

Список литературы:

1. Кнут Д. Искусство программирования для ЭВМ. Т. 2. – М.: Мир, 2001. – 730 с.
2. Задирака В. К., Мельникова С. С. Анализ сложности алгоритма умножения сверхбольших чисел на основе коэффициентов Уолша//Кибернетика и системный анализ. – 2001. – № 6. – С. 99-110.
3. Pitassi D. A. Fast convolution using the Walsh transform//Appl. of Walsh Funktions. – 1971. – P. 130-133.
4. Толстых Г. Д. Сверхбыстрое спектральное преобразование по функциям Хаара//Изв. вузов – радиоэлектроника. – 1979. – № 7. – С. 86-89.
5. Andrews H. C. Computer Techniques in Image Processing, New York: Academic Press, 1970, pp. 73-90.
6. Alexits G. Convergence Problems of Orthogonal Series, New York: Pergamon, 1961, pp. 46-62.
7. Файн Б. Связь между преобразованиями Хаара и Уолша-Адамара//ТИИЭР, 1972. №5.

УДК 681.3

С.Р. Коженевский, Г.Т. Солдатенко

**ЗАЩИТА ИНФОРМАЦИИ В ЦЕПЯХ ЭЛЕКТРОПИТАНИЯ
ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА**

Что имеем – не храним,
Потерявши – плачем.
Народный ЭПОС

В современном мире большие объемы информации обрабатываются, хранятся и передаются электронными методами, и, следовательно, сопровождаются электромагнитными излучениями. Поэтому существует реальная возможность несанкционированного доступа к этой информации посредством радиоперехвата или контактного подключения к коммуникациям [2]. В подтверждение этому достаточно привести такие примеры.

В отчетах Агентства Национальной Безопасности США опубликованы сведения о том, что около 80% разведывательной информации поступает по техническим каналам утечки информации за счет радиоперехвата.

Фирма «ЕПОС» и ЦТЗИ «Барьер» ОАО «НИИЭМП» демонстрировали на выставке EnterEx-2001 перехват информации с монитора по радиоканалу с помощью радиолобительских устройств.

Но информацию можно перехватить и путем подключения к цепям электропитания. Так, в частности, на рис. 1 показана установка, с помощью которой мы демонстрируем возможность перехвата информации, отображаемой на мониторе компьютера, путем анализа напряжения в линии электропитания.

В установке применены стандартные приборы: селективный вольтметр SMV-11, эквивалент сети NNB-111, осциллограф С1-65А.

Персональный компьютер является центральным звеном в информационных системах обработки информации и находится в зоне пристального внимания конкурентов, злоумышленников и разведывательных служб. Для получения информации используются все доступные средства, в том числе и различные анализаторы, подключаемые к линиям электропитания.

Прежде чем приступить к рассмотрению обозначенной проблемы необходимо дать некоторые пояснения используемой терминологии.

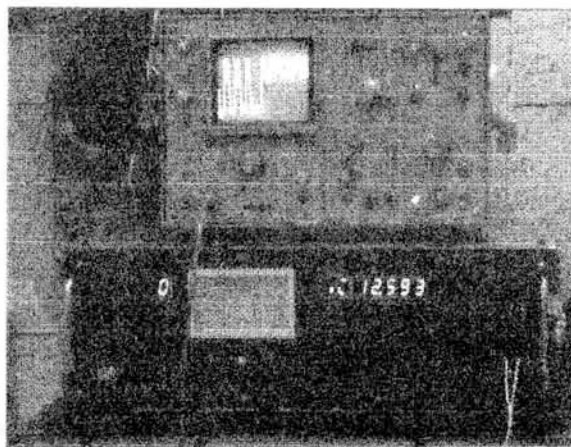


Рис. 1 Демонстраційна установка

Что следует понимать под термином технический канал утечки информации?

Под техническим каналом утечки информации в общем случае следует понимать способ получения с помощью технических средств разведывательной информации (независимо от формы ее представления) об объекте.

