УДК 681.3

Чеховский С.А.

ЭЛЕКТРОМАГНИТНЫЕ ИЗЛУЧЕНИЯ КОМПЬЮТЕРНЫХ СИСТЕМ И ЗАЩИТА ИНФОРМАЦИИ

«Тот факт, что электронные приборы такие как, например, компьютеры, принтеры, излучают электромагнитные волны, представляет собой угрозу для Правительства США. Злоумышленники … могут перехватить секретную информацию…»
(Из отчета "Redefining Security" Комиссии по Безопасности Соединений директору ЦРУ, 1994)

Одним из возможных каналов утечки информации является излучение элементов компьютера. Принимая и декодируя эти излучения, можно получить сведения обо всей информации, обрабатываемой в компьютере. В Украине этот канал утечки информации называется ПЭМИН (Побочные ЭлектроМагнитные Излучения и Наводки). В Европе и Канаде применяется термин "compromising emanation" – компрометирующее излучение. В Америке применяется термин «TEMPEST».

Аббревиатура TEMPEST (Telecommunications Electronics Material Protected From Emanating Spurious Transmissions) появилась в конце 60-х – начале 70-х годов, как название секретной программы Министерства Обороны США по разработке методов предотвращения утечки информации через различного рода демаскирующие и побочные излучения электронного оборудования. В настоящее время термин «TEMPEST» не является аббревиатурой и применяется и как синоним компрометирующих излучений (по-нашему ПЭМИН), и как название технологии, минимизирующей риск утечки секретной информации путем перехвата и анализа различными техническими средствами побочных электромагнитных излучений. В понятие TEMPEST входят также стандарты на оборудование, средства измерения и контроля. Вполне допустимы названия типа "TEMPEST tests", "TEMPEST computer" и т.п. Довольно часто термин TEMPEST используется и в контексте описания средств нападения (TEMPEST - атака, TEMPEST - подслушивающие устройства). В принципе, это неправильно. TEMPEST предназначен для пресечения побочных излучений, а не для их использования. Однако, такое применение термина встречается довольно часто и не приводит к неправильному толкованию.

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"

даже вплоть до несерьезных:

- "Tiny ElectroMagnetic Pests Emanating Secret Things" (крошечные электромагнитные вредители, выделяющие секретные вещи)

Официально же к проблемам TEMPEST в развитых странах относятся очень серьезно. Так, в США национальная TEMPEST политика была установлена National Communications Security Committee Directive 4 в 1981 году ("National Policy on Control of Compromising Emanations"). В секретном документе NACSIM-5100A (National Communication Security Instruction) описаны стандарты и требования к измерительным приборам и методикам, инструкции по защите от побочных излучений.

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

• TEMPEST Level 1 (аналог стандарта NATO AMSG-720B) – оборудование данного класса относятся к категории высшей степени секретности. Оборудование должно быть утверждено Агентством Национальной Безопасности США (NSA) и предназначено для использования только правительственными учреждениями США.

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

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

Для частного бизнеса используется классификация ZONE, которая позволяет применять менее дорогие устройства.

Сертификация TEMPEST оборудования описана в документе Агентства Национальной Безопасности "NSA TEMPEST Endorsement Program".

История возникновения TEMPEST своими корнями уходит в далекий 1918 год, когда Герберт Ярдли (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. С этого времени средства радио- и радиотехнической разведки стали непременным реквизитом шпионов различного уровня. По мере развития технологии развивались как средства TEMPEST-нападения (разведки), так и средства TEMPEST-защиты.

Современные достижения в области технологии производства радиоприемных устройств позволили создавать очень миниатюрные чувствительные приемники. Успешно внедряется многоканальный прием сигналов (как с различных направлений, так и на различных частотах), с последующей их корреляционной обработкой. Это позволило значительно увеличить дальность перехвата информации.

Для борьбы с TEMPEST-атаками разрабатываются специальные конструкции компьютеров, обладающих малым уровнем побочных излучений. В конструкции таких компьютеров применяются экранирующие покрытия из специальных материалов и высокоэффективные фильтры, разработанные с целью получения большого затухания в широкой полосе частот.

Особенно бурное развитие TEMPEST-технологии получили в конце 80-х, начале 90-х годов. Это связано как с осознанием широкой общественностью опасности TEMPEST угроз, так и с широким развитием криптографии. Применение при передаче информации стойких алгоритмов шифрования зачастую не оставляет шансов дешифровать перехваченное сообщение. В этих условиях TEMPEST-атака может быть единственным способом получения хотя бы части информации до того, как она будет зашифрована.

Некоторые вехи истории развития TEMPEST как технологии и практики разведки приведены в приложении к данной статье.

