значений и хотя бы на двух соседних наборах ее значения совпадают (в этом случае M=2), то ее относительная автокорректирующая способность не ниже $\frac{2}{k^n 2n} = \frac{1}{k^n n}$. При k=2, $n \geq 2$ и минимальном, но не равном нулю количестве соседних наборов с одинаковыми значениями функции, абсолютная автокорректирующая способность равна $2n$ и поэтому для этого случая $L = \frac{2n}{2^n n} = 2^{-n+1}$.

Таким образом, предложенные выше характеристики абсолютной и относительной автокорректирующей способности переключательных функций и методика их получения позволяют оценивать и проводить сравнение степени развития автокорректирующих свойств переключательных функций.

Литература: 1. Збитнев С., Коновалов И., Меалковский Д., Поляков А. Контроль и восстановление целостности информации в автоматизированных системах / К.: Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 2002, № 4. – с. 119–128. 2. Самофалов К. Г., Корнейчук В. И., Тарасенко В. П. Цифровые ЭВМ. Теория и проектирование. – К.: Вища школа, 1989. – 424 с. 3. Тарасенко В., Коваль С. Імітаційне моделювання функціонування на канальному рівні відкритих мереж передачі даних в умовах загроз / К.: Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 2001, № 3. – с. 219–221. 4. Тарасенко В. П., Тарасенко-Клятченко О. В. Автокоригуючі властивості логічних операцій / Хмельницький, Вимірювальна та обчислювальна техніка в технологіних процесах, 2001, № 8. – с. 334–337. 5. Самофалов К. Г., Корнейчук В. И., Романкевич А. М., Тарасенко В. П. Цифровые многозначные элементы и структуры. – К., "Вища школа", 1974, 168 с. 6. Tarasenko V. P. Logical Models of Elementary Automats in k-valued Alphabet. Engineering Simulation, Amsterdam, 1997, Vol. 14, p. p. 747–752.

УДК 621.96

ВОПРОСЫ ПОСТРОЕНИЯ КОМПЬЮТЕРОВ, ЗАЩИЩЕННЫХ ОТ УТЕЧКИ ИНФОРМАЦИИ ПО КАНАЛАМ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ

Сергей Чеховский
ООО «ЭПОС»

Аннотация: **Приведены основные положения построения защищенных компьютеров для работы как в автономном режиме, так и в составе локальной сети. Рассмотрены особенности мер технической защиты для различных применений.**
Summary: **In this paper are considered the basic principles of concept of building of TEMPEST computers intended for operation in autonomous mode as well as in local area networks. The measures on technical protection of information for different applications are considered.**
Ключевые слова: **Информация, информационная безопасность, техническая защита информации.**

Проблема защиты компьютеров от утечки информации по каналам побочных излучений известна уже давно. На западе широко применяется известная аббревиатура TEMPEST (Telecommunications Electronics Material Protected from Emanating Spurious Transmissions).

История возникновения TEMPEST уходит своими корнями в далекий 1918 год, когда Herbert Yardley со своей командой был привлечен Вооруженными Силами США для исследования методов обнаружения, перехвата и анализа сигналов военных телефонов и радиостанций. Исследования показали, что оборудование имеет различные демаскирующие излучения, которые могут быть использованы для перехвата секретной информации, что серьезно обеспокоило Правительство США.

Однако, сама аббревиатура TEMPEST появилась только в конце 60-х начале 70-х годов, как секретная программа Министерства Обороны США по разработке методов предотвращения утечки информации через различного рода демаскирующие и побочные излучения электронного оборудования.

Долгое время все, связанное с понятием TEMPEST, было окутано завесой секретности. Первое сообщение, появившееся в открытой печати, принадлежит голландскому инженеру Wim van Eck, опубликовавшему в 1985 году статью "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?". Статья посвящена потенциальным методам перехвата сигнала видеомониторов. В марте 1985 года на

выставке Securecom-85 в Каннах Van Eck продемонстрировал оборудование для перехвата излучений монитора. Завеса тайны была прорвана.

