УДК 537.531+537.87

Антясов И. С., Сафонов А. В., Соколов А. Н.

ПРОГРАММНО-ТЕХНИЧЕСКАЯ РЕАЛИЗАЦИЯ ТЕХНОЛОГИИ «МЯГКИЙ» ПЭМИН

В статье рассмотрена возможность программно-технической реализации технического канала утечки информации с использованием побочных электромагнитных излучений и наводок (ПЭМИН). Описана история возникновения понятия «мягкий» ПЭМИН. Рассмотрены способы применения ПЭМИН для перехвата информативного сигнала, технология скрытой передачи данных по каналу побочных электромагнитных излучений с помощью программных средств, а также возможности реализации этой технологии. Исследованы способы защиты информации от утечки по каналу с использование технологии «мягкий» ПЭМИН.

Ключевые слова: *технический канал утечки информации, побочные электромагнитные излучения и наводки (ПЭМИН), мягкий ПЭМИН, вирус.*

Antyasov I. S., Safonov A. V., Sokolov A. N.

SOFTWARE AND HARDWARE IMPLEMENTATION OF THE TECHNOLOGY OF SOFT TEMPEST

The article considers the possibility of software and technical implementation of technical channels of information leakage by using the electromagnetic radiation and interference (TEMPEST). Is described History of the appearance of the concept "soft" TEMPEST. The methods of application for the interception TEMPEST informative signal technology secure communication channel by electromagnetic radiation with the help of software, as well as the feasibility of this technology. Explore ways to protect information from leaking via the use of technology with a "soft" TEMPEST.

Keywords: *technical channel of information leakage, side electromagnetic emanations (TEMPEST), soft TEMPEST, virus.*

Термин побочные электромагнитные излучения и наводки (ПЭМИН) появился в конце 60-х - начале 70-х годов при разработке методов предотвращения утечки информации через различного рода демаскирующие и побочные излучения электронного оборудования. В Европе и Канаде для обозначения данного термина используется «compromising emanation» - компрометирующее излучение. Несмотря на то, что проявления ПЭМИН были замечены еще в XVIII веке, полномасштабные исследования начались во время Второй мировой войны, что было обусловлено, в первую очередь, желанием правительств стран-участниц сохранить втайне свою информацию и получить доступ к информации противников. Опасность ПЭМИН с точки зрения защиты информации впервые наглядно была продемонстрирована голландским инженером ВимванЭку, который в 1985 году опубли-

ковал статью «Электромагнитное излучение видеодисплейных модулей: Риск перехвата?». Статья была 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. Опыт был достаточно прост: в автомобиле, стоящем на улице, был установлен обычный телевизионный приемник с усовершенствованной антенной, на экране которого можно было наблюдать ту же самую картину, которую воспроизводил монитор компьютера в здании рядом с автомобилем. Эксперимент доказал, что перехват информации с монитора возможен с помощью незначительно доработанного обычного телевизионного приемника.

Под перехватом ПЭМИН понимают, как правило, перехват естественных излучений от технических средств (ТС). Однако процесс перехвата конфиденциальной информации путем приема паразитного излучения композитного сигнала монитора вполне реален, но процесс этот достаточно длителен - нужно дождаться, пока пользователь выведет на экран монитора интересующую конфиденциальную информацию. Это может занять дни или даже недели. Это вызвано особенностями проведения специальных исследований ТС [1]. Но также существует вероятность искусственного возникновения электромагнитных излучений, так называемого «мягкого ПЭМИН».

Проведенные Маркусом Куном в 1998 году экспериментальные исследования подтвердили, что существует другая возможность добывания конфиденциальной информации. Нужный компьютер «заражается» специальной программой-закладкой («троянский конь») любым из известных способов. 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 конфиденциальные 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.

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

Основная опасность технологии SoftTempest заключается в скрытности работы программы-вируса. Под этим следует понимать использование специальной программной закладки, которая бы посредством увеличения или уменьшения уровня ПЭМИН передавала бы закодированную защищаемую информацию посредством некой цифровой последовательности из нулей и единиц. Стоит оговориться, что мы будем в этом случае понимать под защищаемой информации не всю циркулирующую на ТС, а только конкретные защищаемые файлы. Для простоты можно предположить, что программная закладка для передачи 1 будет использовать увеличение сигнала, для передачи 0 уменьшение уровня излучений.