Долгое время все, что было связано с понятием TEMPEST, было окутано завесой секретности. Первое сообщение, появившееся в открытой печати, принадлежит голландскому инженеру Вим ван Эку (Wim van Eck), опубликовавшему в 1985 году статью «Электромагнитные излучения видеодисплейных модулей: Риск перехвата?» [1]. Статья посвящена потенциальным методам перехвата композитного сигнала видеомониторов. В марте 1985 года на выставке Securecom-85 в Каннах ван Эк продемонстрировал оборудование для перехвата излучений монитора. Эксперимент показал, что перехват

возможен с помощью слегка доработанного обычного телевизионного приемника. Завеса тайны была прорвана.

Известные Tempest-атаки

Показательными были откровения бывшего сотрудника английской разведки МИ-5 Питера Райта (Peter Wright), опубликованными в его книге воспоминаний «Шпионский улов» [2] 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 усилия МИ-5 по вскрытию шифра не увенчались успехом. Тем не менее, Питер 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, впрочем, как и любая другая электрическая машина, 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. Классический пример использования TEMPEST-атаки!

Безусловно, это далеко не единственный пример результативного применения TEMPEST-атаки, но шпионские организации не стремятся поделиться своими тайнами с широкой общественностью. Более того, TEMPEST-атаки по отношению друг к другу стали применять и конкурирующие коммерческие фирмы, и криминальные структуры. Так, в частности, проблема применения TEMPEST-технологий мошенниками с кредитными карточками к 1997 году стала настолько острой, что ей специально уделено внимание на конференции "Eurocrypt'97".

Развитие тактики применения TEMPEST-атак позволило не только пассивно ждать, когда в перехваченных сигналах появится нужная информация, но и целенаправленно управлять излучением компьютера с помощью программных закладок.

Сегодня разработаны методы программного управления электромагнитными излучениями, т.н. Soft TEMPEST. Эта технология является совершенно новым подходом к несанкционированному съему информации.

Процесс перехвата секретной информации путем приема паразитного излучения композитного сигнала монитора вполне реален, но процесс этот достаточно длителен - нужно дождаться, пока пользователь выведет на экран монитора интересующую секретную информацию, а не традиционный Солитер. Такой процесс может занимать дни и недели.

А нельзя ли компьютер заставить передавать нужную информацию и не ждать пока пользователь сам обратится к секретным документам? Таким вопросом задались сотрудники компьютерной лаборатории Кембриджского университета Маркус Кун (Markus G.Kuhn) и Росс Андерсон (Ross J.Anderson).

Суть их идеи была достаточно проста.

Нужный компьютер «заражается» специальной программой-закладкой («троянский конь») любым из известных способов (по технологии вирусов: через компакт-диск с презентацией, интересной программой или игрой, дискету с драйверами, а если ПК в локальной сети – то и через сеть). Программа ищет необходимую информацию на диске и путем обращения к различным устройствам компьютера вызывает появление побочных излучений. Например, программа-закладка может встраивать сообщение в композитный сигнал монитора, при этом пользователь, играя в любимый Солитер, даже не подозревает,

что в изображение игральных карт вставлены секретные текстовые сообщения или изображения. С помощью разведывательного приемника (в простейшем варианте все тот же доработанный телевизор) обеспечивается перехват паразитного излучение монитора и выделение требуемого полезного сигнала.

Проведенные Маркусом в 1998 году экспериментальные исследования подтвердили такую возможность добывания секретной информации.

Так родилась технология Soft Tempest – технология скрытой передачи данных по каналу побочных электромагнитных излучений с помощью программных средств [3]. Предложенная учеными Кембриджа технология Soft Tempest по своей сути есть разновидность компьютерной стеганографии, т.е. метода скрытной передачи полезного сообщения в безобидных видео, аудио, графических и текстовых файлах.

Методы компьютерной стеганографии в настоящее время хорошо разработаны и широко применяются на практике. По информации спецслужб США методы компьютерной стеганографии интенсивно используются международным терроризмом для скрытой передачи данных через Интернет, в частности во время подготовки теракта 11 сентября.

Особенностью технологии Soft Tempest является использование для передачи данных канала ПЭМИН, что значительно затрудняет обнаружение самого факта несанкционированной передачи по сравнению с традиционной компьютерной стеганографией. Действительно, если для предотвращения несанкционированной передачи данных по локальной сети или сети Интернет существуют аппаратные и программные средства (FireWall, Proxy server и т.п.), то средств для обнаружения скрытой передачи данных по ПЭМИН нет, а обнаружить такое излучение в общем широкополосном спектре (более 1000 МГц) паразитных излучений ПК без знания параметров полезного сигнала весьма проблематично.

