

ЭЛЕКТРОМАГНИТНОЕ ИЗЛУЧЕНИЕ ВИДЕОДИСПЛЕЙНЫХ МОДУЛЕЙ: РИСК ПЕРЕХВАТА ИНФОРМАЦИИ?

Вим ван Эйк,
PTT Dr. Neher Laboratories



Вышедшая в 1985 году в открытой печати статья Вима ван Эйка «Электромагнитное излучение видеодисплейных модулей: риск перехвата информации?» наделала много переполоха в стане спецслужб, до этого времени считавших удаленный перехват информации с видеодисплейных модулей своей прерогативой.

«Перепевы» этой статьи появлялись в российской открытой печати в начале 90-х годов, однако мы приняли решение опубликовать полный и максимально приближенный к оригиналу перевод статьи ван Эйка, поскольку пока в России этого так и не было сделано.

Мы считаем, что, несмотря на солидный для периодической публикации возраст, она будет интересна не только историкам, но и специалистам, занимающимся исследованием ПЭМИН.

1. Введение

Известно, что электронное оборудование генерирует электромагнитные поля, которые могут являться помеховыми для радио- и телевизионных приемников. Лежащие в основе этого явления были достаточно основательно изучены в течение предыдущих нескольких десятилетий. Результаты проведенных исследований нашли свое отражение в виде международных соглашений в области норм и методик измерения радиопомех, создаваемых различным электронным и электротехническим оборудованием.

Однако радиопомехи — не единственная проблема, которую создает электромагнитное излучение используемого оборудования. В некоторых случаях, принимая это излучение и декодируя его, можно получить доступ к информации, содержащейся в сигналах, используемых внутри оборудования, особенно цифрового.

Эта проблема отнюдь не новая. Специалисты из различных секретных ведомств знают об этом уже в течение более чем двадцати лет. Однако информация относительно того, каким образом этот вид «подслушивания» может быть нейтрализован, свободно не распространяется. Оборудование, разработан-

ное для того, чтобы зашифровать секретную информацию от такого способа утечки, будет, возможно, в три или четыре раза дороже аналогичного оборудования, используемого для обработки несекретной информации.

До недавнего времени восстановление данных, содержащихся в излучаемом электромагнитном поле, считалось очень трудным делом. Следовательно, предполагалось, что «подслушивание» цифрового оборудования под силу только профессионалам, у которых есть доступ к очень сложным устройствам обнаружения и декодирования. Как результат — цифровое оборудование для обработки частной и деловой информации остается не защищенным от «подслушивания» такого рода.

В этой статье приводятся результаты программы исследований, выполненной в Dr. Neher Laboratories of the Netherlands PTT. Эти результаты показывают, что вышеупомянутые предположения были ограничены определением возможности «подслушивания» видеодисплейных модулей, результаты ясно показывают, что в некоторых случаях задача может быть выполнена при использовании оборудования, которое является широко доступным на рынке. В случае

«подслушивания» видеодисплейных модулей это может быть обычный телевизионный приемник. При внесении незначительных изменений в схему этого устройства

пример такой излучающей цепи — линия питания какой-либо части оборудования.

дают с телевизионными, полученное изображение будет очень неустойчивое и, следовательно, трудно читаемое. Качество приема может

где требуется низкий или средний уровень защиты данных. Это наводит на мысль, что возможность подслушивания может воздействовать на telebanking¹ и другие действия, выполняемые при помощи персонального компьютера. Это возможность для соседа копировать информацию (например, данные о финансовом положении), отображаемую при выполнении означенных действий, используя его собственный ТВ-приемник.

В некоторых случаях прием конфиденциальной информации соседями может быть осуществлен даже случайно. Информация может отображаться на телевизоре при получении им обычного сигнала какой-либо телевизионной вещательной станции. Это не искусственное предположение: служба радиоконтроля Нидерландов, которая следит за использованием радиочастотного спектра, получала несколько жалоб от людей, которые принимали таким образом информацию из близлежащего туристического агентства.

Все это означает, что проблема подслушивания требует принятия мер во всем диапазоне уровней информационной безопасности, начиная с «конфиденциально» и до «совершенно секретно».