Показательными были откровения Peter Wright (бывшего сотрудника английской разведки МИ-5), опубликованные в его книге воспоминаний в 1986 году. В конце 60-х Англия вела переговоры о вступлении в ЕЭС и английскому правительству очень важна была информация о позиции Франции в этом вопросе. Сотрудники МИ-5 вели постоянный перехват зашифрованных сообщений французской дипломатии, но все их усилия по вскрытию шифра не увенчались успехом. Тем не менее, Peter Wright при анализе излучений заметил, что наряду с основным сигналом присутствует и другой, очень слабый сигнал. Инженерам удалось настроить приемную аппаратуру на этот сигнал и демодулировать его. К их удивлению, это было открытое незашифрованное сообщение. Оказалось, что шифровальная машина французов имела побочное электромагнитное излучение, которое модулировалось информационным сигналом еще до момента его кодирования. Таким образом, путем перехвата и анализа побочных излучений французской шифровальной машины английское правительство, даже не имея ключа для расшифровки кодированных сообщений, получало всю необходимую информацию. Задача, стоящая перед МИ-5, была решена.

В настоящее время понятие TEMPEST означает технологию, предотвращающую утечку секретной информации (или минимизирующую риск ее утечки) при перехвате и анализе различными техническими средствами побочных электромагнитных излучений. В понятие TEMPEST входят стандарты на оборудование, средства измерения и контроля. Расширение понятия TEMPEST увеличило и количество его неофициальных названий:

"Transient EManations Protected from Emanating Spurious Transmissions"

"Transient Electromagnetic Pulse Emanation STandard"

"Telecommunications Emission Security STandards"

Многие фирмы выпускают широкую номенклатуру мощных современных компьютеров, полностью удовлетворяющих всем требованиям TEMPEST. При этом полностью сохраняются как эргономические показатели компьютера, так и его дизайн. В последнее время заметна тенденция применения в защищенных компьютерах современных жидкокристаллических мониторов. Современные защищенные компьютеры поддерживают все функции обычных компьютеров, включая мультимедийные возможности. Отдельное направление в производстве защищенных компьютеров представляют модели портативных компьютеров с защитой информации.

Важно отметить, что возможность серийного изготовления защищенных компьютеров обусловлена тем, что в большинстве развитых стран государственные органы определяют строгие правила, регламентирующие производство подобных устройств, и существует развитая система стандартов, определяющая требования к защищенным компьютерам, правила измерения их параметров и порядок их аттестации.

В США национальная TEMPEST политика была установлена National Communications Security Committee Directive 4 в 1981 году (“National Policy on Control of Compromising Emanations”). Стандарты и требования к измерительным приборам и методикам описаны в секретном документе NACSIM-5100A (National Communication Security Instruction).

В США введена следующая классификация устройств и систем с защитой информации:

TEMPEST Level 1 – оборудование данного класса относится к категории высшей степени секретности; оборудование должно быть утверждено АНБ США и предназначено для использования только правительственными учреждениями США (аналог стандарта NATO AMSG-720B);

TEMPEST Level 2 – оборудование данного класса предназначено для защиты менее секретной, но «критичной» информации, однако также требуется одобрение АНБ США (аналог стандарта NATO AMSG-788A);

TEMPEST Level 3 – оборудование данного класса предназначено для защиты несекретной, «критичной» и коммерческой информации; оборудование регистрируется NIST (National Institute of Standards and Technology).

Особенностью TEMPEST как государственной политики является то, что в ней предусмотрена классификация ZONE, устанавливающая требования для устройств, предназначенных для частного бизнеса. Классификация ZONE позволяет применять менее дорогие устройства, но она обязательна для производителей аппаратуры данного назначения. Поэтому негосударственные организации также имеют возможность защиты от разведывательных действий конкурентов с определяемой государственными стандартами степенью надежности.

В нашей стране защищенные компьютеры не получают широкого распространения не только из-за того, что действующие нормы несколько устарели, но и вследствие непонимания важности защиты компьютеров от утечки информации по каналам побочного электромагнитного излучения. В частности, широко

распространено мнение, что основным источником излучения ПК является излучение монитора и что перехват этого излучения в техническом плане наиболее прост. Отсюда следуют советы, что достаточно только применить хороший монитор, чтобы защитить информацию. Однако, в ПК присутствует ряд других не менее опасных излучений, например излучение клавиатуры, перехват которого может вскрыть пароли, не отображаемые на экране монитора. Классическим примером является удачный перехват информации, который описал бывший сотрудник английской разведки МИ-5 Peter Wright. В описанном им случае было перехвачено излучение не монитора.

