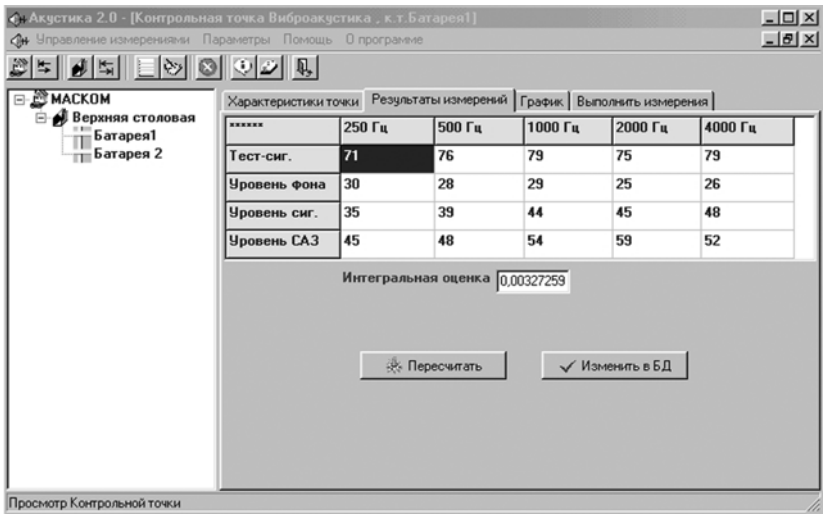

Рисунок 4 – Рабочее окно программы комплекса «ШЕПОТ»

Управляющий компьютер подключается к измерительному комплексу через стандартные COM (RS 232) и LPT порты. Все необходимые измерения производятся комплексом в автоматическом режиме, включая управление акустическим тест-сигналом и переключение датчиков. Задачей оператора является только правильное размещение датчиков комплекса (микрофонов, акселерометра и акустического излучателя) и ручное включение (при необходимости) системы акустического или виброакустического зашумления по команде комплекса. Расчёт значений защищённости помещения по окончании цикла измерений выполняется также автоматически. Программный модуль расчёта результатов позволяет ручное занесение данных оператором и перерасчёт значений после их занесения или коррекции. Наличие у всех составляющих комплекса автономного электропитания увеличивает его мобильность и расширяет сферу применения. Построение программного обеспечения позволяет с минимальными доработками адаптировать его к другой модели шумомера, имеющего управление по стыку RS232. ПО комплекса может использоваться самостоятельно для выполнения расчетов и хранения результатов, полученных при измерениях акустическими приборами с ручным управлением.

IV Заключение

Представленные комплексы резко снижают время и трудоемкость проведения специальных исследований технических средств и систем, а также защищаемых помещений и являются мощным инструментарием для работы испытательных лабораторий и служб технической защиты информации.

УДК 621.391.883

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ СРЕДСТВ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ЗА СЧЕТ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ И НАВОДОК

Владимир Луценко, Александр Архипов, Валерий Худяков*
НТУУ КПИ, Физико-технический институт
**НИИ Электромеханических приборов, Киев*

Аннотация: **Рассматриваются вопросы технической защиты национальных информационных ресурсов в средствах вычислительной техники, автоматизированных компьютерных системах и сетях ЭВМ. Сформулированы направления, в которых необходимо развивать работы для защиты информации от утечки за счет побочных электромагнитных излучений и наводок, проводится анализ имеющихся и реально создаваемых сейчас средств и методов защиты. Определен круг наиболее дефицитных технических средств, систем, методик и норм в области ТЗИ, и возможные пути их создания в ближайшее время.**
The summary: **The problems of technical protection of national information resources in means of computer facilities automated computer systems and computer networks are esteemed. The directions are**

formulated, in which one it is necessary to develop activities for protection of the information against outflow at the expense of spurious electromagnetic radiation and aiming, the analysis of available and substantially created now means and methods of protection is carried out. The circle of the most deficient means, systems, techniques and standards in area of technical information protection, and possible paths of their creation as soon as possible is determined.
Ключевые слова: **Защита информационных ресурсов, компьютерная безопасность, методики и нормы в ТЗИ, активные и пассивные методы защиты.**

