Значення кута $\theta_{с.з}$ напрямку на джерело завади може розраховуватись в процесорі. Перевагою пристрою є також можливість компенсації завади при зміні місцеположення її джерела.

Список літератури:

1. Ямпольский В.Г., Фролов О.П. Антенны и ЭМС. –М.: Радио и связь, 1983. -272 с.

Надійшла 12.01.2002

УДК 681.3

С.Р. Коженевский, Г.Т. Солдатенко

ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ В ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРАХ

Цель данной статьи – это попытка упорядочить понимание задачи обеспечения безопасности информации, циркулирующей в ПК, и помочь заказчику, приобретающему защищенный ПК (в специальном исполнении), более квалифицировано ориентироваться в инженерно-технических аспектах проблемы.

Проблема обеспечения информационной безопасности в Украине, как и во всех странах мира, не утрачивает своей актуальности, поскольку она непосредственно связана с национальной безопасностью страны.

В конце прошлого и начале этого столетия начала происходить существенная переоценка ценностей цивилизации. К сожалению, сфере информационных ресурсов, приобретающих первостепенное значение в научно-техническом, социально-экономическом и политическом развитии мирового сообщества уделяется на наш взгляд недостаточно внимания. Развитие рыночных отношений в нашей стране обострило проблему безопасности информации, при этом одновременно стали стремительно развиваться два процесса:

- **первый**, по защите информационных ресурсов;
- **второй**, по добыванию информации или причинения ей ущерба, вплоть до трагических ситуаций.

Информационная безопасность страны базируется на правовой и нормативной базах. В Украине это отражено в ст. 34 Конституции Украины "Про державну таємницю" и Постановлении Кабинета Министров от 13.01.95г., №24 "Про захист інформації в автоматизованих системах", а также в Указах Президента Украины от 27.09.99г., №1229/99 и №1193/2001 от 06.12.01г.

Тенденции развития современного мира характеризуются созданием единого глобального информационного пространства на планете, а, следовательно, проблема информационной безопасности становится проблемой коллективной, а не отдельно взятой страны. Изучение юридических проблем, связанных с расследованием компьютерных преступлений привело, например, к разработке « Проекта Европейской Конвенции о киберпреступности» [1], в США к пересмотру «Национальной информационной стратегии, как основе внешней и внутренней политики США в XXI веке» [2], а в России помимо Федерального закона «Об информации, информатизации и защите информации», «Об участии в международном информационном обмене» принята «Доктрина информационной безопасности РФ».

В начале 70-х годов прошлого столетия в СССР государственная задача по обеспечению безопасности информации была сформулирована в концепции

противодействия иностранным техническим разведкам. Было введено понятие – **канал утечки информации**. Основное внимание уделялось следующим каналам утечки информации:

- прямое хищение носителей информации (в том числе копирование информации, находящейся на носителях);
- несанкционированное подключение к аппаратуре и линиям передачи данных или незаконное использование зарегистрированных терминалов пользователей;
- несанкционированный доступ (НСД) к информации за счет специального приспособления математического и программного обеспечения;
- перехват электромагнитного излучения (ЭМИ) с информационными сигналами при обработке информации.

Для предотвращения утечки информации необходимы специальные мероприятия, методы и средства. С целью выявления потенциальных каналов утечки информации были созданы межотраслевые комиссии и проведено обследование категорированных объектов – от кабинетов членов правительства до выделенных помещений в организациях, предприятиях и заводах. Соответствующим Министерствам было поручено закрытие каналов утечки информации и разработка средств защиты информации в средствах вычислительной техники (ВТ), оргтехники и т.д. С этого момента началось широкомасштабное развитие методов, способов и средств защиты информации, с целью предотвращения ее утечки по каналам побочных электромагнитных излучений и наводок (ПЭМИН) и за счет НСД.