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 побочные излучения электронного оборудования для передачи данных, могут работать годами, не обнаруживая себя.

В настоящее время технология SoftTempest включает в себя не только способы разведки, но и программные способы противодействия разведке, в частности использование специальных TEMPEST - шрифтов, минимизирующих высокочастотные излучения. [2]

Данный канал утечки информации является программно-техническим, т.е. используется программная закладка для передачи защищаемой информации по техническому каналу утечки через ПЭМИН.

Необходимо заметить, что уровень излучений ПЭМИН достаточно сложно детектиро-

вать, для этого применяются специальные альтернативные измерительные площадки, в которых уровень фоновых помех сводится к минимуму. [3] Выгодная особенность для злоумышленника от естественных ПЭМИН заключается в следующем. При обычном ПЭМИНе вероятный противник перехватывает большой поток информации, малая доля которого представляет интерес, например при перехвате ПЭМИН монитора интерес представляет прежде всего не само изображение экрана, а именно текстовая информация, имеющая конфиденциальный характер. При использовании же мягкого ПЭМИНа противник получает информацию, представляющую непосредственный интерес. Так же позволяет использовать наиболее мощный источник излучения, тем самым увеличивая полезный сигнал. Например отправляя его с флешкарты подключенной через USB на VGA интерфейс видеокарты.

Практически реализовать данный канал можно, используя обычные и широко распространенные тест-программы для оценки канала ПЭМИН. Известно, что как правило наиболее сильный уровень ПЭМИН дает монитор, но для передачи по данному каналу информации, нам необходимо будет менять изображение, выводимое на экран, что будет заметно для пользователя, что неприемлемо. Стоит оговориться, что исключение составляет ситуация, когда видеокарта имеет два параллельных выхода - тогда возможно изменять уровень излучения на втором выходе, тем самым оставаясь незамеченными. Однако, используя более сложные алгоритмы передачи, например изменение яркости в некоторых точках монитора, возможно успешно передавать информацию на заранее известных частотах [4].

Также возможно осуществить передачу информации по ПЭМИН через SATA интерфейс, данный способ вряд ли будет замечен пользователем. Для демонстрации уровней излучений, используем настольный ПК с жестким диском Seagate Desktop SSHD подключенный через SATA интерфейс. Для перехвата используется спектроанализатор Agilent NS30A, полностью синтезированный анализатор спектра с диапазоном частот от 1 кГц до 3 ГГц, фильтры полос пропускания от 10 Гц до 3 МГц, диапазон входных уровней –110…30 дБм Вт, режим приемника сигналов с ЧМ и АМ демодуляторами, наличие автоматических и маркерных измерений, режим частотомера, автоматическая и ручная калибровка, и антенна АИ5-0 размещенной на высоте 1 м и расстоянии 1 м от системного блока исследуемого компьютера. Программное обеспечение, используемое для формирования тест-сигналов, это ПО Sigurd-test, которое генерирует меандры на тестируемый канал, в данном случае SATA интерфейс. Аналогично тестируются и остальные каналы.