При организации защиты информации необходимо рассматривать всю совокупность основных технических средств, хранящих и обрабатывающих информацию с ограниченным доступом, соединительно-распределительное и коммутационное оборудование, систему электропитания и заземления, а также вспомогательные технические средства, такие как телефонная связь, пожарная и охранный сигнализация, коммуникации которых выходят за пределы контролируемой зоны.[2]

Технические каналы утечки информации в зависимости от физической природы образования и среды распространения побочных излучений и наводок разделяют на электромагнитные, электрические и параметрические. Электромагнитные и электрические каналы утечки информации формируются за счет электромагнитных излучений и наводок, модулированных сигналами, формируемыми в компьютере в процессе обработки информации. Параметрический канал утечки информации образуется за счет изменения параметров радиокомпонентов и элементов функциональных связей (выходящих за пределы контролируемой зоны), которые происходят при воздействии на них акустических полей и сигналов ВЧ-навязывания. Под ВЧ-навязыванием следует понимать контактный способ введения в кабели и провода, выходящие за пределы контролируемых зон, токов высокой частоты, которые при определенных условиях отражаются промодулированными информационными сигналами. Существует также канал утечки информации образуемый при помощи закладок (радиотрансляторов), устанавливаемых непосредственно в компьютер или в цепях электропитания. [2]

В настоящее время на рынке средств вычислительной техники доступны изделия в общепромышленном исполнении с зарубежными и отечественными сертификатами, подтверждающими, что эти изделия удовлетворяют требованиям действующих норм на уровни электромагнитного излучения. Как правило, подразумеваются медицинские нормы или нормы по обеспечению электромагнитной совместимости средств. Для обеспечения защиты информации соблюдение указанных норм оказывается недостаточным.

В общем случае источники электромагнитных излучений и наводок, среда и путь их распространения однозначно и неразделимо физически связаны с элементами компьютера, осуществляющими хранение, обработку или передачу информации, а также с паразитными контурами цепей электропитания и заземления.

Побочные электромагнитные излучения и наводки можно рассматривать как радиотехнические отходы процессов обработки информации и формирования вспомогательных сигналов управления и индикации. При этом все эти процессы сопровождаются возникновением колебаний на комбинационных частотах и различного рода шумами. Случайный характер образования побочных колебаний не позволяет однозначно определить способ гарантированного их подавления, т.е. в этом случае присутствует вероятностный подход. Подробный и исчерпывающий анализ процессов образования побочных излучений представлен в источнике [3]. Далее мы воспользуемся только некоторыми практическими рекомендациями по снижению влияния этих процессов на параметры каналов утечки информации.

В качестве объекта исследований возьмем систему электропитания компьютера в общепромышленном (бытовом) исполнении, т.е. то, что чаще всего предлагается на компьютерном рынке. Для электропитания персональных компьютеров чаще всего используют промышленную сеть переменного напряжения 220В 50Гц, реже – источники автономного электропитания (например, мотор-генераторы, дизель-генераторы или аккумуляторы), и только на специфических объектах применяют комбинированные источники электропитания. У каждого из этих источников электрической энергии есть достаточно весомые положительные и отрицательные факторы, которые определяются условиями эксплуатации и специальными требованиями.

В общем случае система электропитания персональных компьютеров решает следующие задачи:

- формирование стабилизированного постоянного напряжения;
- фильтрацию промышленных помех и помех от устройств компьютера;
- защиту потребителей электроэнергии от перегрузок и т.д.

Типовая структурная схема электропитания компьютера представлена на рис.2.

