2.1 Тестовый режим

Для проведения исследований технических средств, необходимо применять «тестовые программы», генерирующие тестовый (исследуемый) сигнал. Тестовый сигнал должен моделировать ситуацию, в которой становится возможен перехват ПЭМИН.

Согласно Положению «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3 марта 2012 г. N 171» тестовые программы должны обеспечивать формирование в соответствии с ГОСТ 29339 тестовых режимов работы средств вычислительной техники следующих стандартов интерфейсов технических средств: VGA, DVI, HDMI, USB, SATA, Ethernet, PS/2

Основные требования, предъявляемые к сигналу: тестовый сигнал должен быть непрерывным, иметь периодическую структуру и обладать максимально возможными частотой повторения и уровнем излучения. Данный набор требований гарантирует генерацию стабильного излучения в окружающую среду, подробнее с требованиями можно ознакомиться в конце раздела.

Комплексные решения применяемых средств измерения, используемых при исследованиях ПЭМИН, как правило, обладают возможностью включить тестовый режим.

В настоящее время сертификаты имеют комплексы «Зарница-П» («Элерон»), «Навигатор» («Нелк»), «Легенда» («Гамма») и «Сигурд» («ЦБИ МАСКОМ»).

Основой комплекса «Зарница» является сканирующий приемник AOR. «Зарница» работает по принципу сравнения излучений исследуемого устройства в двух режимах: тестовый и с выключенным тестом. Комплекс не способен своими силами опознать опасный сигнал на фоне других сигналов. Остальная часть исследования ложится на плечи оператора.

Следующий комплекс «Навигатор» выполнен на анализаторах спектра фирм «Agilent Technology» и последние версии «R&S». Этот комплекс так же не опознает самостоятельно опасный сигнал на фоне других, а работает на принципе сравнения излучения в двух режимах исследуемого устройства, с выключенным и включенным тест-режимом.

Два последних комплекса, построенные на анализаторах «Agilent Technology» и «R&S» (Легенда) и «IFR» (Сигурд), отличаются тем, что способны самостоятельно опознавать опасный сигнал по форме их огибающих, заданных соответствующими тест-программами. Программа "Сигурд-Тест" предназначена для формирования тест-сигналов для ПЭВМ, функционирующих под управлением операционных систем семейства Windows. О комплексе «Сигурд» дополнительно можно сказать, что к настоящему времени он уже способен работать с целым рядом анализаторов спектра разных фирм-производителей. Кроме этого, также в автоматическом режиме выполняет оценку эффективности систем активной защиты, как в эфире, так и в линиях. Он является единственным комплексом, в котором по негальваническому каналу производится автоматическое управление режимами тест-программы на исследуемой ПЭВМ.

Наиболее мощным источником ПЭМИ, является видеотракт. По этой причине для проведения исследований используются именно его интерфейсы.

Далее следует сказать о том, как именно с помощью тест-сигнала генерируется излучение. Допустим, в некой цепи пересылается, в последовательном коде, бесконечная последовательность байтов FF (т.е. в двоичном коде 11111111). Есть вполне реальная тактовая частота и длительность импульса. Метод кодирования – последовательный импульсный код, единица кодируется наличием импульса, ноль - отсутствием. Пауза между соседними импульсами равна длительности импульса.

Можно изменить пересылаемый байт, например, на 10101010. При этом изменится тактовая частота следования импульсов, она упадет в два раза. Возможно изменится и амплитуда частотных составляющих. Но для наблюдателя (приемника), «видящего» одну конкретную частоту, ее амплитуда упадет до нуля, сигнал просто исчезнет. Такая ситуация недопустима. Именно поэтому так важно точно знать, что «делает» тест-программа. И правильно ее «сконструировать».

Чтобы кабель излучал, в нём должен протекать переменный ток. Это значит, что злоумышленник будет наблюдать сигнал в эфире только тогда, когда в кабеле меняется уровень напряжения, т.е. когда в изображении возникает цветовой переход. В связи с этим, а также с тем, что через ПЭМИН неразличимы цветовые компоненты, перехват, в первую очередь, рассчитан на двухцветные изображения (чёрный текст на белом фоне – наиболее распространённый вид такого изображения). Перехваченное изображение, в этом случае, содержит контуры исходного. Тогда качество распознавания изображения можно определять по точности определения границ цветовых переходов на изображении. Очевидно, что, благодаря построчной развёртке, имеют значение только горизонтальные переходы, поэтому, тестовый сигнал может представлять собой чередование вертикальных полос двух цветов

Для наибольшей эффективности обнаружения тестового сигнала для видеоинформации, рекомендуется применять в качестве тестового режима – чередование черных и белых пикселей. При таком подходе, уровень излучаемых ПЭМИ максимален. Существуют разные подходы, учитывая данное обстоятельство. На примере программы Сигурд-Тест используются варианты «точка через точку», «пять точек через пятнадцать» и «зебра» из чёрных (максимальная амплитуда видео компонент) и белых (минимальная амплитуда видео компонент) полос. Для лучшего опознавания – разной ширины (высоты). Соответственно, уровни (точнее – разность уровней) ПЭМИН на «тёмных» и «белых» полосах и будет представлять собою информативную часть общей энергии ПЭМИН (поскольку энергия ПЭМИН

«синхросмеси» постоянна и не зависит от собственно видеосигнала). Какой подход применять – зависит от используемой техники. Насколько высокая необходима точность.