3. Электромагнитное «подслушивание»

Принцип действия большинства видеодисплейных модулей аналогичен обычному черно-белому телевидению. Следовательно, генераторы сигналов синхронизации в ТВ-приемнике могут иногда генерировать сигналы разверток с той же самой частотой, которая используется в видеодисплейных модулях. Если это случается, отображаемая ВДМ информация может быть легко воспроизведена на экране телевизора, и это может происходить даже случайно.

Проблема не может быть решена путем использования только ви-

деодисплейных модулей с частотами синхронизации, не входящими в диапазон частот синхронизации обычного телевидения, так как преступник, который решился копировать информацию на экран своего телевизора, имеет в своем распоряжении несколько способов корректировки частот синхронизации в своем телевизионном приемнике. Все, что для этого требуется – немного знаний о принципах телевизионного приема и капитало- вложения в размере приблизительно 5\$.

3.1. Восстановление синхронизации

3.1.1. Решение с внешним генератором

Самый простой и самый дешевый способ восстановления синхронизации в ТВ-приемнике – использование устройства, содержащего два генератора:

- один регулируемый генератор с частотным диапазоном 15–20 кГц, чтобы генерировать сигнал горизонтальной синхронизации (синхронизация строк);
- один регулируемый генератор с частотным диапазоном 40–80 Гц, чтобы генерировать сигнал вертикальной синхронизации (синхронизация кадров).

Оба сигнала могут быть объединены и поданы в селектор сигналов синхронизации (рис. 2) телевизионного приемника. Довольно трудно подстраивать два генератора на частоты синхронизации видеодисплейного модуля, потому что они оба должны постоянно подстраиваться в течение приема.

Хорошо известно, что вертикальные и горизонтальные частоты синхронизации связаны следующим отношением:

$$f_{\text{hor}} = k * f_{\text{vert}}$$

где k – число строк, отображаемых на экране электроно- лучевой трубки (ЭЛТ). Следовательно, на практике необходимо генерировать только сигнал горизонтальной синхронизации, а сигнал

вертикальной синхронизации получать посредством деления f_{hor} на k . Программируемый цифровой делитель частоты, который может использоваться для этой цели, приобретает по цене приблизительно 10 \$. Один раз назначенное число строк на экране позволяет восстанавливать синхронизацию регулировкой только одного генератора. На рис. 1 показана установка для «подслушивания», в которой используется этот способ восстановления синхронизации.

3.1.2. Восстановление информации из принятого сигнала

Горизонтальная и вертикальная частоты синхронизации доступны в спектре видеосигнала видеодисплейного модуля, так как видеосигнал отсутствует в течение горизонтального и вертикального обратного хода электронного луча в ЭЛТ². Поскольку сигналы синхронизации не доступны в «формате», ожидаемом ТВ-приемником, необходимо разработать схему восстановления синхронизации. Простой подход в этом отношении – извлечение частоты горизонтальной синхронизации из сигнала перевода строки [LF], используя узкополосный фильтр. Полученный сигнал – синусоидальная волна с частотой 15–20 кГц с порядочным количеством фазового шума, который может быть легко удален путем использования инерционной схемы захвата фазы. Импульс, формируемый схемой, помогает преобразовать синусоидальную волну в прямоугольную (сигнал синхронизации). После этого вертикальная частота синхронизации может быть легко получена делением частоты горизонтальной синхронизации на число экранных строк. Чтобы получить устойчивый сигнал синхронизации, необходимо иметь или высокое отношение сигнал/шум в полученном сигнале или включить узкополосный фильтр в схему. В последнем случае необходимо использовать перестраиваемый фильтр, чтобы получить пригод-

¹ telebanking – просмотр состояния и другие операции с банковским счетом. – Примеч. перев.

² Налицо противоречие предположению, сделанному в техническом приложении, о том, что видеосигнал есть случайный цифровой сигнал, что, впрочем, не влияет на применимость теоретической модели для этой цели.

ную для использования в большинстве случаев схему для восстановления синхронизации.

3.2. Место измерений

Первые измерения напряженности электромагнитного поля, генерируемого различными типами ВДМ, были выполнены точно в соответствии с Публикацией № 16 CISPR¹. Измерения напряженностей полей в соответствии с рекомендациями CISPR для оборудования обработки данных и офисного оборудования показали, что ни один из ВДМ во время тестирования не генерировал электромагнитных помех выше предельных ограничений.

