

УДК 004.2

УТЕЧКА ИНФОРМАЦИИ ПО КАНАЛАМ ПЭМИ И СПОСОБЫ ИХ ЗАЩИТЫ

Киреева Н.В., Семенов А.В.

ФГБОУ ВПО «Поволжский государственный университет телекоммуникаций и информатики»,
Самара, e-mail: semenovaleksey93@gmail.com

Исследование съема информации по каналам ПЭМИ и разработка средств защиты, является востребованной областью с сфере защиты информации от утечки по техническим каналам. Понимание того, что от какого технического средства конкретно ПЭМИ несет в себе большую угрозу безопасности информации, дает нам возможность наиболее полно оценить возможный ущерб. Произведен анализ каналов утечки информации по ПЭМИ с расположением технического средства разведки относительно контролируемой зоны. Приведен пример реализации на практике перехвата информации по каналам ПЭМИ. А так же произведена классификация средств защиты от утечки информации по побочному электромагнитному излучению.

Ключевые слова: ПЭМИ, технические средства, ТСПИ, опасная зона, контролируемая зона, активные и пассивные меры защиты

LEAKAGE OF INFORMATION THROUGH CHANNELS COMPROMISING EMANATIONS AND METHODS OF PROTECTION

Kireeva N.V., Semenov A.V.

*Povolzhskiy State University of Telecommunications and Informatics, Samara,
e-mail: semenovaleksey93@gmail.com*

Research on removal of compromising emanations channels and the development of means of protection of information is a popular area with the protection of information against leakage through technical channels. Understanding what some of the specific technical means compromising emanations carries a great threat to the security of information, gives us an opportunity to more fully assess the potential damage. The analysis of information leakage channels compromising emanations with the location of the technical means of intelligence with respect to the controlled area. An example of practicing the interception of information through compromising emanations. As well as a classification of protection against leakage of information on stray electromagnetic radiation.

Keywords: Compromising emanations, hardware, TSPI, dangerous zone, controlled area, active and passive protection measures

Сегодня информация, обрабатываемая в технических средствах (ТС) представляет наибольшую ценность, так как она более проста в обработке. При обработке информации ТС возникает побочное электромагнитное излучение (ПЭМИ), перехватив которое становится возможным раскрытие обрабатываемой информации без прямого доступа к устройству пользователя.

Термин ПЭМИ (побочное электромагнитное излучение) появился при разработке методов предотвращения утечки информации через различного рода демаскирующие и побочные излучения электронного оборудования.

Впервые теория ПЭМИН (побочное электромагнитное излучение и наводки) была применена в начале 20-го века 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 сред-

ства радио- и радиотехнической разведки стали неперенным реквизитом шпионов различного уровня. По мере развития технологии развивались как средства ПЭМИН-нападения (разведки), так и средства ПЭМИН-защиты.

Виды каналов утечки информации по ПЭМИ

Утечка информации через ПЭМИН возможна по электромагнитным и электрическим каналам. К электромагнитным относятся каналы утечки информации, возникающие за счет различного вида побочных электромагнитных излучений (ЭМИ) технических средств передачи информации (ТСПИ):

- излучений элементов ТСПИ;
- излучений на частотах работы высокочастотных (ВЧ) генераторов ТСПИ;
- излучений на частотах самовозбуждения усилителей низкой частоты (УНЧ) ТСПИ.

Схема технического канала утечки информации ТКУИ показана на рис. 1.

