# Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА – Российский технологический университет»**

Кафедра КБ-1 «Защита информации»

**Дисциплина:** «Технические средства контроля эффективности мер защиты информации»

# Отчет по практической работе № 6

**Тема:** Методика контроля эффективности мер защиты информации от утечки по каналу ПЭМИН

# Вариант 2

**Выполнили:**

Студенты 3 курса,

группы БББО-05-20 Муханов М.Э.

Кутьин З.С.

Романько М.И.

Акмурзаев И.М.

Крутов А.М.

# Проверил:

Жиряков В.Д.

# Ход работы

Дано*:* Линия, проходящая непосредственно в месте размещения СВТ, играет роль случайной антенны. Линия выходит за пределы КЗ.

Требуется рассчитать:

— напряженность поля информативного сигнала на границе КЗ

— ОСШ на границе КЗ

— напряжение ПЭМИН, наводимое в случайной антенне

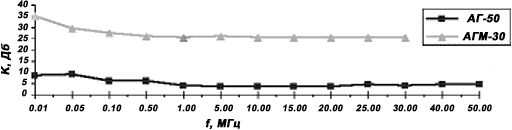
— напряжение ПЭМИН в линии на границе КЗ

|  |  |
| --- | --- |
| **Величина** | **Значение** |
| Частота информативного сигнала, F [МГц] | 4,9 |
| Калибровочный коэффициент антенны, KА [1/м] | 1,78 |
| Калибровочный коэффициент пробника |  |
| Нормированное отношение сигнал/шум, qн | 0,3 |
| Удаление изм. антенны от корпуса ТС, R [м] | 0,7 |
| Минимальное удаление границы КЗ от корпуса ТС, Ri [м] | 15 |
| Спектр. плотность норм. шума для стационарных TCР [мкВ/м×кГц0,5] | 0,025 |
| Спектр. плотность норм. шума для возимых TCР [мкВ/м×кГц0,5] | 0,025 |
| Спектр. плотность норм. шума для носимых TCР [мкВ/м×кГц0,5] | 0,025 |
| Коэффициент затухания электромагнитного поля, КЗ |  |
| Напряжение сигнал+шум рядом с СВТ, UС+Ш [дБмкВ] | 17 |
| Напряжение шума рядом с СВТ, UШ [дБмкВ] | -5 |

**Шаг 1***.* Расчёт частоты информативного сигнала:

*F* = 𝐻 ∗ 𝐿 ∗ 𝐹кадр ∗ 1,36/2 = 750 ∗ 300 ∗ 60 ∗ 1,36/2 = 9,18 МГц

**Шаг 2***.* Калибровочный коэффициент антенны находится по графику:



**Шаг 3***.* Измерение напряженности поля информативного сигнала:

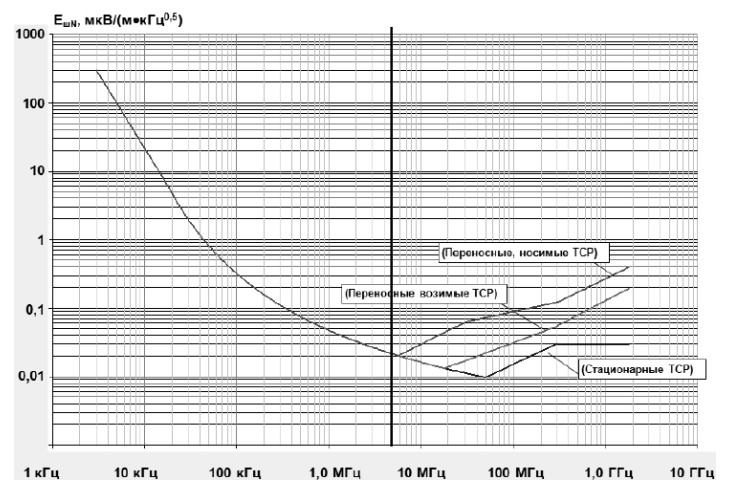
**Шаг 4***.* Расчет ослабления сигнала на трассе распространения от СВТ до границы КЗ:

* расстояние от измерительной антенны до ТС удовлетворяет условию R < λ/2π
* расстояние от границы КЗ до корпуса ТС удовлетворяет условию λ/2π < D <