I Введение

Со времен Обнинской конференции по "Безопасности информации, обрабатываемой в АСУ, СВТ и ТСПИ", проходившей в декабре 1990 года, вопросы технической защиты национальных информационных ресурсов в средствах вычислительной техники (СВТ), автоматизированных компьютерных системах и сетях ЭВМ непрерывно обсуждаются авторами с разных позиций. Тот факт, что эти вопросы ставились на конференциях и в Белогорске, и в Гурзуфе, и в Ялте, и в Киеве еще раз подтверждает актуальность данного вопроса. Мало того, важность вопроса не уменьшается по причине возрастания объемов оснащения различных структур импортной техникой, не имеющей сертификации по технической защите информации (ТЗИ). И если оснащение Государственных структур в какой-то мере поставлено под контроль Департамента специальных телекоммуникационных систем и защиты информации СБ Украины, то в остальных случаях этот процесс практически бесконтролен. Одной из причин такого положения дел является отсутствие целостной программы создания системы компьютерной безопасности в рамках национальной системы ТЗИ. Кроме того, актуальность вопроса возрастает в связи с интенсивной информатизацией страны на фоне мировых информационных процессов, характеризующихся повышенным вниманием к уязвимости информационных ресурсов коммерческих и государственных структур и стран в целом. Уязвимость приводит к заметному ущербу для владельцев информационных ресурсов в результате увеличения вероятности утечки конфиденциальной информации.

II Постановка задачи

Ключевым условием быстрейшего создания комплекса технических средств (ТС) для его реализации в целях защиты национальных информационных ресурсов Украины в СВТ и сетях ЭВМ, а также в средствах связи, является формирование направлений, в которых необходимо развивать работы для защиты информации от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН), анализ имеющихся и реально создаваемых сейчас средств и методов защиты и на этой основе определение круга наиболее дефицитных ТС, систем, методик и норм в области ТЗИ, а также определение возможных путей их создания и реализации в ближайшее время.

III К вопросу защиты информации от утечки за счет ПЭМИН

По нашему мнению первый пункт постановки задачи, изложенной выше, достаточно глубоко проработан и изложен в [1]. Задачи ТЗИ в интересующей нас области формулируются по четырем направлениям, а именно: 1) исследование и разработка методов, устройств и алгоритмов анализа пространственных, временных и частотных характеристик сигналов, излучаемых средствами ВТ; 2) создание автоматизированного радиоизмерительного комплекса для специальных исследований излучений СВТ при их разработке, испытаниях и сертификации; 3) разработка методов и устройств активной защиты СВТ путем формирования шумоподобных или структурноподобных помех; 4) разработка методов и устройств пассивной защиты СВТ и связи, обеспечивающих снижение уровней побочных излучений и наводок в СВТ.

Рассмотрим каждый из этих четырех пунктов в отдельности.

Создание методов, алгоритмов и на их основе устройств анализа характеристик сигналов требует, как минимум, создания математического обеспечения для идентификации и восстановления информационных сигналов в шумах, в том числе при проведении работ по обследованию в каналах ПЭМИН аппаратуры, осуществляющей криптографическую защиту информации с ограниченным доступом (ИсОД). Требуется идентификация тест-сигналов в шумах, в том числе в собственных шумах (которыми могут быть и служебные сигналы) самой ТСПИ. Для этого, несомненно, потребуется привлечение методов корреляционного анализа. Для специального исследования СВТ и ТСПИ с уровнем сложности выше бытового телефона немедленно возникает проблема разработки тест-ключей (тестовых чип-карт) и т. п. [2-4].

С точки зрения создания ТС с малыми уровнями ПЭМИН видимо назрела необходимость рассмотреть возможность разработки и идеологии, и технологии создания электронных средств с прогнозируемыми характеристиками ПЭМИН, начиная от электронных компонентов в корпусном и бескорпусном исполнении, активных (с нелинейными вольт-амперными характеристиками p-n переходов, МОП, МДП и др. структур) и