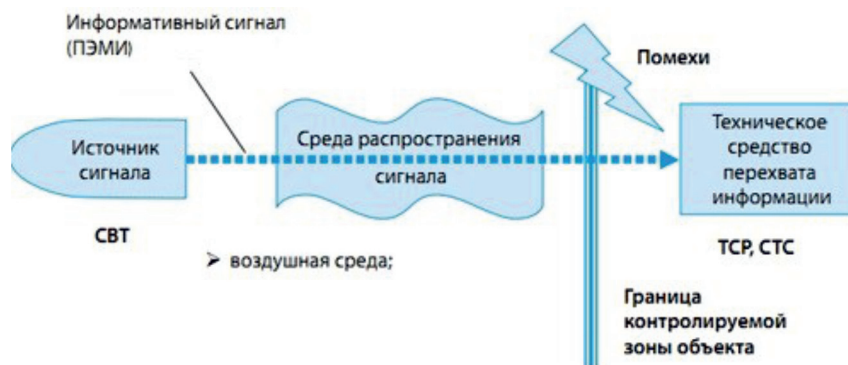


Рис. 1. Схема технического канала утечки информации

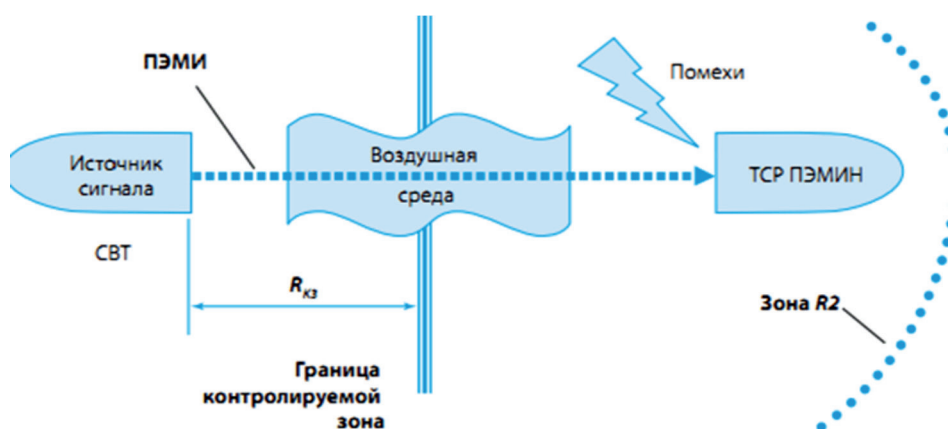


Рис. 2. Схема расположения ТСР ПЭМИН в пределах опасной зоны

В ТСПИ носителем информации является электрический ток, параметры которого (сила тока, напряжение, частота и фаза) изменяются по закону информационного сигнала. При прохождении электрического тока по токоведущим элементам ТСПИ вокруг них (в окружающем пространстве) возникает электрическое и магнитное поле. В силу этого элементы ТСПИ можно рассматривать как излучатели электромагнитного поля.

В состав ТС могут входить различного рода высокочастотные генераторы. К таким устройствам можно отнести: задающие генераторы, генераторы тактовой частоты, генераторы радиоприемных и телевизионных устройств, генераторы измерительных приборов и т.д. В результате внешних воздействий информационного сигнала (например, электромагнитных колебаний) на элементах ВЧ-генераторов наводятся электрические сигналы. Приемником магнитного поля могут быть катушки индуктивности колебательных контуров, дроссели в цепях электропитания и т.д.

Приемником электрического поля являются провода высокочастотных цепей и другие элементы. Наведенные электрические сигналы могут вызвать непреднамеренную модуляцию собственных ВЧ-колебаний генераторов. Эти промодулированные ВЧ-колебания излучаются в окружающее пространство.

Самовозбуждение усилителей низкой частоты ТСПИ (например, систем звукоусиления и звукового сопровождения, магнитофонов, систем громкоговорящей связи и т.п.) возможно за счет случайных преобразований отрицательных обратных связей (индуктивных или емкостных) в паразитные положительные, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов

Перехват ПЭМИ

Перехват побочных электромагнитных излучений ТСПИ осуществляется средствами радио-, радиотехнической разведки, размещенными вне охраняемого пространства.