Основная опасность технологии Soft Tempest заключается в скрытности работы программы-вируса. Такая программа, в отличие от большинства вирусов не портит данные, не нарушает работу ПК, не производит несанкционированную рассылку по сети, а значит, долгое время не обнаруживается пользователем и администратором сети. Поэтому, если вирусы, использующие Интернет для передачи данных, проявляют себя практически мгновенно, и на них быстро находится противоядие в виде антивирусных программ, то вирусы, использующие ПЭМИН для передачи данных, могут работать годами, не обнаруживая себя.

В настоящее время технология Soft Tempest включает в себя не только способы разведки, но и программные способы противодействия разведке, в частности использование специальных Tempest – шрифтов, минимизирующих высокочастотные излучения.

Практически все открытые работы по проблеме Soft Tempest посвящены именно возможностям программного формирования изображения на экране монитора, в котором содержится другая информация, и возможностям программной защиты от этой напасти. Но программно можно управлять излучением практически любого элемента компьютера. Так, на прошедшей недавно выставке «Безпека 2002» мы демонстрировали возможность программной передачи информации путем вывода в незадействованный последовательный порт (см. также [4]). Интерфейс программы представлен на рис.1.

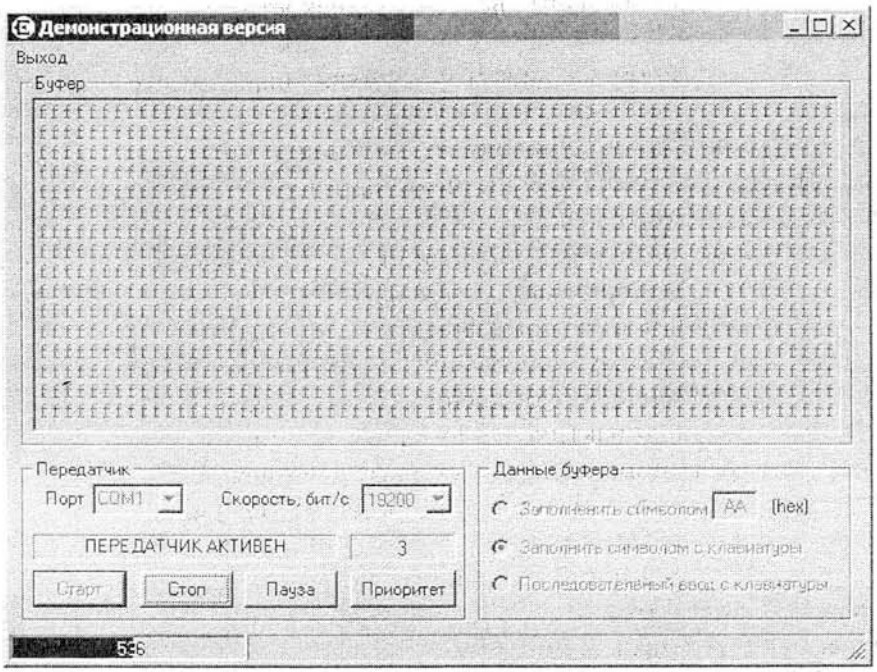
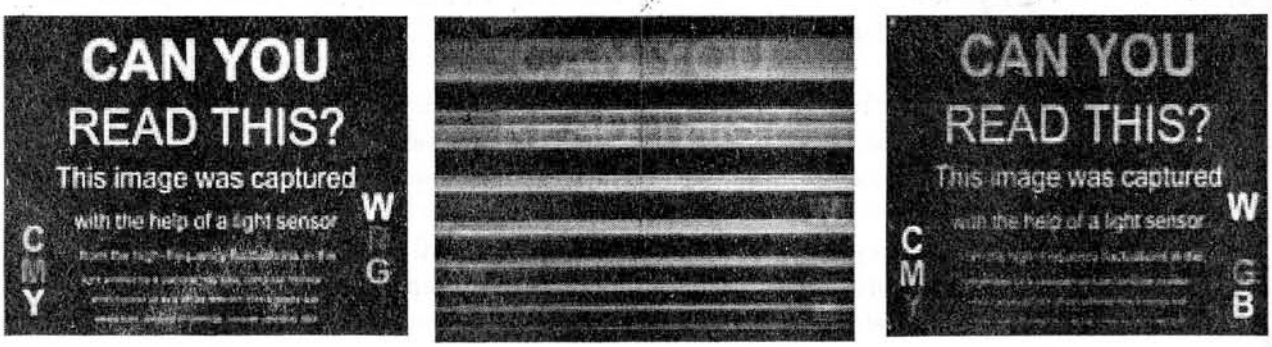


Рис. 1 Интерфейс Soft-TEMPEST программы, разработанной ЕПОС

Прием возникающего при этом излучения осуществлялся с помощью приемника AR3000A.