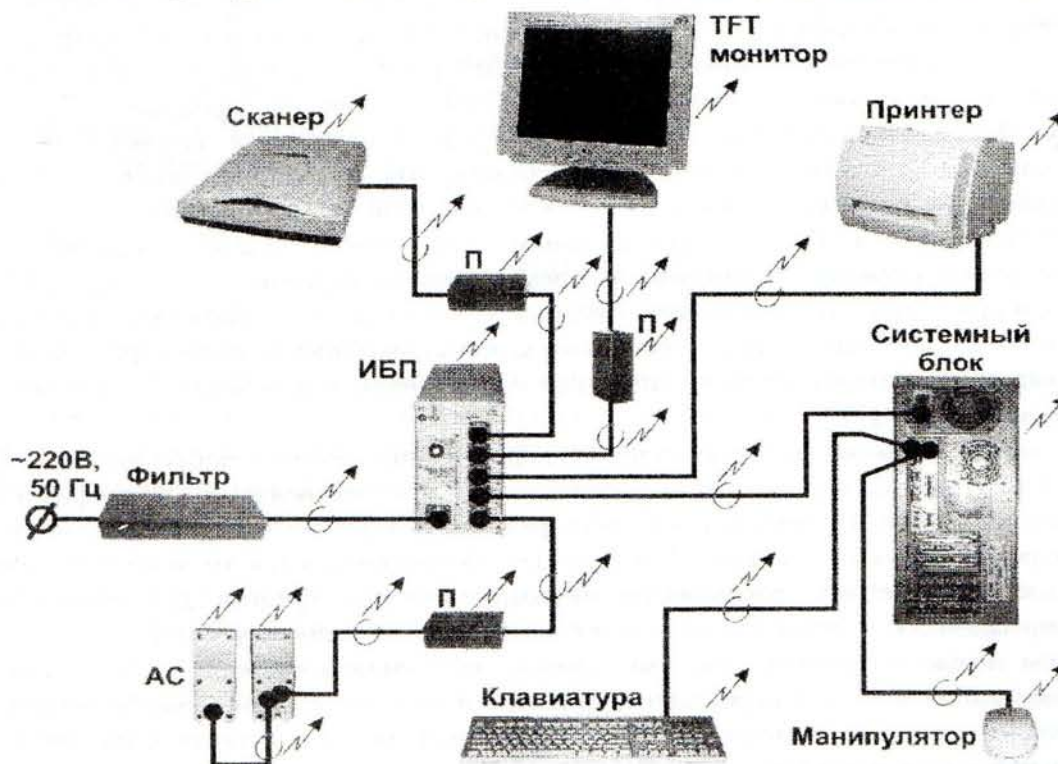


Рис.2. Типовая структурная схема электропитания компьютера.

Где:

- ИБП – источник бесперебойного питания;
- П – преобразователь переменного напряжения 220В в постоянное 12В;
- АС – акустическая система.

Первичными и общими устройствами электропитания для компьютера являются сетевой фильтр и ИБП, а распределение электропитания для отдельных устройств осуществляется по следующей схеме:

- сканер, акустическая система и TFT монитор потребляют электрическую энергию через соответствующие **преобразователи** переменного напряжения в постоянные 12В, конструктивно выполненные как **автономные** устройства (адаптеры);
- принтер получает электропитание непосредственно от первичной сети через фильтр или от ИБП (т.е. **преобразователь** переменного в постоянное напряжение **встроен** в принтер);
- устройства системного блока (НЖМД, НГМД, CD-ROM, материнская плата, видео и другие карты), клавиатура и мышь получают электропитание от сети ~220В 50Гц через **многоканальный блок вторичного питания, встроенный** в корпус системного блока, т.е. находящийся в одном конструктиве с устройствами обработки и хранения информации.

Из практики проектирования изделий с нормированными уровнями излучений известно, что для достижения цели необходимо минимизировать паразитные контуры и исключить их взаимное влияние. Как же, эти вопросы решены в типовой схеме электропитания компьютера?

1. Автономные преобразователи переменного напряжения в постоянное создают дополнительные паразитные контуры, такие как: первичная сеть – вход адаптера, выход адаптера – нагрузка; а встроенные преобразователи: первичная сеть – преобразователь – нагрузка.

2. Наличие общей точки (сетевой фильтр или ИБП) в схеме распределения электропитания для всех устройств компьютера создает условия для взаимного проникновения побочных колебаний от одного устройства в другие, например, от принтера к монитору и наоборот, не только путем излучения и наводок, но и непосредственно по цепям электропитания[4].

3. Общй многоканальный источник вторичного электропитания для устройств системного блока превращает задачу разделения паразитных контуров на практике в неразрешимую проблему.