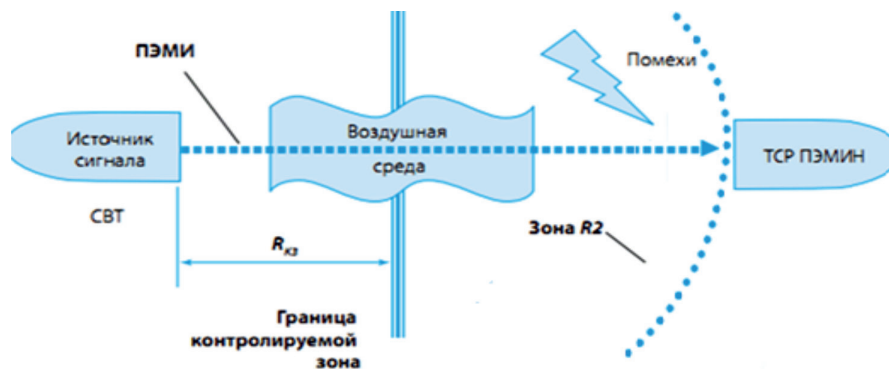


Рис. 3. Схема расположения ТСП ПЭМИН за пределами опасной зоны



Рис. 4. Устройство PKI2715



Рис. 5. Антенна R&S®HL007A2

Рассмотрим два случая излучения ПЭМИ:
1) пусть техническое средство разведки (ТСП) ПЭМИ находится за границами контролируемой зоны, но в пределах опасной зоны (рис. 2).

2) пусть ТСП ПЭМИ находится за границами контролируемой зоны и за пределами опасной зоны, что гарантирует невозможность съема информации за счет побочного электромагнитного излучения от средства вычислительной техники, так как ТСП ПЭМИ находится вне зоны распространения информативного сигнала (рис. 3).

Зона, в которой возможен перехват (с помощью разведывательного приемника) ПЭМИ и последующая расшифровка содержащейся в них информации, называется опасной зоной 2. Это зона, в пределах которой отношение «информационный сигнал/помеха» превышает допустимое нормированное значение. Пространство вокруг ТСПИ, в пределах которого на случайных антеннах наводится информационный сигнал выше допустимого (нормированного) уровня, называется опасной зоной 1.

Перехват ПЭМИ имеет смысл, при следующих режимах обработки информации технических средств (ТС):

- вывод информации на экран монитора;

- ввод данных с клавиатуры;
- запись информации на накопители;
- чтение информации на накопители;
- передача данных в каналы связи;
- вывод данных на периферийные печатные устройства-принтеры, плоттеры, запись данных от сканера на магнитный носитель.

Перехват информации по каналам ПЭМИ от компьютерной мыши входящей в состав СВТ, не имеет смысла, так как импульсы от нажатия клавиши не несут в себе никакого информативного сигнала, а по координатам курсора на экране монитора осуществить перехват защищаемой информации почти невозможно.

Пример состава комплекса, предназначенного для осуществления разведки ПЭМИ:

а) специальное приёмное устройство PKI2715 (дальность перехвата ПЭМИ от 10 до 50 м) (рис. 4);

б) логопериодическая антенна с перекрестными элементами R&S®HL007A2 (диапазон частот от 80 МГц до 1,3 ГГц, коэффициент усиления 5-7 дБ) (рис. 5).

Разведка ПЭМИ на практике

Для перехвата ПЭМИ достаточно приемной антенны, анализатора спектра, устройства цифровой обработки сигналов и ТС.

№ п/п	Наименование	Рабочий диапазон частот, (МГц)
1	Антенна дипольная активная «АИ5-0»	0,009...2000
2	Анализатор спектра Rohde & Schwarz «FSL3»	0,009...3000
3	Устройство «Вензель»	-
4	Ноутбук	-
5	ПАК «НАВИГАТОР»	-



Рис. 6. Изображение с ПАК «Навигатор», на котором приведен список частот выделенных программой