Вплотную к вопросу скрытой передачи информации путем излучения монитора примыкает вопрос визуального наблюдения за экраном монитора. Если к вопросу сохранности секретных сведений относятся сколь-нибудь внимательно, то монитор будет установлен таким образом, чтобы его нельзя было рассмотреть через окно. Недоступен монитор будет и для обзора случайными посетителями. Однако световой поток экрана монитора отражается от стен, и этот отраженный световой поток может быть перехвачен. Современная техника позволяет восстановить изображение на мониторе, принятое после многократных отражений его от стен и всех предметов (рис.2, [5]).



а) *б)* *в)*

Рис.2. Изображение на экране монитора: а) тестовое изображение; б) перехваченное после многократных переотражений изображение; в) перехваченное изображение после специальной обработки.

Однако извлечь информацию в оптическом диапазоне можно не только из светового излучения монитора. Практически любое электронное устройство имеет светодиодные индикаторы режимов работы. Светодиоды имеют малую инерционность, и

позволяют модулировать световой поток сигналами с частотой до сотен мегагерц. Наводки от всех элементов блока, в котором установлен светодиод, приводят к тому, что световой поток постоянно включенного светодиода оказывается промодулирован высокочастотными колебаниями, незаметными для глаза, но которые могут быть обнаружены с помощью специальной аппаратуры.

Бытует мнение, что ПЭМИН (в США TEMPEST) – это надуманная проблема. Считается, что криптография может решить все проблемы. Временами бросаются в другую крайность: ПЭМИН – это самый опасный канал утечки информации.

Бросаться из крайности в крайность не следует. Не надо ни переоценивать, ни недооценивать опасность утечки информации по каналам ПЭМИН. Техническая защита информации – это трудоемкое и очень дорогое удовольствие. Но и разведчику не сладко. Его аппаратура еще дороже. Поэтому к вопросу применения технической защиты информации необходимо подходить философски. Если Вы вообще никаких мер не предпринимаете для защиты информации, то и на TEMPEST можно уверенно махнуть рукой. Информацию у Вас украдут более дешевым способом. Если же у Вас вся информация шифруется (в том числе и при обмене в локальной сети), если на границе Вашей сети установлен надежный FireWall и предприняты все другие подобные меры, то Вы ничего не оставили охотникам за Вашей информацией. Они предпримут TEMPEST-атаку.

Более того, нельзя, например, полагаться на канальный шифратор, подключаемый к последовательному порту компьютера, если это не TEMPEST-компьютер. Последовательная передача информации очень легко перехватывается, а в данном случае это ведь и есть секретная информация в открытом виде.

Ходит миф, что самым опасным источником излучений является монитор. Довольно часто конкретизируют: опасен CRT монитор. (Отсюда следует, что TFT монитор безопасен).

Скорее всего, это миф появился, потому что наиболее известные и популярные работы в открытой печати (например, упомянутая выше статья голландского инженера Вим ван Эка) связаны именно с исследованием вопросов перехвата излучений мониторов. Более того, эти эксперименты очень эффектно выглядят, поэтому в такой миф легко поверить. Мы демонстрировали подобный эксперимент на выставке «Безпека – 2000» (через 15 лет после голландца, но в Украине такими вещами не часто балуют). Как правило, после демонстрации приходилось долго убеждать, что не только монитор является источником побочных излучений.

Излучение монитора это, безусловно, очень опасный канал утечки информации, но далеко не единственный. Излучают большинство элементов компьютера, и в большинстве случаев излучение этих элементов может содержать ценную информацию. Так, в частности, наиболее важной информацией является, как правило, пароль администратора локальной сети. При вводе пароля последний не отображается на экране монитора, поэтому не может быть разведан путем анализа излучений монитора или визуальным наблюдением. Однако сигналы, излучаемые клавиатурой, могут быть непосредственно перехвачены [8]. При этом доступной становится вся информация, вводимая с клавиатуры, в том числе и пароль администратора сети.

Любое излучение, даже не содержащее информации, обрабатываемой в компьютере, может быть информативным в плане разведки. При недостаточной жесткости корпуса компьютера любое излучение может модулироваться речевой информацией. Получается, что если не предпринять специальных мер, то, устанавливая на рабочем месте компьютер, Вы своими руками устанавливаете подслушивающее устройство.

Даже если излучение каких либо элементов действительно не несет никакой информации, это излучение индивидуально для каждого компьютера. По индивидуальным

признакам можно отследить перемещение компьютера, определить временной режим работы данного компьютера.

