2) стеганография; 3) кодирование [7];

Процесс шифрования заключается в проведении обратимых математических, логических, комбинаторных и других преобразований исходной информации, в результате которых зашифрованная информация представляет собой хаотический набор букв, цифр, других символов и двоичных кодов.

Для шифрования информации используются алгоритм преобразования и ключ. Как правило, алгоритм для определенного метода шифрования является неизменным. Исходными данными для алгоритма шифрования служат информация, подлежащая шифрованию, и ключ шифрования. Ключ содержит управляющую информацию, которая определяет выбор преобразования на определенных шагах алгоритма и величины операндов, используемые при реализации алгоритма шифрования. Преобразование шифрования может быть симметричным (с одним ключом) или ассиметричным (с двумя ключами) относительно преобразования расшифрования [8].

В отличие от других методов криптографического преобразования информации, методы стеганографии позволяют скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации.

Содержанием процесса кодирования информации является замена смысловых конструкций исходной информации (слов, предложений) кодами. При кодировании и обратном преобразовании используются специальные таблицы или словари.

На рис. 9 показана разработанная концепция построения защищенной видеосистемы с использованием устройств на основе Soc-архитектуры.

Рис.9. Концепция построения защищенной видеосистемы

Разработанная концепция позволит обеспечить защиту видеоинформации от утечки через ПЭМИН в видеосистеме без использования дополнительных внешних средств защиты.

Выводы

Предложена концепция построения защищенных видеосистем, учитывающая максимально возможный спектр угроз, которые приводят к утечке информации через ПЭМИН, при работе незащищенных ПЭВМ. Данная концепция основана на использовании оптимизации структуры устройства обработки информации и на изменении структуры потока данных видеоинформации.

Основной идеей разработанной концепции является предложение использовать в качестве средства обработки конфиденциальной информации персональную электронно-вычислительную машину, построенную на основе SoC-архитектуры. SoC-архитектура сегодня широко используется в планшетах и смартфонах.

Несмотря на то, что применение непосредственно планшетов и смартфонов для обработки конфиденциальной информации имеет ряд ограничений, сама идея построения защи всё большую популярность завоёвывают однокристальные ПЭВМ, вмонтированные в монитор (моноблоки).

Другим перспективным направлением является разработка специальных шрифтов, что позволит повысить защищенность уже существующих и используемых видеосистем.

Список литературы:. 1**.** *Петраков А. В.* Основы практической защиты информации : учеб. пособие. ; 3-е изд. – М. : Радио и связь, 2001. – 368с. 2. *Лыков Ю.В., Сягаева О.А.* Анализ источников ПЭМИ в современных ПЭВМ // Радиотехника. – 2012. 3. *Каторин Ю.Ф., Разумовский А.В., Спивак А.И.* Защита информации техническими средствами : учеб. пособие**.** – СПб. : НИУ ИТМО, 2012. – 416 с. 4. *Солонина А.И. и др.* Алгоритмы и процессоры цифровой обработки сигналов. – СПб. : БХВ – Петербург, 2001. – 464 с. 5. *Хорев А.А.* Способы и средства зашиты информации. – М. : МО РФ, 2000. – 316 с. 6. *Kuhn M., Anderson R.,* Soft TEMPEST: Hidden Data Transmission Using Electromagnetic Emanations // Workshop on Information Hiding, LNCS 1525, Springer-Verlag, 1999. 7. *НД ТЗІ 1.1-003-99***.** Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу (НД ТЗІ 1.1-003-99). – К. : ДСТСЗІ СБ України, 1999. – 21 с. 8. *Соколов А.В., Степанюк О.М.* Защита от компьютерного терроризма : справ. пособие. – СПб. : БХВ – Петербург, 2002. – 496с. (с.309-330, 417-435).

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 12.02.2013