№	Частота, МГц	Ес+п дБмВ/м	Еп дБмВ/м	Ес дБмВ/м	Интервал расчета, МГц	Номер гармоники от Ft
1	0074.290000	50.93	35.14	53.61	0.010000 - 241.400000	0.6155 от Ft
2	0172.000000	47.46	38.05	50.02	0.010000 - 241.400000	1.4250 от Ft
3	0936.700000	60.10	49.23	62.71	724.200000 - 965.600000	7.7606 от Ft
4	0938.200000	59.13	41.82	61.82	724.200000 - 965.600000	7.7730 от Ft
5	0938.400000	61.26	45.29	63.94	724.200000 - 965.600000	7.7746 от Ft
6	0944.600000	60.31	51.29	62.86	724.200000 - 965.600000	7.8260 от Ft

Рис. 7. Список выделенных частот после анализа найденных гармоник

Для эксперимента было выбрано оборудование, указанное в таблице.

Побочное электромагнитное излучение, которое образуется в результате вывода информации на экран монитора, принимается антенной и, после усиления, передается в анализатор спектра.

На рис. 6 приведена панорама частот при выводе информации на экран от СВТ, где выделены гармоники, на которых может присутствовать информативный сигнал.

После анализа найденных частот, были выделены частоты, где есть информативный сигнал, которые показаны на рис. 7.

Это дает возможность увидеть осциллограмму и спектр принимаемого сигнала.

Затем, промодулированный информативным сигналом на промежуточной частоте, полученный сигнал поступает в модуль цифровой обработки сигналов (рис. 8).

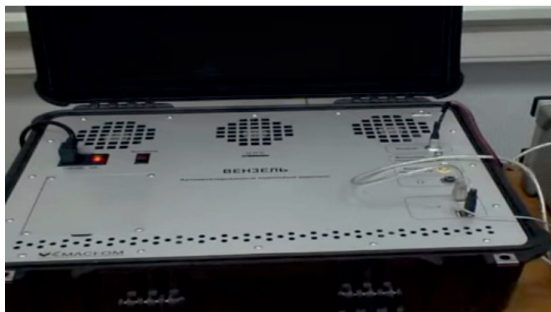


Рис. 8. Модуль цифровой обработки сигналов

После обработки и преобразования видеосигнал поступает на ТС (в данном случае использовался ноутбук). На мониторе отображается информация, полностью идентичная информации на исходном компьютере. Пример исходного и перехваченного изображений показаны на рис. 9, 10.

Выводы

В лабораторных условиях приемная антенна находилась непосредственно вблизи монитора, однако изменив конфигурацию оборудования возможно снятие информации до 100 м, несмотря на препятствия вроде стен и прочих ограждающих конструкций.

Меры защиты информации от утечки по каналам ПЭМИ. Активный и пассивный методы

На сегодняшний день наиболее известными методами защиты информации от утечки по ПЭМИ являются, такие методы как:

1. *Активный метод.* Заключается в применении специальных широкопо-

лосных передатчиков помех. Метод хорош тем, что устраняется не только угроза утечки информации по каналам побочного излучения компьютера, но и многие другие угрозы. Как правило, становится невозможным также и применение закладных подслушивающих устройств. Становится невозможной разведка с использованием излучения всех других устройств, расположенных в защищаемом помещении.

В качестве недостатков можно выделить:

- вредность достаточно мощного источника излучения для здоровья;
- наличие маскирующего излучения свидетельствует, что в данном помещении есть защищаемые секреты, что само по себе привлекает к этому помещению повышенный интерес злоумышленников;
- при определенных условиях метод не обеспечивает гарантированную защиту компьютерной информации.

На рис. 11 и 12 показаны генераторы создания помех.

Устройство «Соната-Р2» является техническим средством защиты информации от утечки информации, за счет побочных электромагнитных излучений и наводок. Устройство соответствует требованиям «Норм защиты информации, обрабатываемой средствами вычислительной техники и в автоматизированных системах, от утечки за счет побочных электромагнитных излучений» (рис. 11).