*Kз=*λ*D2/*2π*R3*

**Шаг 5***.* Расчет напряженности поля информативного сигнала на границе КЗ:

**Шаг 6***.* Определение спектральной плотности нормированного шума для стационарных, возимых и носимых TCР по графику:

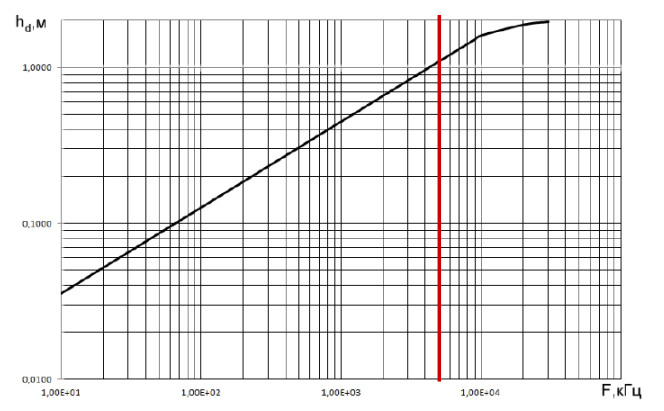


**Шаг 7***.* Определение нормированного уровня напряженности поля помех:

𝐸ш.𝑛𝑗[мкВ/м] ≈ 𝐸ш𝑁𝑗[мкВ⁄м ∗ кГц0,5] ∗∆𝐹0,5[кГц] = 0,02 \* 5000 ≈ 100 мкВ/м

**Шаг 8.**Расчет ОСШ на границе КЗ:

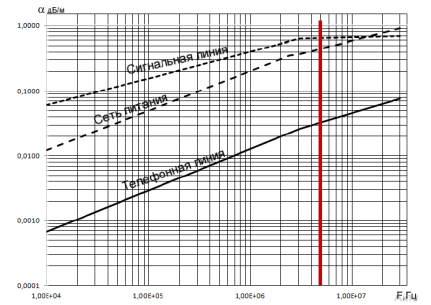
**Шаг 9.**Оценка действующей длины линии hd, как случайной антенны, на основной тактовой частоте:



ℎд ≈ 1,05 м

**Шаг 10.** Измерение напряжения ПЭМИН в линии возле СВТ

**Шаг 11.** Измерение затухания в сети питания на основной такт. частоте:

****

𝛼 ≈ 0,45 дБ/м

**Шаг 12.** Измерение напряжения ПЭМИН в линии на границе КЗ:

**Вывод:** На границе контролируемой зоны напряженность поля информативного сигнала составляет . Отношение «сигнал/шум» на границе КЗ равно , что меньше 0,3. Напряжение побочных электромагнитных наводок составляет:

* возле СВТ:
* на границе КЗ:

**Ответы на контрольные вопросы.**

**1. Причины возникновения ТКУИ за счет ПЭМИ.**

Вокруг проводника, по которому протекает электрический ток возникает электромагнитное поле (ЭМП). Если по данному проводнику передается какой-либо сигнал, то, следовательно, и электромагнитное поле тоже будет изменяться по тем же законам, что и сигнал, протекающий в линии. Если вспомнить, что в проводнике, помещенном в электромагнитное поле, возникает электрический ток, то очевидно, что могут возникать наводки ПЭМИ на любые токоведущие элементы, в том числе и любые линии и ТС, подключенные к ним, попадающие под действие данного электромагнитного поля. Перехват этой информации можно осуществить путем анализа изменений параметров ПЭМИН с помощью специальных высокочувствительных радиоприемных устройств, оснащенных специализированными антеннами, пробниками напряжения, токосъемниками.

**2. Случайные антенны.**

Случайные антенны могут быть сосредоточенными и распределенными.

Сосредоточенная случайная антенна представляет собой компактное техническое средство (например, телефонный аппарат, громкоговоритель радиотрансляционной сети, датчик пожарной сигнализации и т. д.), подключенное к линии, выходящей за пределы контролируемой зоны.

К распределенным случайным антеннам относятся случайные антенны с распределенными параметрами: кабели, провода, металлические трубы и другие токопроводящие коммуникации, выходящие за пределы контролируемой зоны. Уровень наводимых в них сигналов в значительной степени зависит не только от мощности излучаемых сигналов, но и от расстояния от линий ТСОИ до линий ВТСС или посторонних проводников, а также длины их совместного пробега.