Следует обратить внимание на весьма существенную особенность в электропитании лазерного принтера. При подготовке к печати принтер потребляет из сети ток в 5-10 раз больше указанного в паспорте, поэтому принтер подключают только к транзитному (белому) разъему ИБП, а если таковой отсутствует, то непосредственно к первичной сети или к выходу сетевого фильтра. Таким образом, цепь электропитания принтера образует дополнительный паразитный контур.

Отдельного рассмотрения заслуживает блок вторичного электропитания системного блока как источник побочных электромагнитных колебаний. В [5] детально представлена классификация электромагнитных помех, создаваемых блоками вторичного электропитания. Помехи от блоков вторичного электропитания создаются побочными колебаниями, возникающими в процессе его работы. Побочные колебания могут быть промодулированы сигналами, формируемыми в процессе обработки информации. В этом случае их можно перехватить и выделить содержащуюся информацию. Мы приведем только те виды помех,

которые имеют прямое отношение к формированию каналов утечки информации по цепям электропитания (Таблица 1).

Таблица 1

Вид помехи	Среда распространения	Факторы, обуславливающие распространение помех
Паразитное электромагнитное излучение	Пространство	Переключательные процессы активных радиокомпонентов
Кондуктивная – внутри корпуса блока вторичного питания	Объемный и печатный монтаж, шины заземления и элементы конструкции	Паразитная емкостная индуктивная связь между электрическими цепями
Кондуктивная симметричная	Прямой и обратный провода электропитания	Паразитная емкостная индуктивная связь между электрическими цепями
Кондуктивная асимметричная	Прямой и обратный провода электропитания относительно провода «земли»	Паразитная емкостная и индуктивная связь между электрическими цепями и заземляющим проводом

Данные таблицы 1 раскрывают характер процессов образования побочных излучений и наводок, а также факторов, обуславливающих их распространение в источнике вторичного электропитания и проводах, подводящих переменное напряжение. Источник вторичного питания является общим для всех устройств системного блока и получает электропитание непосредственно от первичной сети, следовательно, все паразитные контуры от разных устройств имеют общую точку, которая по цепи первичного электропитания соединена с устройствами за пределами контролируемой зоны.

Таким образом, перечисленные особенности схемы электропитания компьютера (рис.2), а, именно, не оптимизированное количество паразитных контуров, наличие у них общей точки, обеспечивающей взаимный обмен электромагнитными колебаниями, и многообразие видов паразитных колебаний источника вторичного питания создают условия для формирования технических каналов утечки информации. На рис.2. стрелками показаны потенциальные источники побочного излучения и наводок, а также пути распространения этих излучений.

Подводя итог вышеизложенному, приходим к выводам, что цепи электропитания компьютера и периферийных устройств могут образовывать каналы утечки информации двух видов:

1. Непреднамеренно образуемые за счет:

- побочного электромагнитного излучения цепями электропитания и устройствами компьютера;
- непосредственного изменения токов, напряжений, фаз и т.д. в первичной сети электропитания адекватного кодовым представлениям информации, обрабатываемой в компьютере.

2. Специально организованные:

- путем контактного введения сигналов ВЧ-навязывания в цепи электропитания и заземления с последующим приемом отраженных сигналов промодулированных информационными сигналами;
- сетевыми закладными устройствами, транслирующими по радиоканалу информационные сигналы.

К традиционным решениям по защите информации относятся:

- экранирование, как способ ослабления побочного электромагнитного излучения и наводок;
- использование автономных источников электропитания для обеспечения гальванической развязки с промышленной сетью;
- установка сетевых фильтров для подавления побочных колебаний, проникающих в сеть электропитания за счет кондуктивных связей;
- активный метод – зашумление (создание маскирующих помех) в пространстве и проводах.

Экранирование и автономные источники электропитания по-прежнему находят достаточно широкое применение, так как обеспечивают гарантированную надежную защиту информации с ограниченным доступом.