Несмотря на это, было возможно получить чистое изображение информации на обычном телевизионном приемнике с расстояния приблизительно 50 метров от видеодисплейного модуля. Для ВДМ в металлическом корпусе максимальное расстояние приема равнялось приблизительно 10 метрам.

Эти измерения были также выполнены вне полос частот широкоэмитательного телевидения. Измерения напряженности поля, однако, показали, что максимальный уровень излучения, генерируемого видеодисплейным модулем, всегда размещался между полосами передачи телевизионного сигнала. Следовательно, максимальное расстояние приема может быть гораздо большим, чем расстояния, упомянутые выше². Поскольку измерения были выполнены с использованием дипольной антенны, использование направленной антенны в состоянии обеспечить по меньшей мере 10 дБ дополнительного усиления, таким образом, приводя к еще большему возрастанию максимального расстояния приема. Иногда видеодисплейный модуль

размещается близко от отражающей поверхности. Это может в самом худшем случае привести к усилению излучения еще примерно на 3 дБ.

Принимая во внимание все эти факторы, представляется справед-

лостоянку около здания, в котором использовался текстовый процессор. Затем была осуществлена попытка копирования информации из ВДМ этого текстового процессора путем фотографирования экрана телевизора, принимающего его излучения. Фотографии убедили даже наиболее скептически настроенных людей в нашей организации в том, что возможность такого рода «подслушивания» является угрозой информационной безопасности.

3.4. Дальнейшие эксперименты

В феврале 1985 года мы совместно с британской Радиовещательной корпорацией (British Broadcasting Corporation) провели в Лондоне эксперимент по «подслушиванию».

Небольшой фургон был оборудован подъемной мачтой высотой 10 метров с закрепленной на конце антенной III-го телевизионного метрового диапазона волн (VHF band III, коэффициент усиления 10 дБ). Принятый антенной сигнал усиливался (коэффициент усиления 18 дБ) и отображался на экране телевизора внутри фургона. По очевидным причинам мы не можем привести информацию относительно данных, перехваченных в результате эксперимента.

Подводя итоги, необходимо отметить следующее:

- используя специально приспособленный автомобиль возможно с большого расстояния «подслушивать» видеодисплейные модули, расположенные в зданиях;
- хотя эксперимент был выполнен среди бела дня на глазах большого количества людей, никто из них не поинтересовался, а что, собственно, мы делаем. ■

(Окончание следует)

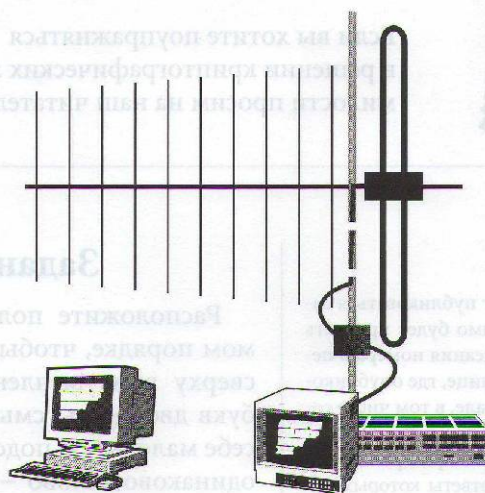


Рис. 1. Установка для «подслушивания» с использованием перестраиваемого генератора и делителя частоты для восстановления синхронизации. Изображение на экране телевизора восстановлено из излучения ВДМ на заднем плане.

ливый оценить максимальное расстояние приема с использованием только обычного телевизионного приемника приблизительно в 1 км для видеодисплейного модуля в пластмассовом корпусе и около 200 м для ВДМ в металлическом корпусе.

3.3. Экспериментальное «подслушивание»

Для доказательства практической возможности «подслушивания» в реальной ситуации был проведен следующий эксперимент с использованием простейшей установки. Автомобиль с размещенным в нем оборудованием (дипольной антенной, телевизионным приемником и генератором синхронизации) поместили на ав-

¹ CISPR – специальный международный комитет по радиопомехам (один из подкомитетов МЭК).

² В будущем телевизионные приемники будут способны принимать сигналы с частотами, лежащими вне полос широкоэмитательного телевизионного вещания, так как эти частоты будут использоваться кабельным телевидением.