Что же касается безопасности TFT мониторов, то она не намного лучше, чем у CRT мониторов. По крайней мере, сейчас можно встретить CRT монитор с уровнем излучений не выше, чем у многих TFT мониторов. Кроме того, сигналы, необходимые для получения изображения, формируются в видеокарте и по достаточно длинному (в радиотехническом смысле) кабелю подаются на монитор. Поэтому сигналы монитора можно перехватить и вообще без монитора. Был бы только кабель.

Встречается заблуждение, что информацию, циркулирующую в локальной сети, перехватить нельзя. Мотивируется это тем, что современные локальные сети строятся по топологии «звезда», при этом всегда параллельно укладывается несколько кабелей, каждый из которых подключен к своей рабочей станции. Считается, что происходит взаимное «глушение» сигналов, распространяющихся в параллельных кабелях. Как следствие, иногда допускается объединение в локальную сеть рабочих станций, каждая из которых имеет разрешение на обработку грифованной информации в автономном режиме.

Сигналы в локальной сети не могут «заглушить» друг друга в силу специфики протоколов передачи данных в локальной сети. Кроме того, не все рабочие станции начинают и заканчивают свою работу одновременно. Чаще всего часть своей работы системный администратор вынужден выполнять в нерабочее время, когда остальные рабочие станции выключены. В это время создаются идеальные условия для перехвата информации, передаваемой по локальной сети. Если администратор в нерабочее время производит архивное копирование содержимого жесткого диска сервера, то он демонстрирует содержимое этого диска всем желающим радиолюбителям и TEMPEST-шпионам.

Более того, подключение кабелей локальной сети создает специфические проблемы. Ведь эти кабели не только участвуют в передаче информации в соответствии с сетевыми протоколами, но и являются очень хорошими антеннами, подключенными к компьютеру. Поэтому подключение в локальную сеть не только создает предпосылки для перехвата информации, передаваемой по локальной сети, но и затрудняет подавление излучений самого компьютера (и монитора, и клавиатуры и всех других его элементов). Эти вопросы настолько важны, что мы планируем посвятить отдельную статью вопросам построения защищенных локальных сетей.

Приложение

Основные вехи истории TEMPEST

1918 г. Герберт Ярдли и Black Chamber открыли, что различные электронные устройства для обработки секретной информации имеют побочные излучения и что эти излучения можно использовать для восстановления секретных данных.

1934 г. Закон о связи (Communications Act) предоставил всем равные возможности для законного использования радиочастотного спектра. Учреждена Федеральная комиссия по связи (FCC); для определения измерений и структуры радиочастотных излучений сформирован Международный специальный комитет по радиопомехам (CISPR).

1946 г. Основана Канадская Организация по защите связи (CSE), ее основной целью является коммуникационная безопасность (COMSEC).

Основано Агентство по перехвату информации Великобритании (GCHQ).

1950-е г.г. Прослушивание NATO телефонных линий в берлинском туннеле определило наличие открытых сигналов в шифрованной телетайп связи стран Варшавского Договора, это первый известный пример атаки путем взлома (HIJACK).

Rand Corporation серьезно изучает вопросы экранирования для защиты от побочных излучений.

1950 г. Китайская разведка использует специальные акустические методы разведки против иностранных посольств в Пекине.

1952 г. Используя метод, подобный лазерному прослушиванию, КГБ прослушивало американское посольство, используя государственную печать как жучка. В дальнейшем технология была развита и получила название высокочастотного навязывания. Технология использовала такие непреднамеренные излучатели, как обычные электролампы и электропроводку.

Середина 1950-х гг. Правительство США начинает интересоваться TEMPEST и учреждает программу TEMPEST. Разработан первый TEMPEST стандарт NAG-1A.

Изготовители телевизоров работают над проблемами побочного излучения гетеродинов. Британия затем использовала эти наработки для введения лицензирования ТВ.

1956 г. Британская разведка взломала шифр египетской машины Hagelin, детектировав шумы, прослушанные с помощью телефонного жучка (операция Engulf).

1957 г. IBM совместно с ITT и Analex дорабатывают Selectric в специальный высокоемкий терминал для ввода/вывода секретной информации. Терминал специально разработан для радикального снижения всех видов излучений.

1958 г. ВВС США запускают противовоздушную систему SAGE с графическими терминалами.

Британская разведка на расстоянии до 200 футов принимает побочные излучения аппаратуры, установленной в советском посольстве, чтобы определить частоты излучения (операция Rafter).

1960 г. Агентство по защите связи Канады включает в цели TEMPEST.

Британская разведка проводит атаку на проводные каналы связи, защищенные французской дипломатической шифровальной машиной (с использованием высокочастотного навязывания).