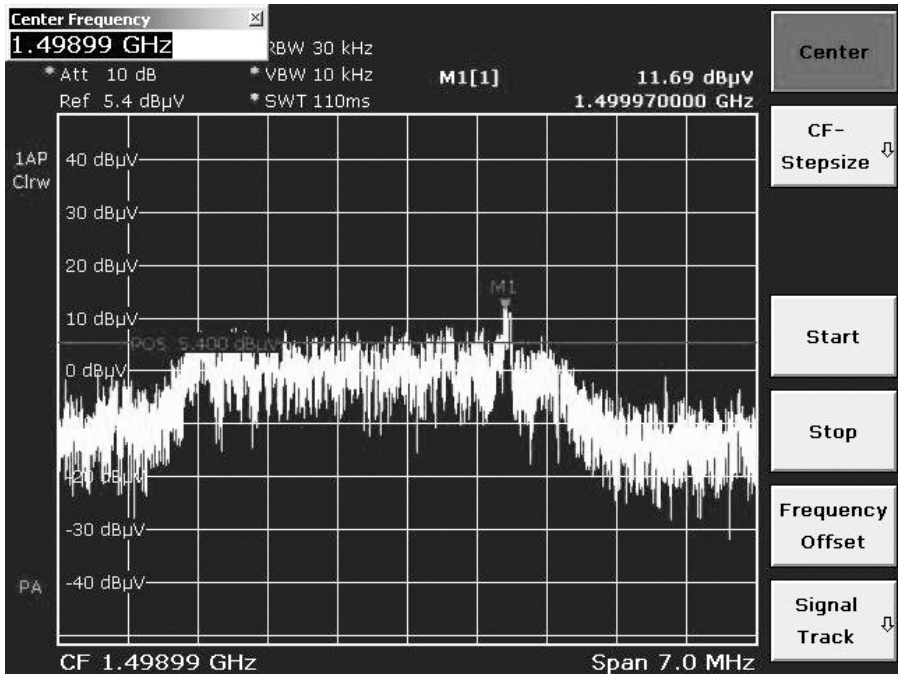

Рис. 1. Сигнал от SATA интерфейса

Частота рассматриваемого сигнала составляет 1500 МГц, ширина сигнала порядка 5 МГц (рис. 1). Без учета калибровочных характеристик антенн измеренные значения составили при включенной тест-программе с передачей единиц - уровень излучений 15дБ (мкВ/м), данный режим будет использован для передачи единицы. Также рассматривалась спектрограмма при выключенной тест-программе - уровень излучений 13дБ (мкВ/м), в этом случае не передается никакой информации. Стоит заметить, что уровни сигналов подлежат пересчету, так как ширина сигнал значительно шире полосы частот фильтра. Вероятному противнику необходимо знать данные уровня для правильной идентификации передаваемой информации.

Необходимо отметить, что уровни отличаются незначительно и частоты около 1500 МГц, на которых происходят излучения от SATA интерфейса, не оптимальны для передач данных – электромагнитная волна быстро затухает. Данный фактор играет против злоумышленника, но при грамотной настройке перехватывающей аппаратуры и последующей цифровой обработке сигнала возможен такой перехват со значительных расстояний.

Говоря о способах защиты важно заметить, что выявление данной угрозы довольно затруднительно, так как изменение работы ТС будет вряд ли замечено пользователем. Поэтому способы защиты от утечки информации по данному каналу остаются такими же, как и для обычных ПЭМИН - генераторы шума и экранирование. Так же возможно устранение таких программ посредством антивирусов, при создании соответствующих сигнатур угроз.

Разработка, применение программного обеспечения использующего ПЭМИН в качестве канала передачи информации, является актуальной и опасной угрозой безопасности информации, так как на данный момент не существует систем защиты контролирующих утечку за счет мягкого ПЭМИН.

Примечания

1. ГОСТ Р 51583 – 2000. Порядок создания автоматизированных систем в защищенном исполнении. – Введ. 2000-06-04. – М.: Госстандарт России, 2000. – 12 с.

2. TEMPEST [Электронный ресурс] //Материал из Википедии — свободной энциклопедии. – URL: https://ru.wikipedia.org/wiki/TEMPEST (дата обращения: 01.09.2015)

3. Антясов И.С., Соколов А.Н. Использование сетчатых материалов при экранировании альтернативной измерительной площадки для проведения специальных исследований технических средств // Безопасность информационного пространства: сборник трудов XIII Всероссийской научно-практической конференции студентов, аспирантов и молодых учёных. – Челябинск: Издательский центр ЮУрГУ, 2015. – С. 8 – 13.

4. Markus Kuhn and Ross Anderson, Soft TEMPEST: Hidden Data Transmission Using Electromagnetic Emanations [Электронный ресурс] // David Aucsmith (Ed.): Information Hiding 1998, LNCS 1525, pp. 124–142, 1998, Springer-Verlag, 1998. – URL: http://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf (дата обращения: 01.09.2015)

Соколов Александр Николаевич, к. т. н., доцент, зав. кафедрой безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет», г. Челябинск. E-mail: ANSokolov@inbox.ru

Антясов Иван Сергеевич, аспирант кафедры безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет», г. Челябинск. E-mail: antyasov@gmail.com

Сафонов Александр Владимирович, студент кафедры безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет).

Alexander Sokolov, a. M. N., Associate Professor, Head. the Department of Information Systems Security "South Ural State University", Chelyabinsk. E-mail: ANSokolov@inbox.ru

Antyasov Ivan, postgraduate Department of Information Systems Security "South Ural State University", Chelyabinsk. E-mail: antyasov@gmail.com

Alexander Safonov, students of the department of information systems security «South Ural State University» (National Research University).