Устройство «генератор шума ГШ-К-1000М» (рис. 12), предназначено для защиты от утечки информации за счет побочных электромагнитных излучений и наводок средств офисной техники на объектах 2 и 3 категорий секретности. Отличительные особенности: использование рамочной антенны для создания пространственного зашумления; установка в свободный слот персонального компьютера; выпускаются для слотов PCI и ISA.

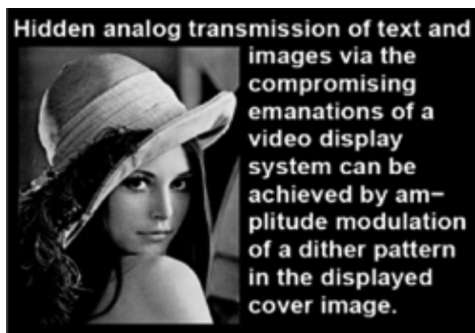


Рис. 9. Исходное изображение



Рис. 10. Перехваченное изображение



Рис. 11. Устройство защиты объектов информатизации от утечки информации за счет ПЭМИН «Соната-P2»

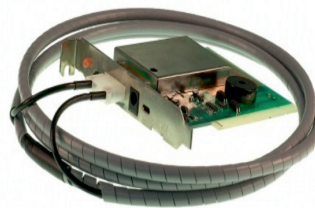


Рис. 12. Генератор шума ГШ-К-1000М

2. *Пассивный метод.* Заключается в экранировании источника излучения технического средства, то есть СВТ размещается в экранированном шкафу или в экранированном помещении целиком. То есть экранируется каждое ТС входящее в состав нашего СВТ. В качестве недостатка такого метода можно выделить высокую стоимость экранированного помещения, если речь идет о нескольких СВТ.

Для экранирования источника излучения применяются современные технологии, которые основаны на нанесении (например, напылении) различных специальных материалов на внутреннюю поверхность существующего корпуса, поэтому внешний вид компьютера практически не изменяется.

Экранирование компьютера, даже с применением современных технологий, сложный процесс. Поэтому реально доработка компьютера осуществляется в несколько этапов:

1) вначале осуществляются специальные работы для собранного компьютера, где определяются частоты, их уровни, на которых присутствует информативный сигнал;

2) далее идут этапы анализа конструктивного исполнения компьютера, разработки технических требований, выбора методов защиты, разработки технологических решений и разработки конструкторской документации для данного конкретного изделия (или партии однотипных изделий);

3) после прохождения первых двух этапов, изделие поступает собственно в производство, где и выполняются работы по защите всех элементов компьютера;

4) после этого, в обязательном порядке, проводятся специспытания, позволяю-

щие подтвердить эффективность принятых решений. Если специспытания прошли успешно, заказчику выдается документ, подтверждающий, что компьютер защищен от утечки информации по каналам ПЭМИ.

Выводы

Разобранный пример наглядно демонстрирует, что с помощью лабораторного оборудования имеющего относительно небольшую стоимость, возможен съем информации через побочное электромагнитное излучение с отображением перехваченных данных на приемном устройстве.

На основании вышеизложенного очевидно, что разрабатываемые средства защиты от утечки по каналам ПЭМИ, являются необходимыми для обеспечения безопасности информации.

Практика показывает, что выполнение работ по изготовлению таких средств защиты информации и реализация данных конструкторско-технологических решений, удовлетворяет техническим требованиям и нормативной документации по предотвращению утечки информации применяемых технических средств.

Список литературы

1. Хорев А.А. Техническая защита информации. Том 1 – НПЦ «Аналитика», 2008. – 436 с.
2. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учебное издание. – 280 с.
3. Рембовский А.М., Ашихмин А.В., Козьмин В.А. Радиомониторинг: задачи, методы, средства. 2-е изд., перераб. и доп., 2010. – 680 с.
4. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В., Солдатов А.А. Технические средства и методы защиты информации. 4-е изд., испр. и доп., 2010. – 616 с.