ФБР также проводит подобную операцию против французского посольства в Вашингтоне.

1962 г. Во время Карибского кризиса NSA (на борту разведсудна Oxford) предприняло попытку обойти непревзойденную советскую систему шифрования, перехватывая излучения шифровальных машин, расположенных на советских радиостанциях в Кубе. Проводились также попытки перехватить шумовые выбросы, раскрывающие установки ротора в старых шифровальных машинах.

1967 г. TEMPEST впервые публично обсуждается на компьютерной конференции Spring. Уиллис Вар (Willis Ware) из Rand отметил TEMPEST угрозы. (Первое упоминание о TEMPEST на несекретной встрече произошло в 1965г.)

Опубликован NAG-8/TSEC (Информационный меморандум TEMPEST). Замещен NACSIM 5000.

1973 г. В соответствии с Постановлением СМ СССР №903-303 от 18 декабря 1973 года создана Государственная техническая комиссия СССР (в составе представителей от КГБ, Минобороны, министерств оборонной промышленности). Аппарат Гостехкомиссии состоял из Управления, Инспекции и территориальные подразделений Гостехкомиссии в Москве, Ленинграде, Киеве, Минске, Тбилиси, Свердловске, Новосибирске, Ташкенте (позднее к ним добавились Рига, Хабаровск).

Середина 1970-х. КГБ уличил польскую разведку в перехвате излучений силовых линий военного объекта в Москве. КГБ убедился, что советские шифровальные машины уязвимы, пока их не поместили в стальные кожухи с генераторами шума (наводящими помехи на телевизоры на расстояниях до одной мили) и автономными двигатель-

генераторами. Последние достижения КГБ в исследованиях методов перехвата радиоизлучений, включающих использование рентгеновского и радиоизотопного излучений, подтвердили их уязвимость.

1979 г. Don Britton Enterprises продает устройства для восстановления сигналов из кабельных систем «с утечкой».

Канадская Организация по защите связи (CSE) заимствует у NSA радиозащитный тент для тестов по операции Pilgrim, тестирование побочных излучений проводилось на расстоянии 150 футов.

FCC принимает минимальные технические и административные требования к ограничению помех компьютеров и др. цифрового электронного оборудования.

1980-е г.г. TEMPEST-прослушивающие устройства производства Великобритании распространяются в таких местах, как гольф клуб Гонконг и Кембриджский университет.

ФБР демонстрирует TRW возможность сбора TEMPEST информации посредством излучений ПК.

1981 г. Опубликован NACSIM 5100A (Требования к лабораторным тестам компрометирующих электромагнитных излучений); замещен NSTISSAM/1-91.

Опубликован NCSC 3 (Глоссарий TEMPEST); замещен NSTISSI 7002.

Отчет Конгресса США допускает TEMPEST шпионаж для иностранных посольств.

1983 г. Совет национальной полиции (National Police Board) Швеции информирует шведских бизнесменов о TEMPEST.

Альберт Гор обсуждает TEMPEST с представителем Национальной лаборатории Лос-Аламоса (Los Alamos National Laboratory) на слушаниях Конгресса.

Вим ван Эк (Wim Van Eck) начинает исследования TEMPEST в Голландии.

1984 г. Опубликована Директива 5004 по национальной коммуникационной безопасности (National Communications Security Instruction, NACSI) (Меры противодействия TEMPEST для предприятий США); замещена NTISSI 7000. NSA публикует требования к TEMPEST безопасности для своих подрядчиков, работающих со SCIF информацией.

FCC вводит сертификацию микрокомпьютеров по помехам.

Правительство Израиля предоставляет Джонатану Полларду (Jonathan Pollard) экранированный фотокопировальный аппарат для копирования секретных документов в вашингтонском посольстве. Правительство Швеции публикует брошюру «Компьютеры с утечкой» (Leaking Computers), ставшую бестселлером шведских бизнесменов.

Западно-Германская полиция задерживает польского разведчика, занимавшегося TEMPEST прослушиванием.

NSA становится во главе TEMPEST программы США и дает рекомендации NTSSC.

1985 г. Iverson создает TEMPEST вариант IBM PC; Grid Federal Systems создает портативный TEMPEST компьютер с плазменным дисплеем, одобренный NSA.

Голландский ученный Вим ван Эк публикует несекретную статью о возможности TEMPEST прослушивания на расстояниях до 1 км после демонстрации такой возможности на Securicom'85 во Франции. Это произвело фурор из-за простоты и общедоступности.

В Tomorrow's World на телеканале BBC показана 5-минутная демонстрация TEMPEST. Цели – новый Скотланд Ярд и офис в Лондоне.