**3. Источники сигналов ПЭМИ (информативные и неинформативные).**

Выделяют два вида сигналов ПЭМИ: информативные и неинформативные.

К неинформативным источникам ПЭМИ относятся все те устройства, интерфейсы и линии, которые никак не связаны с обработкой, хранением и передачей конфиденциальной информации. Например, излучение от блока питания системного блока или монитора. Также не относится к информативным излучение от интерфейсов подключения манипулятора «мышь»

К информативным источникам относятся:

— клавиатура (интерфейсы USB или PS/2);

— видеотракт (монитор, кабели, видеоадаптер, KVM коммутатор);

— D-SUB (VGA) или DVI, а также внутренние интерфейсы формирования изображения на экране монитора (LVDS);

— HDD/SSD (SATA, интерфейс IDE не рассматривается из-за его большой разрядности, также он уже практически не встречается);

— USB накопители

— FDD приводы;

— Оптические приводы (только с SATA интерфейсом);

— Периферийные устройства

— Сетевое оборудование

**4. Контрольно-измерительное оборудование (антенны)**

В полосе частот от 200 Гц до 30 МГц в комплект антенн должны входить магнитная и (или) электрическая антенны

Для измерения магнитной составляющей электромагнитного поля, антенна должна быть: электрически экранированной рамочной антенной, имеющей такие размеры, чтобы ее рамка помещалась в квадрат со стороной не более 0,6м, или ферритовая антенна длиной не более 0,5 м.

Конструкция антенн (антенного штатива) должна обеспечивать возможность плавного изменения высоты расположения антенны над землей от 0,8 м до 1,25 м, а также возможность поворота магнитной и электрической антенн на 360° вокруг оси

В полосе частот от 30 до 1000 МГц в комплект антенн должны входить одна или несколько электрических антенн одного из следующих типов:

а) линейный симметричный вибратор на полосу частот от 30 до 80 МГц

б) биконическая антенна, максимальный размер которой должен быть не более 1,35 м в полосе частот от 30 до 300 МГц и с КСВН не более 3,0, и биконическая антенна, максимальный размер которой – не более 0,5м в полосе частот от 300 до 1000 МГц с КСВН не более 2,5;

в) широкополосная антенна, главный лепесток диаграммы направленности которой должен быть таким, чтобы в направлении непосредственного излучения от источника ПЭМИН и в направлении отраженного от земли луча разность коэффициентов усиления антенны не превышала бы 1дБ, с КСВН не более 2,5.

**5. Контрольно-измерительное оборудование (анализаторы)**

Особенность анализаторов в том, что на входе не фильтр перестраивается относительно сигнала, что вызывает существенные проблемы в создании перестраиваемого фильтра с неизменной характеристикой, а сигнал сдвигается относительно фильтра ПЧ путем смешивания с сигналом гетеродина.

**6. Принцип работы анализатора спектра**

Принцип действия анализатора спектра очень схож с работой супергетеродинного приемника. Входной сигнал проходит через аттенюатор, а затем через фильтр нижних частот (позже фильтр для подавления помехи по зеркальному каналу) на смеситель, где он смешивается с сигналом от гетеродина. В результате перемножения двух гармонических сигналов с разными частотами на выходе получатся два сигнала с частотами, соответствующими сумме и разности частот входных сигналов

**7. Программно-аппаратные комплексы**

На рынке представлены программно-аппаратные комплексы следующих производителей, распространителей: «Навигатор ПxГ» – «НЕЛК», «СигурдМx» – «МАСКОМ», «Легенда» – «АВМ-СИСТЕМС». Все комплексы должны иметь сертификаты ФСТЭК России и метрологический сертификат соответствия на измерительное оборудование

**8. Измеряемые физические величины**

В процессе проведения оценки защищенности ОТСС от утечки по каналам ПЭМИН необходимо производить измерения следующих физических величин:

— напряженность электромагнитного поля по электрической составляющей (*E, В/м*);

— напряженность магнитного поля (*H, А/м*);

— напряжение в линиях и токоведущих конструкциях (*U, В*).