пассивных, микросхем с малой и высокой интеграцией, печатных плат (с учетом возможности внедрения экранирующих или поглощающих слоев, а также встроенных фильтров), приборов и устройств в целом (с учетом особенностей конструктивов, межблочных соединений, экранов блоков и экранов, нанесенных на диэлектрические элементы и узлы конструкций), вплоть до защищенных помещений и объектов информационной деятельности в комплексе. Иными словами, необходима Украинская программа наподобие программы TEMPEST. Надо отметить, что опыт в разработке таких технологий в мире имеется. Например, продукция фирм Siemens Nixdorf (Германия) (компьютеры семейства PC SCENIC типа 01 SCENIC66/97) или мюнхенской фирмы ROHDE & SCHWARZ (на примере монитора "Industrial Monitor PMC4"), а также фирмы Siemens (Egro-Scan 15C-V (фирмы Siemens), который сами разработчики окрестили "Tempest by Siemens"). Эта продукция была представлена на Украинском рынке еще 5 лет назад, а фирма SAGEM (Франция) ведет сейчас разработку защищенных компьютеров на основе технологий по TEMPEST. Необходимо отдавать себе отчет в том, что результат такой работы в полной мере зависит от квалифицированной постановки задачи на ее проведение, что уже само по себе весьма сложно. Такая работа должна учитывать уже имеющиеся наработки и ряд ограничений, связанных, прежде всего, с существующей нормативной базой [5]. Для абонентских пунктов электронной почты специального назначения с использованием криптосистем, сетей правительственной и засекреченной связи уровень защиты информации в ЭВМ по ПЭМИН должен отвечать требованиям защищенности информации на объектах первой категории, поскольку размеры зоны 2, определенные по действующим нормам защиты информации для объектов второй категории (или третьей) по мнению авторов работы [6] (и мы с этим полностью согласны), может находиться в зоне уверенного перехвата при обеспечении "особых условий размещения", которые при наличии современной портативной аппаратуры можно оперативно создать практически для любого объекта. Такая предпосылка автоматически накладывает жесткие требования к условиям размещения ТСПИ, их активной и пассивной защите. Это может быть связано как с электромагнитным экранированием выделенных помещений объекта эксплуатации, так и с защитой коммуникаций при наличии незащищенных линий связи. В ответственных случаях применение ПЭВМ, выполненных в защищенном исполнении, требует проведения предэксплуатационных дополнительных исследований на конкретных объектах с учетом возможных вариантов условий эксплуатации. Для проведения таких работ лицензиаты не имеют и не могут иметь достаточно ресурсов. Поэтому необходима программа создания единого полигона испытаний объектов ТЗИ, возможности и состав которого направлены на имитацию реальных условий, фактически существующих на реальных объектах различного характера. В этом случае любой лицензиат сможет воспользоваться возможностями такого полигона, качественно и значительно более объективно, чем в настоящее время подготовить технику и рекомендации к конкретному объекту для введения его в эксплуатацию. Автомобилист может воспользоваться услугами СТО с целью проведения техосмотра, пользователь измерительного прибора общего назначения может воспользоваться услугами метрологической лаборатории с целью аттестации и калибровки своего прибора, лицензиат должен иметь возможность воспользоваться услугами полигона имитации свойств реальных объектов.

Обобщая вышеизложенное, можно сформулировать требования к методам, устройствам и алгоритмам анализа характеристик сигналов:

- методы и алгоритмы должны использовать качественно новые, более сложные модели и методы обработки информации с развитым математическим аппаратом;
- методы должны полнее учитывать наработанную на сегодня нормативную базу, которая бурно разрастается, и иметь возможность гибко реагировать на ее стремительное развитие;
- сложность требуемых алгоритмов настолько высока, что настоятельно требует применения компьютерных возможностей обработки данных, а значит, требуется создание специальных пакетов программ, направленных на решение задач в данной области;
- проблема создания тест-ключей должна неразрывно увязываться и с методикой, и с алгоритмами обработки результатов специальных исследований;
- устройства анализа должны быть сориентированы на более высокий качественный и функционально наполненный уровень, что само по себе накладывает отпечаток на следующий, второй пункт постановки задачи – создание автоматизированного измерительного комплекса для проведения специальных исследований.

Наиболее известными на сегодня украинскими комплексами специальных измерений являются комплексы "Астра-В" и "АКОР-1ПК".

Комплекс специальных измерений "Астра-В" [7] (ЧПФ "Бумекс" г. Киев) является автоматизированным программно-аппаратным комплексом для обнаружения радиосигналов, анализа характеристик электромагнитного поля, проведения специальных исследований на ПЭМИН, регистрации, хранения, обработки и документирования результатов. Отличительные особенности комплекса - это удобный

интерфейс, гибкий пакет программ, возможность развития и модернизации ПО, соответствие определенным методикам, действующим в Украине.