Активный метод, по нашему мнению, может применяться в ограниченных масштабах, поскольку он: экологически «грязный» (загрязняет эфир и сеть электропитания), биологически вреден для здоровья человека, не обеспечивает гарантированной защиты в широком диапазоне частот и является демаскирующим признаком объекта. Между тем, несмотря на факторы, отрицательно воздействующие на экологию и человека, **активный метод** защиты информации пропагандируется достаточно широко. Трудно понять авторов, агитирующих за применение метода. Очевидно, не наступило время осознания того, что простота или упрощенные методы достижения цели, привлекающие призрачной дешевизной, наносят непоправимый вред здоровью человека. [6]

Сетевые фильтры в последние годы претерпели существенное изменение как с точки зрения конструктивных и схемотехнических решений, так и вариантов их применения. В [7,8] проанализированы процессы фильтрации с точки зрения подавления паразитных колебаний и защиты информации, приведены рекомендации по выбору подавляющих фильтров. В рекомендациях основное внимание уделяется важности учета импеданса для обеспечения стабильных характеристик подавления побочных колебаний.

На практике не всегда удастся подобрать необходимый по всем параметрам сетевой фильтр из предлагаемых производителями, и, следовательно, появляется необходимость в разработке специального фильтра. Общие рекомендации по проектированию фильтров достаточно полно освещено во многих публикациях и трудах, например, [3]. И, тем не менее, на базе приобретенного опыта по практическому исследованию частных решений по фильтрации сети электропитания компьютера, считаем полезным привести некоторые рекомендации по созданию основного элемента фильтра – дросселя, а именно по:

- выбору типа дросселя;
- выбору магнитопровода;
- выбору направления намотки обмоток;
- выбору технологии изготовления обмоток;
- технологии изготовления дросселя;
- способу подключения обмоток дросселя.

При выполнении общих требований и расчете нагрузочных показателей дросселя необходимо с позиции предотвращения утечки информации удовлетворить условию, при котором результирующее сопротивление дросселя переменному напряжению электросети будет равно активному сопротивлению обмотки дросселя, что достигается при выполнении условия $I_{\text{пр}} = I_{\text{обр}}$ и при равенстве индуктивностей обмоток. Выравнивание индуктивностей обмоток достигается измерением их значений измерителем RLC и уменьшением витков одной из обмоток до получения значения равного меньшей индуктивности (рис.3).

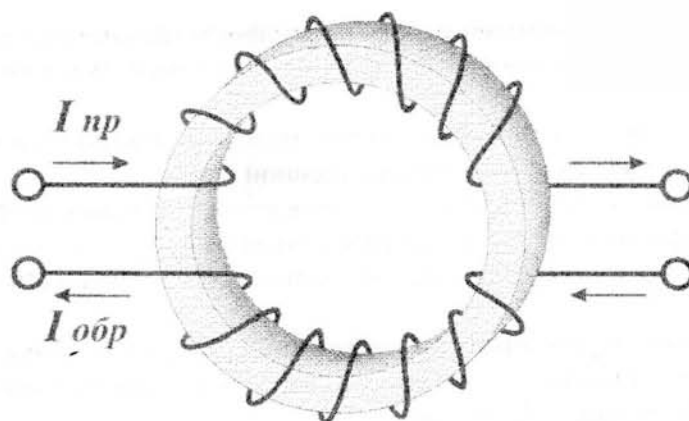


Рис.3. Основной элемент сетевого фильтра-дроссель,

Где:

- $I_{пр}$ – прямой ток электропитания.
- $I_{обр}$ – обратный ток электропитания.

Для исключения перемещения витков обмоток от внешних воздействий необходимо предусмотреть заливку дросселя, например «эпоксидным компаундом». Так обеспечивается исключение проявления микрофонного эффекта в дросселе при воздействии на него акустических полей и снижение параметрических свойств для сигналов ВЧ-навязывания. Вид промышленного образца дросселя, выполненного с учетом сделанных выше замечаний, представлен на рис. 4.