Поправка к криминальному кодексу (Criminal Amendment Act) Канады делает прием TEMPEST криминально наказуемым.

NSA COMSEC публикует «Методику для обработки TEMPEST информации в устройствах, системах, оборудовании».

1986 г. Правительство США запретило демонстрацию на конференции Института компьютерной безопасности (Computer Security Institute, CSI) системы, защищающей от TEMPEST.

NSA запретило Wang Corporation демонстрировать TEMPEST.

В правительственном отчете США говорится о необходимости лучшей оценки мер противодействия для Министерства обороны.

Опубликована Директива 4002 по безопасности национальных телекоммуникаций и информационных систем (National Telecommunications And Information Systems Security Instruction, NTISSI).

Список TEMPEST целей (приблизительно 180 объектов) польской разведки обнаружен в Германии.

МИД ГДР обеспокоен повышенным уровнем излучения Robotron PC, установленных в посольствах ГДР.

1987 г. Zenith поставляет Пентагону 12 тыс. TEMPEST ПК.

NSA предлагает компании не проводить TEMPEST демонстрацию на конференции Interface '87.

Чехословацкие разведчики предположительно проводили TEMPEST прослушивание военных объектов США, маскируясь под туристов.

Шин Уолкер (Sean Walker), репортер BBC, продемонстрировал TEMPEST на ярмарке с помощью устройства ван Эка, настраиваясь на компьютеры экспонентов.

NTISSAM COMPUSEC/1-87 рассматривает TEMPEST как потенциальную угрозу.

Ван Эк получает патент на TEMPEST видео терминал, использующий скремблирование растра.

1988 г. Реструктурирован Список рекомендованной TEMPEST продукции (Endorsed TEMPEST Product List). Опубликован NTISSP 300 (Национальная политика контроля компрометирующих излучений); замещен NTISSI 7000 (Средства и меры противодействия TEMPEST); замещен NSTISSI 7000.

В программе BBC «High Tech Spies» проведена вторая демонстрация TEMPEST; цели – лондонские юридические и брокерские конторы.

Редактор Computers and Security корректирует информацию ван Эка в журнале Abacus и позже в Computers and Security.

Consumertronics из Нью-Мехико публикует схемы устройства ван Эка и др. информацию в брошюре Beyond Van Eck Phreaking. Ян Мерфи (Ian Murphy) представляет схемы TEMPEST приемника.

В Италии прошел Первый международный симпозиум по электромагнитной безопасности и защите информации (SEPI).

1989 г. Центральное агентство по компьютерам и телекоммуникациям Великобритании публикует TEMPEST:The Risk.

NSA издает проект спецификаций для высококачественных экранированных камер.

1990 г. Британский Закон о некорректном использовании компьютеров исключает TEMPEST прослушивание из угроз и утверждает его как законное действие.

Журнал публикует статью Питера Смулдерса (Peter Smulders) из Университета Ейндховена о технологии прослушивания TEMPEST по кабелю RS-232.

Кристофер Селин (Christopher Seline) опубликовал в Интернет обзор американских законов, касающихся TEMPEST.

Для стимулирования национальной деятельности в области TEMPEST при NSTISSC создана консультативная группа по TEMPEST (TEMPEST Advisory Group, TAG).

Инженерный корпус армии США публикует «Защита объектов от ЭМП и TEMPEST» (EMP and TEMPEST Protection for Facilities).

1991 г. Отчет ЦРУ заставил пересмотреть и снизить внутренние требования к TEMPEST. Это привело к разумной политике в отношении TEMPEST.

Опубликован (NSTISSAM)/1-91 (Требования к лабораторным тестам компрометирующих электромагнитных излучений); замещен NSTISSAM/1-92. Опубликован NSTISSAM/2-91 (Анализ компрометирующих излучений).

Опубликован NSTISSAM/3-91 (Обслуживание и ликвидация TEMPEST оборудования). До этой директивы NSA уничтожала все.

Опубликован NACSEM 5009 (Техническое обоснование границ электромагнитных компрометирующих излучений).

В Италии состоялся очередной Международный симпозиум по электромагнитной безопасности и защите информации (SEPI).

Оборот TEMPEST индустрии составляет 1,5 миллиарда долларов.

1992 г. Spy Supply из Нью-Гемпшира измучен требованиями NSA прекратить продажи устройства ван Эка.

Chemical Bank – прозрачная цель для TEMPEST атак против процессингового центра.

Опубликован NSTISSAM/1-92 (Требования к лабораторным тестам компрометирующих электромагнитных излучений). Опубликован NSTISSAM/2-92 (Методика TEMPEST зонирования)

1994 г. «Переоценка безопасности: Доклад Объединенной комиссии по безопасности министру обороны и Директору ЦРУ» рекомендует не применять мер противодействия TEMPEST, если не определена угроза. Растет важность решений зонирования.