Таким образом, наряду с разработкой новых нормативных требований по защите информации, необходима разработка концепции построения компьютеров с защитой информации. В основе концепции построения защищенных компьютеров должен лежать системный подход. В рамках такого подхода компьютер как объект ТЗИ необходимо рассматривать как сложную систему, состоящую из генераторов, модуляторов, нелинейных элементов и антенн. В такой системе опасными являются как излучения элементов компьютера (клавиатура, монитор и т. п.), так и излучения на комбинационных частотах, возникающих в результате воздействия излучений двух любых элементов компьютера на нелинейные элементы. Вторым опасным каналом является утечка информации в результате высокочастотного навязывания. Применение в конструкции компьютера элементов, обладающих микрофонным эффектом, приводит к тому, что стороне, ведущей разведку, становятся доступны не только данные, обрабатываемые в компьютере, но и содержание разговоров, ведущихся в помещении, где установлен компьютер. Более того, воздействие посторонних высокочастотных колебаний, подаваемых, например, по цепям электропитания или непосредственно по эфиру, на нелинейные элементы также приводит к появлению комбинационных частот, излучаемых в эфир.

Выбор метода защиты такой системы должен основываться на следующих критериях:

- обеспечение требуемого уровня защиты;
- биологическая защита оператора;
- технологическая пригодность к серийному производству;
- защита от электромагнитного терроризма;
- сохранение дизайна и эргономических показателей.

Наиболее полно удовлетворяет вышеперечисленным критериям пассивный метод, т. е. сочетание экранирования корпуса и отдельных элементов компьютера с фильтрацией. При применении пассивного метода одновременно решаются как задачи устранения побочных излучений, так и задача защиты от высокочастотного навязывания. Кроме того, при применении пассивного метода можно получить достоверные результаты эффективности защиты в условиях специализированной лаборатории, а не только непосредственно на объекте. Поэтому именно пассивный метод лежит в основе производства мультимедийных ПК “Expert” с защитой информации, которые соответствуют современным требованиям по обработке текстовой, графической, аудио и видеоинформации.

Производство таких ПК организовано в соответствии с действующими в настоящее время стандартами и нормативными документами. Однако, проведенные нами исследования особенностей побочных электромагнитных излучений выявили потенциальную опасность перехвата информации даже у ПК, полностью удовлетворяющих существующим нормативным требованиям. Это заставляет нас применять более жесткие внутренние нормативные требования. Такое положение дел свидетельствует о настоятельной необходимости приведения существующей нормативной базы в соответствие с требованиями по эксплуатации ПК и возможностями современной техники перехвата информации.

Системный подход показывает также, что компьютер – это базовый элемент сложной системы. Информация в электронном виде может храниться, передаваться и обрабатываться (рис. 1).

Рисунок 1 – Возможные состояния информации в электронном виде

Каждому состоянию информации соответствует определенная конфигурация вычислительных средств и должны соответствовать определенные меры защиты этой информации.

В автономных компьютерах осуществляется обработка и хранение информации, а при удаленном подключении или подключении к глобальной сети интернет – и передача информации (обмен информацией). В локальной вычислительной сети осуществляются все виды работ с информацией: ее хранение, обработка и передача. Поэтому наиболее жесткие требования по защите информации должны устанавливаться для компьютеров, работающих в составе локальной вычислительной сети. Поэтому и вопросы технической защиты компьютера на современном этапе необходимо рассматривать в предположении, что компьютер работает в составе локальной вычислительной сети.

В локальной вычислительной сети все элементы сети связаны между собой кабельной системой (обычно экранированная или неэкранированная витая пара). Наряду с возможностью перехвата по побочному излучению информации, передаваемой в локальной сети, кабельная система играет роль антенны для побочных излучений каждого компьютера и сервера. Кроме того, активное оборудование локальной сети так же является источником электромагнитных колебаний. Излучение активного оборудования само по себе может не представлять опасности с точки зрения защиты информации, но это излучение по проводам кабельной системы проникает в компьютер и может вызывать дополнительные излучения на комбинационных частотах. Таким образом, спектральный состав излучения одного и того же компьютера при автономной работе и при работе в локальной сети может значительно отличаться.

Для технической защиты информации в локальной сети возможны три метода: экранирование системных блоков нескольких компьютеров и сетевых соединений в одном монтажном шкафу с выносом на рабочее место монитора и клавиатуры, создание единого экранированного объема для всех компьютеров и серверов и применение волоконно-оптических линий. Любой метод имеет определенные особенности в реализации, но общим (и самым трудным) вопросом является создание единого замкнутого экранированного объема, в котором располагаются все элементы локальной сети (рис. 2).