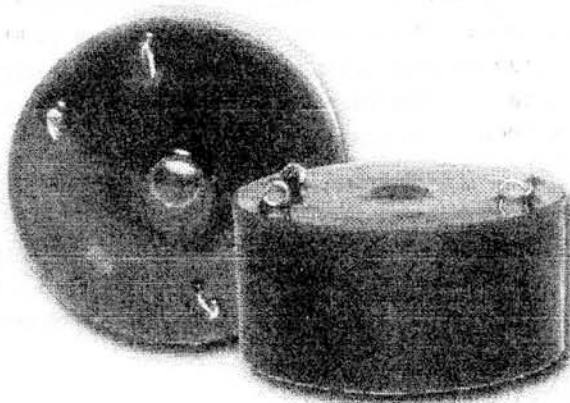


Рис.4. Внешний вид дросселя после заливки компаундом.

С целью снижения уровней электромагнитных излучений, проникающих в сеть электропитания, дроссель следует устанавливать в экранированном отсеке, а монтаж всех компонентов фильтра выполнять согласно рекомендациям[3].

Правильный выбор сетевого фильтра или изготовление фильтра собственной оригинальной конструкции не всегда дает положительные результаты при решении задач защиты информации. При прочих равных условиях на эффективность защиты оказывает большое влияние способ подсоединения сетевого фильтра к нагрузке.

Рассмотрим следующие варианты:

1. **коллективная** организация фильтрации электропитания – когда один сетевой фильтр обеспечивает несколько однородных или незначительно отличающихся разнородных потребителей.
2. **индивидуальная** фильтрация электропитания для каждого потребителя, которая может быть выполнена по схеме:

2.1. **фильтр**, размещенный в **конструктиве** нагрузки, т.е. он является узлом компьютера;

2.2. **фильтр** только для одной нагрузки, т.е., как **автономное** изделие;

2.3. **несколько фильтров**, объединенных в **одном** многосекционном экранированном конструктиве, где каждая нагрузка получает отфильтрованное электропитание от фильтра автономно экранированной секции, т.е. исключается возможность взаимного проникновения побочных колебаний и снижается уровень излучений. В этих секциях размещены и преобразователи переменного напряжения 220В 50Гц в постоянное 12В.

Коллективная организация фильтрации электропитания из-за наличия общей точки подключения разных и разнородных потребителей не всегда удовлетворяет нормативным требованиям защиты информации. Недостатки – наличие общей точки для всех паразитных контуров и изменение качества защиты информации от количества потребителей (чем меньше потребителей, тем выше качество).

Вариант 2.1. При определенных условиях может удовлетворять требованиям по реализации функции защиты информации, но не всегда его можно реализовать в корпусах покупных изделий. Наиболее он подходит для вновь разрабатываемых технических средств. Недостаток – не всегда конструктивно совместим с изделием.

Вариант 2.2. По реализации функций защиты информации удовлетворяет требованиям, но основным недостатком является количество фильтров равное количеству устройств и разветвленная кабельная система при организации электропитания даже для одного персонального компьютера.

Вариант 2.3. Свободен от вышеназванных недостатков и имеет высокие показатели по предотвращению утечки информации по техническим каналам, образуемым по сети электропитания.

Итак, защита информации в цепях электропитания устройств компьютера – это сложный многоаспектный процесс. С одной стороны необходимы средства предотвращения утечки информации по непреднамеренным каналам утечки информации, с другой – по специально организованным. К сожалению универсального решения этих задач не имеется, но есть набор способов и средств защиты информации, варьируя которыми для конкретного случая можно получить желаемую эффективность защиты информации.

Эффективным способом снижения уровней побочных излучений является экранирование цепей электропитания, узлов компьютера и периферийных устройств (как сосредоточенных и рассредоточенных источников излучения), в том числе и от радиозакладок. При этом следует учитывать, что для достижения требуемых показателей ослабления излучений необходимо нормативное решение задач по заземлению экранов, с целью исключения образования паразитных контуров и уменьшения уровней побочных излучений, возникающих при одновременно работающих устройствах (например, на комбинационных частотах).

На рис.5. представлена схема электропитания компьютера и подключенных к нему периферийных устройств, в которой учтены изложенные выше рекомендации.