**9. ПЭМИ видеотракта**

Одним из основных и, зачастую, самых мощных источников сигналов ПЭМИ является видеотракт. Сигнал, который нас интересует, это сигнал интерфейса передачи видеосигнала, но и все устройства видеотракта, включающие видеоконтроллер, соединительные кабели, KVM коммутаторы и конечные устройства отображения существенно влияют на уровень сигнала и направление его излучения, потому как выступают в качестве антенн.

**10. ПЭМИ USB интерфейса**

Опасными режимами работы USB-флеш-накопителя с точки зрения утечки информации – является момент записи/чтения. Чтобы отличить при исследовании ПЭМИ сигнал, излучаемый флеш-накопителем от постороннего, необходимо сформировать специальный тестовый сигнал. Тестовый сигнал должен представлять из себя непрерывную (за время измерения) последовательность импульсов тока (напряжения) в исследуемом тракте с постоянными известными периодом и длительностью импульсов. Такой сигнал обладает линейчатым спектром с известными параметрами

**11. ПЭМИ SATA интерфейса**

Особенности интерфейса SATA в том, что в нем до передачи информации по линии подключения предусмотрен ряд серьезных методов логического кодирования и преобразования для оптимизации пакета передаваемых данных и увеличения скорости передачи информации. Таким образом, на данный момент, практически невозможно задать такой тестовый режим (записи/чтения файла определенного содержания), чтобы выполнялось однозначное условия максимальной и постоянной частоты следования импульсов в канале

В результате, чаще всего HDD SATA обнаруживаются исключительно опытным путем. Сигналы возникают на частотах 1,5 и 3 ГГц с достаточно широкой полосой в 50-80 МГц. В таком случае рекомендуется применять описанный ранее подход для измерения энергии широкополосных сигналов ПЭМИ

**12. ПЭМИ клавиатуры PS/2**

Во всем многообразии клавиш нашлась и такая, которая удовлетворяет условиям формирования тестового сигнала для анализа ПЭМИ. При нажатии клавиши «+=», команда, передающаяся через интерфейс PS/2 представляет из себя последовательность импульсов, в которых длительность импульса равна длительности пауз между импульсами (такая последовательность называется «меандр»).

Частота следования импульсов порядка 6…7 кГц, но сигнал достаточно слабый и находится в области низких частот, в которой уровнифонового шума значительно выше, что затрудняет поиск и измерениесигналов ПЭМИ. В ряде случаев, на практике удавалось обнаружитьсигнал ПЭМИ от клавиатуры в эфире только на очень близком расстоянии, при проведении измерений на расстоянии 1 м в большинствеслучаев сигнал не удавалось выделить на уровне фонового шума. Втаких случаях рекомендуется производить так называемый расчет радиусов «по шумам».

**13. Средства защиты информации**

Во избежание утечки информации используются средства защиты информации, которые увеличивают отношение «сигнал/шум», увеличивая затухание информативного сигнала или смешивая его с шумом

**14. Средства пассивной защиты**

К пассивным техническим способам защиты относят:

— установка комплексных систем защиты от несанкционированнного доступа (НСД) на ТСПИ и кабельные линии связи

—экранирование ВП, ТСПИ и отходящих от них соединительных линий

**15. Порядок проведения измерений при оценке ПЭМИН**

— Производится составление перечня источников сигналов ПЭМИ в составе АС

— Производится поиск частот сигналов ПЭМИ

— После определения частот сигналов ПЭМИ производятся измерения уровней напряженности электромагнитного поля по электрической и по магнитной составляющим в соответствующих диапазонах

— Производится осмотр помещения, в котором располагается ОТСС с целью выявления проводных линий и токоведущих коммуникаций, выходящих за пределы КЗ.

— В линиях, выходящих за КЗ необходимо произвести поиск и оценку защищенности по каналу, возникающему за счет наводок побочных электромагнитных излучений (ПЭМИН).

— Поиск и измерение сигналов в линиях осуществляется путем непосредственного подключения пробника напряжения к исследуемой линии

— На выявленных частотах в соответствующих линиях производятся измерения напряжения шума и смеси сигнала + шум, аналогично измерению сигналов ПЭМИ

— Оформляется протокол оценки защищенности ОТСС от утечки за счет побочных электромагнитных излучений и наводок