Наибольшее внимание было уделено:

- программным средствам;
- программно-аппаратным средствам;
- пассивному методу – экранированию и фильтрации;
- активному методу – зашумлению;

На достоинствах и недостатках прежней концепции противодействия иностранным техническим разведкам не стоит останавливаться, так как это достаточно освещено в различных источниках. Между прочим, следует отметить, что активный метод (зашумление) разрабатывался интенсивнее и быстрее внедрялся, так как не требовал серьёзных финансовых затрат при постановке на производство. Такое положение сохранялось до начала 90-х годов. Процесс, так называемой переходной экономики, сгенерировал создание структур негосударственной собственности, занимающихся проблемами безопасности информации, в которые пришли опытные специалисты из госпредприятий. Доступнее стали и высокие технологии, и публикации по проблеме защиты. Эти факторы простимулировали ускоренное развитие целого ряда методов, способов и средств защиты информации, так как негосударственные структуры более мобильны в достижении цели.

В общем случае **под защитой информации** понимают совокупность технических средств, организационных мероприятий и правовых норм для предупреждения причинения ущерба интересам собственника информации. При этом средства защиты информации направлены на осуществление следующих целей:

- предупреждение уничтожения или искажения информации;
- исключение несанкционированного доступа к информации;
- предупреждение несанкционированной модификации информации;
- снижение уровней ЭМИ и т. д.

Перечень сведений, разглашение которых может причинить вред интересам собственника информационных ресурсов, это:

1. В сфере основной деятельности:

- сведения о научно-производственных возможностях;
- сведения о планах развития предприятия и методах управления;
- объемы закупок и продаж;

2. В сфере финансов:

- банковские счета и операции;
- международные расчеты с инофирмами;
- источники и размеры кредитов.

3. В сфере партнерских отношений:

- списки контрагентов и сведения об их финансовом состоянии;
- сведения о подготовке переговоров, включая тактику их ведения.

Перечисленные объемы информации хранятся, обрабатываются в средствах ВТ и передаются по линиям связи абонентов. Поэтому, если не приняты необходимые и достаточные меры по предотвращению утечки информации по каналам, образованным средствами ВТ, то ни о какой защите информации не может идти речи – т.е. несанкционированный доступ к информационным потокам предприятия имеет место быть.

В настоящее время в концепции технической защиты информации появились дополнительные требования по:

- аутенфикации, достоверности и целостности информации;
- биологической защите оператора;
- противодействию электромагнитному терроризму и т. д.

Расширение спектра требований, которые необходимо учитывать при изготовлении ПК в специсполнении, вызвало изменения в концепции защиты информации. Например, при применении активного метода защиты необходимо понимать суть его негативного воздействия для решения задачи обеспечения биологической защиты оператора.

Электромагнитное излучение (ЭМИ) имеет следующие факторы воздействия на организм человека:

- биологический;
- специфический (биохимическое изменение);
- тепловой (локальный нагрев тканей).

Такие воздействия приводят к профзаболеваниям, по статистике [3] наиболее компьютеризованной страны – США – темпы роста компьютеризации населения соответствуют темпам роста профзаболеваний. В настоящее время ряд Европейских стран, Россия и 25 штатов США разработали документы, регламентирующие правила пользования ПК. Наиболее известны Шведские стандарты MPRII и TCO, а также Российские СанПиН 2.2.2.542-96 и ГОСТ 50948-96. В этих документах содержатся рекомендации по защите от вредных факторов: это применение различных классов фильтров, например «полная защита» или «максимальная защита». Эти фильтры изготовлены из стекла [4] сильно легированного атомами тяжелых металлов. На стороне, обращенной к пользователю, нанесено полиэфирное и 5-слойное диэлектрическое покрытие, а на противоположной стороне вакуумным напылением нанесен слой металлического серебра.

При этом достигается ослабление:

- магнитной и электрической составляющих поля на 40 дБ;
- электростатического поля на 40 дБ;
- ультрафиолетовое излучение – полностью;
- рентгеновское излучение в 250 раз;
- блики отсутствуют полностью, контрастность повышается в 10 раз.

При выборе метода, обеспечивающего комплексное предотвращение утечки информации, необходимо учитывать следующие требования:

- гарантированное обеспечение степени защиты информации;
- биологическую защиту оператора;
- защиту от электромагнитного терроризма;
- технологическую пригодность к серийному производству;

- приемлемые экономические показатели;
- сохранение дизайна устройств ПК.