Комплекс “Акор-1ПК” является измерителем ПЭМИ и, по сути, представляет собой анализатор спектра и высокочувствительный селективный измерительный приемник с развитым набором режимов измерений. Не вдаваясь в подробности и нисколько не уменьшая несомненные достоинства комплексов, отметим три важных момента. Во-первых, данные комплексы не адаптированы к методикам проведения специальных исследований ТСПИ телевизионной информации и ТСПИ, осуществляющих криптографическую защиту информации. Во-вторых, верхняя граница частотного диапазона измеряемых комплексами сигналов не ограничена частотой 1 ГГц, однако в соответствии с существующими “Нормами…” и “Методиками…” обработка сигналов и расчет величин, характеризующих параметры защищенности ТСПИ, могут быть проведены только до 1 ГГц. В то же время компьютеры с тактовой частотой ниже 433 МГц сегодня уже считаются устаревшими, а информационные сигналы на частотах поднесущих второй, третьей и других кратных гармоник основной частоты явно выше 1 ГГц. В-третьих, аппаратура специсследований и мониторинга ПЭМИН уже требует иметь в своем составе устройства памяти, способные хранить электрический образ сигналов, записанных в течение длительного времени. Это позволит использовать корреляционные алгоритмы за счет большой статистики измеряемых сигналов. Требуется, также, наличие средства обработки (компьютера), адаптированного к приемнику-измерителю сигналов, что позволит в режиме реального времени реализовывать автоматический подбор (поиск) алгоритмов обработки текущих измеряемых сигналов непосредственно во время сеанса измерения. Это особенно важно при анализе ПЭМИН от устройств с динамическим режимом работы или динамическим шифрованием данных методами криптозащиты.

С другой стороны, если рассмотреть вариант технического задания на разработку аппаратуры с учетом приведенных выше замечаний, выясняется, что проблема возникает уже на этапе постановки задачи на разработку аппаратуры и математического обеспечения, поскольку, как указывалось выше, на частоты свыше 1 ГГц нет “Норм…” и “Методик…” проведения специальных исследований ПЭВМ, нет достаточно глубокого научного материала по вопросам экспериментальных исследований информативных излучений ТС в диапазоне частот свыше 1 ГГц. Поэтому наиболее реален, видимо, качественно новый подход к разработке методологии работы аппаратуры специсследований. Он заключается в том, что новые измерительные и поисковые комплексы, а также система обработки полученных от этих комплексов данных, должны ориентироваться на методы и модели математического прогнозирования, моделирования возможных ситуаций при определении стратегии поиска информативных характеристик сигналов на фоне шумов, в том числе при отношении сигнал/шум меньше единицы для ТСПИ цифровой информации. При этом появляется возможность применять вероятностный подход к анализу и расчету возможностей образования каналов утечки информации.

Рассмотрим третий пункт постановки задачи, относящийся к разработке методов и устройств активной защиты СВТ путем формирования шумоподобных или структурноподобных сигналов. Заметим, что возможность применения структурноподобных постановщиков шумов вероятными информационными противниками сама по себе оправдывает необходимость создания измерительно-обрабатывающих поисковых комплексов с характеристиками, обозначенными в предыдущем абзаце. Средства пространственного зашумления типа “Шатер”, “Волна”, “Смог”, “Базальт” и др., в частности за счет применения принципа стохастизации колебаний, обеспечивают перекрытие информативного излучения ПЭВМ в полосе частот от нескольких сотен килогерц до 1,5 ГГц. А этого опять же недостаточно для зашумления излучений на гармониках тактовых частот современных компьютеров, тем более, что и здесь отсутствие “Норм…” и “Методик…” проведения исследований ПЭВМ не позволяет определять эффективность мер защиты в каналах ПЭМИН. Кроме того, отсутствуют данные о специальной надежности работы генераторов с заданной величиной неравномерности спектра шума и спектральным значением коэффициента качества шума, например, на уровне не менее 0,8. Встроенная система автоконтроля не позволяет с заданной степенью достоверности контролировать указанные параметры. Это привело к тому, что появились такие понятия, как “хорошая” или “плохая” система “Волна-4” и др. Зависимость уровня шумового сигнала от условий размещения излучающих петель позволяет применить против них метод пространственной селекции и тем самым ликвидировать или уменьшить маскирующее действие генераторов шума (ГШ). И, наконец, самое опасное – это то, что возможность срыва стохастизации приводит к мгновенному превращению ГШ из средства защиты в дополнительный канал утечки информации за счет модуляции информативными сигналами (в т. ч. акустическими) множества несущих, вырабатываемых устройством.