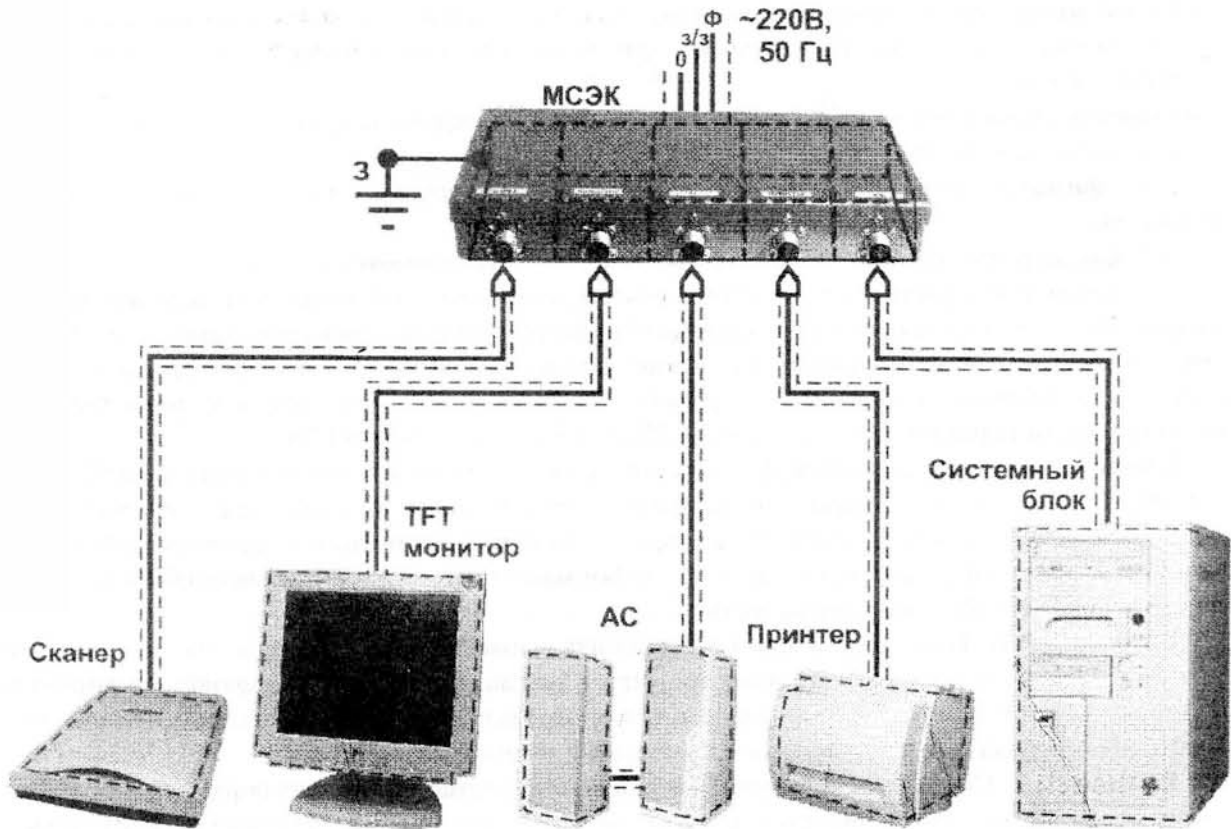


Рис.5 Вариант 2.3

Где:

- 3/3 – провод защитного заземления.
- МСЭК – многосекционный экранированный конструктив.
- $\perp$ – заземлитель.
-  – провод в экране.
- ---- условное обозначение экрана.

Рекомендации по проектированию и изготовлению заземлителя и системы заземления достаточно профессионально и полно рассмотрены в источниках [2, 3, 4]. Тем не менее, в связи с тем, что электропитание компьютера зарубежного производства требует трехпроводной системы: фаза-ноль-земля, а традиционно выполненная отечественная разводка имеет только фазу и ноль (фазный и нулевой провод), считаем уместным отметить, что запрещается использовать в качестве заземляющих устройств нулевые фазы электросетей, металлоконструкции зданий, соединенные с землей, металлические оболочки подземных кабелей, металлические трубы систем отопления, водоснабжения и т.д.