В наибольшей степени удовлетворяет этим требованиям только **пассивный метод защиты** информации. В общем плане – это локализация источников побочных ЭМИ, т. е. экранирование и фильтрация токонесущих цепей.

Следует отметить, что в последние 1,5 – 2 года заметно оживление на рынке ПК с защитой информации. Но все многообразие производителей независимо от формы собственности действует по одной технологии, которая была отработана в 70-80 годах прошлого столетия на промпредприятиях СССР. Эта технология обеспечивала хорошие результаты, поскольку базировалась на ПК отечественного производства. Полное и безвозвратное исчезновение отечественного производителя ПК и ориентация на поставку ПК зарубежных производителей потребовала новых подходов в решении задач проблемы защиты информации.

Комплектующие для сборки ПК на Украине поставляются из-за рубежа. С периодичностью 3-6 месяцев, происходит изменение их конструкторских решений, технических характеристик, форм, габаритов и конфигураций. Следовательно, технология, ориентированная на защиту каждой новой модели ПК, требует высочайшей маневренности производства. При этом возможен **вариант** изготовления из металла набора универсальных корпусных изделий и размещения в них комплектующих ПК, а также периферийных устройств зарубежного производства. Недостатком этого подхода является то, что он приемлем только для полигонного или катастрофоустойчивого исполнения. **Другой вариант** – это выбор комплектующих для ПК из большого количества однотипных изделий по признаку минимальной излучательной способности. Этот вариант необходимо рассматривать как непрофессиональный подход к проблеме, так как он противоречит нормативной документации. **Вариант** защиты информации методом зашумления, т.е. радиомаскировки, имеет недостатков на много больше, чем достоинств. Например, является демаскирующим признаком категорированного объекта, ухудшает экологию на рабочем месте и, главное то, что при определенных условиях, не обеспечивает гарантированную защиту информации.

Таким образом, появилась необходимость в разработке нового подхода, который обеспечивал бы функции защищенности информации, обрабатываемой на ПК, любого состава, структуры построения, назначения, геометрических форм и размеров, при сохранении всех эксплуатационных характеристик, дизайна и был бы свободен от вышеуказанных недостатков.

Новый подход к решению задач защиты информации базируется на **пассивном методе** (экранирование и фильтрация), но в отличии от прежних универсальных вариантов его применения, мы предлагаем индивидуальный подход к закрытию каналов утечки информации. В основу индивидуального подхода положен анализ устройств и комплектующих ПК с целью определения общих конструкторских и схемо-технических решений исполнения, определения параметров побочных излучений и на основании анализа этих данных осуществляются мероприятия по защите.

В общем случае ПК состоит из:

- системного блока;
- монитора;
- клавиатуры;
- манипулятора (мышь);
- принтера;
- акустической системы.

Анализ конструктивного исполнения устройств ПК позволил определить у них обобщенные признаки подобия (ОПП) и различия в зависимости от функционального назначения.

1. **Системный блок.** Большое многообразие корпусов вертикального и горизонтального исполнения.

ОПП: каркас, кожух, передняя панель, органы управления и индикации, блок питания и ввод-вывод коммуникаций.

2. **Монитор.** Различные геометрические формы корпусов из пластмассы, три типа экранов (ЭЛТ): плоский, цилиндрический и с двумя радиусами кривизны в различных плоскостях.

ОПП: пластмассовые корпусные детали, ввод коммуникаций, органы управления и сигнализации.

3. **Клавиатура.** Незначительные различия в геометрии корпусов из пластмассы (у некоторых типов поддон из метала).

ОПП: пластмассовые корпусные детали, ввод коммуникаций и органы сигнализации.

4. **Манипулятор (мышь).** Незначительные различия в геометрии корпусных деталей из пластмассы.

ОПП: пластмассовые корпусные детали, ввод коммуникаций.

5. **Принтер (лазерный, струйный).** Корпуса различной геометрии из пластмассы, органы управления и различные разъёмные соединения.

ОПП: пластмассовые корпусные детали, ввод коммуникаций, органы управления и сигнализации.