Опубликован NSTISSI 7001 (NONSTOP Countermeasures).

1995 г. Опубликован NSTISSI 7002 (Глоссарий TEMPEST). Опубликован NSTISSAM/1-95 (Экранированные камеры). Опубликован NSTISSAM/2-95 (Red/Black Installation Guidelines). Федеральный стандарт обработки информации (Federal Information Processing Standard, FIPS) 140-1 «Требования к безопасности криптографических модулей» установил, что TEMPEST защита не требуется (для несекретных федеральных компьютерных систем).

Шифровальное ПО Blowfish Advanced 95 препятствует ведению TEMPEST мониторинга.

1997 г. На конференции Hacking in Progress демонстрировалась аналоговая TEMPEST установка на дисплее.

В ответ на проблемы сетевой безопасности WANG Corporation выпустила новые TEMPEST ПК и принтер. На Eurocrypt '97обсуждаются вопросы применения TEMPEST против смарт-карт.

WANG Corporation заключил U.S. Government Systems Acquisition and Support Services (SASS II) контракт на TEMPEST системы и их поддержку стоимостью $105 миллионов на 5 лет.

1998 г. В открытой печати появляются сообщения о "Soft TEMPEST". Для препятствования мониторинга используются специальные видеошрифты. Публикации Маркуса Куна (Markus Kuhn) и Росса Андерсона (Ross Anderson) удивили многих.

1999 г. С целью концентрации усилий в сфере защиты информации решением Президента Украины на базе Главного управления правительственной связи Службы безопасности Украины создан Департамент специальных телекоммуникационных систем и защиты информации СБ Украины, который стал головной структурой в государстве по вопросам криптографической и технической защиты информации.

2000 г. На выставке «Безпека 2000» в Киеве ЕПОС демонстрирует возможность перехвата и демодуляции излучения монитора компьютера (TEMPEST атака).

2002 г. На выставке «Безпека 2002» в Киеве ЕПОС демонстрирует возможность передачи информации путем программного управления излучением компьютера (вариант Soft TEMPEST).

Список литературы

1. Wim van Eck. Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk. Computers & Security, #4, 1985, pp. 269-286.

2. Peter Wright. Spycatcher - The Candid Autobiography of a Senior Intelligence Officer. William Heinemann Australia, 1987.

3. Markus G. Kuhn, Ross J. Anderson. Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations

4. Peter Smulders. The Threat of Information Theft by Reception of Electromagnetic Radiation from RS-232 Cables. Computers & Security, #9, 1990, pp. 53-58.

5. Markus G. Kuhn. Optical Time-Domain Eavesdropping Risks of CRT Displays. IEEE Symposium on Security and Privacy, Oakland, California, May 12-15, 2002.

6. С. Чеховский. Концепция построения компьютеров, защищенных от утечки информации по каналам электромагнитного излучения. Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах». Тезисы докладов. Издательство "Інтерлінк", Киев, 2002, стр. 80.

7. С.Р. Коженевский, Г.Т. Солдатенко. Предотвращение утечки информации по техническим каналам в персональных компьютерах. Научно-технический журнал "Захист інформації", 2002, №2, стр.32-37.

8. В. В. Овсянников, Г. Т. Солдатенко. Нужны ли нам защищенные компьютеры? Научно–методическое издание «Техника специального назначения», 2001, №1, стр. 9-11.

Поступила 23.01.2003г.

УДК 681.3

О.І.Гарасимчук, В.М.Максимович

ГЕНЕРАТОРИ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ, ЇХ ЗАСТОСУВАННЯ, КЛАСИФІКАЦІЯ, ОСНОВНІ МЕТОДИ ПОБУДОВИ І ОЦІНКА ЯКОСТІ

Послідовність називається псевдовипадковою, якщо вона виглядає, як безсистемна і випадкова, хоча насправді вона створювалась з допомогою суто детермінованого процесу, відомого під назвою псевдовипадкового генератора. Подібні генератори переважно задаються деяким початковим значенням і за допомогою певних алгоритмів отримують з нього випадкові послідовності. В цьому сенсі псевдовипадкові генератори можна розглядати як розповсюджувачі випадковості.

Комп'ютери є детермінованими машинами, що завжди роблять саме те на що вони запрограмовані і це усуває можливість звертатися до комп'ютерів як до джерела істинної випадковості. Саме краще, на що здатний комп'ютер, – це згенерувати псевдовипадкову послідовність, яка хоча і виглядає випадковою, але, насправді, такою не є [1].