Кабели электропитания необходимо размещать в экранированных конструктивах типа металлических рукавов, коробов, плетенок и т.д., что позволит исключить или значительно уменьшить взаимные паразитные наводки от различных потребителей электроэнергии и снизить уровни излучений от рассредоточенных источников. Таким образом, будет создан общий экранированный объем для системы электропитания компьютера и всех периферийных устройств, обрабатывающих информацию с ограниченным доступом. Степень эффективности принятых мер по предотвращению утечки информации будет зависеть в основном от качества изготовления и монтажа экранирующих конструктивов, выбранных систем электропитания и заземления. Иногда это не обеспечивает требуемой эффективности и тогда приходится прибегать к некоторым частным решениям,

представляючим практичний інтерес, наприклад, просторове рознесення слабо і сильноточних кабелів друг відносно друга і шини заземлення, симетризування проводів кабеля живлення, застосування варисторів для захисту від перенапружень і супресорів для місцевої локалізації електромагнітних випромінювань і т.д.

В висновок відзначимо, що розглянуті рекомендації по запобігання витоку інформації по технічним каналам комп'ютера, є складовою частиною загальної технології захисту інформації в Концепції забезпечення безпеки інформаційних ресурсів, розробленої в нашому підприємстві.

Желающим получить дополнительную информацию по проблеме защиты информации советуем обратиться на сайт www.epos.kiev.ua

Ключевые слова: *Технический канал утечки информации, предотвращение утечки информации, помехообразующие контуры, коллективная и индивидуальная фильтрация помех.*

Список литературы:

1. Коженевский С.Р., Солдатенко Г.Т. Предотвращение утечки информации по техническим каналам персонального компьютера. *Захист інформації*, №2, 2002г. с. 32-37.
2. Хорев А.А. Способы и средства защиты информации, М., 1998г.
3. Волин М.Л. Паразитные процессы в радиоэлектронной аппаратуре, М., «Радио и связь» 1981г.
4. ОТТ Г. Методы подавления шумов и помех в электронных системах, М., «Мир», 1979г.
5. Векслер Г.С. Подавление электромагнитных помех в цепях электропитания. Киев, «Техника», 1990г.
6. Емельянов С.Л., Логиненко Н.Ф., Марков С.И., Носов В.В. Технические методы защиты каналов утечки информации по электросети, ж-л «Бизнес и безопасность» №2, 2000г., стр.8
7. Бландова Е.С. Помехоподавляющие изделия, рекомендации по выбору и применению, ж-л «Специальная техника» №1, 2001г., стр.36
8. Бландова Е.С. Выбор сетевых помехоподавляющих фильтров, ж-л «Специальная техника» №2, 2001г. стр. 45

УДК 681.3

Вертузаев М.С., Вертузаев О.М.

«ІНТЕГРОВАНІЙ НАЦІОНАЛЬНИЙ БАНК ДАНИХ ДЕРЖАВТОІНСПЕКЦІЇ МВС УКРАЇНИ» ЯК СКЛАДОВА НАЦІОНАЛЬНОГО ІНФОРМАЦІЙНОГО РЕСУРСУ УКРАЇНИ

Державна політика України в галузі формування інформаційних ресурсів і інформатизації повинна бути спрямована на створення умов щодо ефективного та якісного інформаційного забезпечення (ІЗ) рішення стратегічних і оперативних завдань соціального та економічного розвитку країни. Метою запропонованої статті є розкриття головних напрямків автоматизації ІЗ діяльності органів внутрішніх справ (ОВС) України на базі сучасних комп'ютерних технологій на прикладі інформатизації діяльності Державтоінспекції (ДАІ) МВС України

Значні темпи зростання автомобілізації в Україні призводять до помітного збільшення числа дорожньо-транспортних пригод (ДТП), навантаження на реєстраційні підрозділи ДАІ,