6. **Акустические системы.** Большое многообразие геометрических форм корпусов из пластмассы и дерева;

ОПП: ввод-вывод коммуникаций, органы управления и сигнализации, а для отдельных групп – пластмассовые корпусные детали.

Таким образом, обобщенные признаки подобия образуют **три основные группы** присущие базовому составу ПК, с которым приходится работать при решении задач защиты информации, такие как:

- **корпусные детали из пластмассы;**
- **ввод-вывод коммуникаций;**
- **органы управления и сигнализации,**

При этом учитываются и **общесистемные проблемные вопросы**, как – то:

- **разводка и организация электропитания и шин заземления;**
- **согласование сопротивлений источников и нагрузок;**
- **блокирование взаимного ЭМИ устройств ПК;**
- **исключение влияния электростатического поля;**
- **эргономика рабочего места и т.д.**

Следующий этап – это разработка типовых конструкторско-технологических решений, реализация которых направлена на предотвращение утечки информации за счет расширения функций конструктивов устройств ПК. Набор типовых конструкторско-технологических решений варьируется в зависимости от состава устройств ПК, но для базовой модели ПК с учетом обобщенных признаков подобия он содержит решения по:

- металлизации внутренних поверхностей деталей из пластмассы;
- экранированию проводных коммуникаций;
- согласованию сопротивлений источников и нагрузок;
- экранированию стекол для монитора и изготовлению заготовок различных форм из стекла;
- фильтрации сетевого электропитания и его защите от перенапряжений;
- нейтрализации влияния электростатического поля;
- расположению общесистемных проводных связей;
- точечной локализации ЭМИ;
- исключению ЭМИ органами управления и сигнализации;

- радиогерметизирующим уплотнителям из различных материалов;
- исключению взаимного влияния ЭМИ устройств ПК.

На основании вышеизложенного разрабатываются технические требования по защите информации в конкретном составе ПК. Практика выполненных опытно-конструкторских работ показала, что реализация таких конструкторско-технологических решений удовлетворяет техническим требованиям и нормативной документации по предотвращению утечки информации.

В рамках настоящей статьи не представляется возможным представить в полном объёме работы, выполняемые ООО «ЕПОС» по обеспечению безопасности информации. Приведём только направления, по которым проводятся научно-исследовательские и опытно-конструкторские работы (НИОКР):

- предотвращение утечки информации в цепях электропитания и заземления;
- защита от НСД к ПК;
- защита от НСД к информационным ресурсам ПК;
- восстановление и стирание информации на НЖМД;
- обеспечение безопасности информации в сетях.

В заключение необходимо отметить, что желание обеспечить высокоэффективную систему безопасности информации вполне оправдано, но это требует значительных финансовых затрат. Вместе с тем чрезмерные затраты на защиту не всегда адекватны гарантированной степени надежности защиты. Чтобы избежать «саморазорения» от чрезмерных затрат на обеспечение безопасности информации следует придерживаться принципа необходимой достаточности, т.е. стоимость защиты не должна превышать риска ущерба от негативного воздействия на информационные ресурсы.

Список литературы:

1. Волеводз А.Г. Проект Европейской Конвенции о киберпреступности, «Конфидент» №5, №6, 2001г.
2. Гриняев С.Н. Национальная информационная стратегия как основа внешней и внутренней политики США в XXI веке, «Конфидент» №5, №6, 2001г.
3. www.pole.ru/spk.htm
4. Бурлаков Г.Н. «Безопасность работы на компьютере» М.: «Финансы и стастика» 1998г.

Ключевые слова:
Информационная безопасность, каналы утечки информации, методы предотвращения утечки информации, типовые конструкторско-технологические решения.

Поступила 10.01.2002

УДК 621.391.7

Яремчук Ю.Є.

ВИКОРИСТАННЯ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ В ЗАДАЧАХ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Вступ

Існує багато методів та засобів забезпечення безпеки інформації. Криптографічні методи [1] застосовуються для вирішення проблем захисту інформації в комп'ютерних системах. Історично криптографія виникла як наука про шифрування інформації [2],