Такие ГШ, как “Волна” и “Базальт” имеют ТУ и разрешены к применению, но не сертифицированы. Возникает вопрос – при всех достоинствах стохастизации колебаний адаптирована ли структура шумов этих

генераторов под типичные сигналы от средств компьютерной техники? Ответ на него может дать только дополнительная программа исследований характеристик, идентифицированных как типичные, сигналов от СВТ и ПЭВМ.

С другой стороны, со времен создания ЭВМ типа ЕС-1840, 1845 и ПЭВМ серии "Багет" (Россия) вопросом разработки адаптированных к СВТ встроенных ГШ занимаются у нас крайне мало. На Западе и в России продолжаются разработки, касающиеся методов и аппаратуры для спектрального распределения излучаемой энергии от цифровых систем. При этом используются разные подходы к минимизации электромагнитных радиочастотных помех [8]. Сама по себе такая минимизация может составить альтернативу разработке ГШ или явится удачным дополнением к имеющимся ГШ, которое обеспечит более полное закрытие каналов ПЭМИН. Таким образом, четвертый пункт постановки задачи о разработке методов и устройств пассивной защиты СВТ и связи тесно переплелся с третьим пунктом, касающимся методов и устройств активной защиты, и методологически создание этих средств и методов является единой задачей. Все это позволяет сделать вывод о том, что при внедрении мер активной защиты для создания электромагнитного маскирующего поля в диапазоне частот 0,01-1000 МГц могут применяться малогабаритные ГШ типа "Шатер", основанные на принципе стохастизации колебаний двух связанных генераторов, но их применению должна предшествовать работа по анализу соответствия специальных параметров выбранных генераторов специальным требованиям, предъявляемым к конкретному ТСПИ, с последующим проведением специальных исследований и инженерного анализа свойств аппаратуры.

IV Выводы

Обобщая изложенное выше с целью оценки ситуации и тенденций развития технических средств защиты информации можно сформулировать следующие положения:

- для проведения разработок по созданию методов, устройств и алгоритмов анализа характеристик опасных сигналов и, соответственно, разработок и создания средств и систем ТЗИ необходимо преодолеть главную проблему, корректно поставить задачу на такую разработку, основывая ее на понимании слабого развития собственных достижений в этой области, используя опыт достижений более развитых возможных информационных противников с настоятельной необходимостью перехода на качественно новый уровень аппаратуры (ее функциональных возможностей и принципов функционирования);
- все исследовательские работы по четырем означенным направлениям необходимо вести в едином комплексе, а значит и задачу на разработки формировать единую, комплексную;
- учитывая тот факт, что создание защищенной техники основано на применении комплектующих иностранного производства, узлов и устройств в целом, сложность которых не дает гарантии защиты от скрытых по воле изготовителей дополнительных функций, необходимо реанимировать разработку идеологии и технологий средств электронной техники на принципах программы типа TEMPEST;
- необходимо параллельно решать "проблему ключа" (тест-ключей) с привлечением разработок математиков в области криптозащиты и программистов, способных создавать программное обеспечение, при функционировании которого процессоры и устройства на их основе имеют низкий уровень ПЭМИН.

Литература: 1. Трутнев Н. В. "Приоритетные направления развития системы компьютерной безопасности", "Безопасность информации" № 1, 1995 г., с 10–13. 2. Левченко Г. Т. и др. "Проблемы создания абонентского пункта электронной почты с криптозащитой", "Бизнес и безопасность" № 6, 2001 г., Киев. 3. Зуев О. В. и др. "Критерий оценки качества функционирования средств защиты информации", "Захист інформації", № 1(6), 2001 г., Киев. 4. Жаринов В. Ф. и др. "Тестовые режимы", "Конфидент", № 2, 1996, с. 49–53. 5. "Нормы эффективности защиты технических средств передачи речевой информации от утечки за счет побочных излучений и наводок", "Нормы эффективности защиты технических средств передачи телеграфной и телекодовой информации от утечки за счет побочных излучений и наводок". 6. Левченко Г. Т., Ильченко М. Ю., Мачуський Є. А. та ін. "Технічна суть та нормативна база технічного захисту інформації від витоку за рахунок ПЕМВ". "Бизнес и безопасность", Киев, 2001, № 5, с. 37-39. 7. Комплекс специальных измерений "Астра-В". "Бизнес и безопасность", № 4, 2001 г. 8. Европейский патент № 85106969. Дата 30. 05. 85. Класс: H03L7118, H04B15/02. Crall, Richard F. "Метод и аппаратура для спектрального распределения излучаемой энергии от цифровых систем".