Наиболее сложным вопросом при построении локальной сети, защищенной от утечки информации по каналам побочного излучения, является правильная организация заземления. Существуют различные схемы организации заземления, не ухудшающего экранирующих свойств системы. Наиболее просто реализуется принцип заземления всего экранированного объема только в одной точке. Однако, корпуса всех компьютеров должны заземляться согласно требования техники электробезопасности. Поэтому защитное заземление, которое требуется по правилам техники безопасности, должно подключаться к каждому компьютеру, но через фильтр. В частности, защищенные компьютеры «Експерт» обязательно комплектуются устройством согласования с сетью электропитания, одной из функций которого и является фильтрация высокочастотных колебаний в цепи защитного заземления.

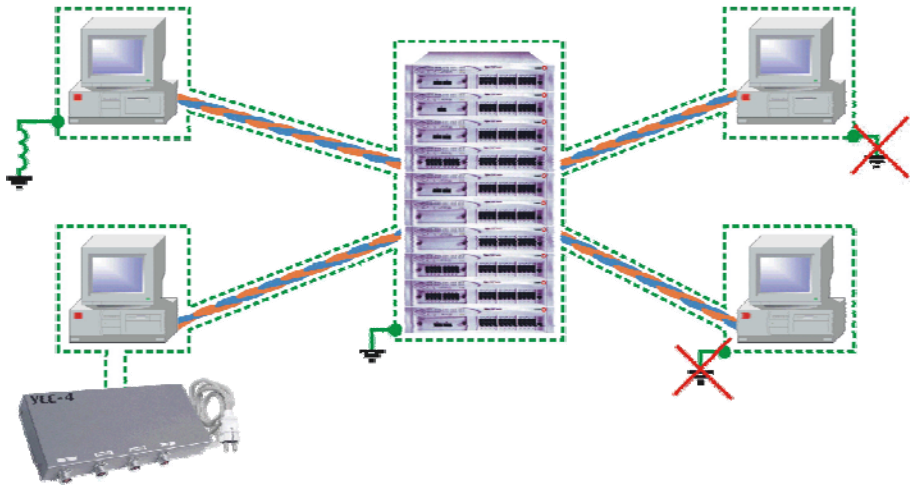

Рисунок 2 – Замкнутый экранированный объем, в котором расположены все элементы локальной сети.

Широкое распространение защищенных локальных сетей сдерживается отсутствием методик построения таких сетей и, что более важно, отсутствием методик оценки уровня защищенности таких сетей. Реально в настоящее время можно получить официальное подтверждение степени защищенности только после проведения специсследования всего объекта, на котором развернута локальная сеть.

Выводы

Концепция построения компьютеров с защитой информации должна быть основана на использовании системного подхода к обеспечению защиты информации, циркулирующей в сети, поскольку компьютер является БАЗОВЫМ ЭЛЕМЕНТОМ сложной распределенной вычислительной СИСТЕМЫ (сети). Системный подход позволяет обеспечить комплексное решение проблемы защиты информации при ее обработке, хранении и передаче.

Производство и применение компьютеров с защитой информации должно быть организовано в четком соответствии с действующими законами, инструкциями и нормативными документами. При этом многие действующие в настоящее время нормы требуют пересмотра. Государство должно также установить определенные требования и правила применения защищенной техники коммерческими (не государственными) структурами.

При производстве защищенных компьютеров необходима стандартизация и унификация используемого оборудования, узлов и компонентов, что обеспечивает возможность серийного производства ПК с защитой информации с низкой стоимостью как покупки, так и эксплуатации.

Производство защищенных компьютеров должно быть основано в основном на пассивных методах предотвращения утечки информации по техническим каналам. В основе таких методов лежит экранирование, фильтрация, заземление и другие аппаратно-программные схемотехнические решения.

Компьютеры с защитой информации должны обладать всеми возможностями современного производительного мультимедийного компьютера для обработки текстовой, графической, аудио и видеоинформации.

Необходимо проведение масштабных исследований, направленных на определение норм и разработку рекомендаций по изготовлению и применению защищенных компьютеров в локальных сетях.

Реализация такой концепции настоятельно требует постоянной совместной исследовательской работы государственных учреждений и частного бизнеса в области защиты информации. Такое сотрудничество позволит своевременно создать и внедрить эффективную законодательную и нормативную базу производства, распределения и эксплуатации компьютеров с защитой информации, что в конечном итоге обеспечит требуемую безопасность современного информационного общества, которым уже становится наша Украина.