УДК 621.391.8

Помехоустойчивость выделения информационного сигнала из интермодуляционного излучения при высокочастотном навязывании

И.И. Шестаков

Представлены результаты практических исследований вольт-амперной характеристики МОМ структуры (металл – оксид – металл) и воздействия сигнала на нелинейный элемент. Разработана математическая модель обработки интермодуляционного излучения при высокочастотном навязывании.

Ключевые слова: интермодуляция, высокочастотное навязывание, помехоустойчивость, шумоподобный сигнал, когерентная обработка, некогерентная обработка.

1. Введение

Побочные электромагнитные излучения (ПЭМИ) – одна из главных причин существования проблемы электромагнитной совместимости технических средств. Поэтому выявление и инструментальный контроль ПЭМИ всегда входили в число важных задач органов радиоконтроля и лиц, связанных с разработкой и эксплуатацией этих средств. В случаях, когда технические средства применяются для обработки информации ограниченного доступа, наибольшую ценность имеют вопросы, связанные с информативными ПЭМИ, называемыми ещё интермодуляционными излучениями, и наводками информативных сигналов на токопроводящие цепи. Под ними понимают ПЭМИ и наводки, которые содержат сведения об обрабатываемой информации и могут быть перехвачены заинтересованными лицами.

Сравнительная простота и скрытность добывания информации за счёт перехвата информативных ПЭМИ и наводок, постоянное совершенствование техники перехвата и алгоритмов выделения информативных сигналов заставляют специалистов проводить специальные исследования технических средств для выявления и контроля информативных ПЭМИ и наводок.

Перехват побочных электромагнитных излучений техническими средствами приёма, обработки, хранения и передачи информации (ТСПИ) осуществляется радиосредствами, размещёнными вне контролируемой зоны.

Перехват обрабатываемой техническими средствами информации может осуществляться путём специальных воздействий на элементы технических средств. Одним из методов такого воздействия является высокочастотное навязывание, т.е. воздействие на технические средства высокочастотными сигналами. В настоящее время используется два способа высокочастотного навязывания:

– посредством контактного или индукционного введения высокочастотного сигнала в электрические цепи, имеющие функциональные или паразитные связи с техническим средством;

– путём облучения высокочастотным электромагнитным сигналом источника информации и приёма отражённого модулированного сигнала.

Возможность утечки информации при использовании высокочастотного навязывания связана с наличием в цепях технических средств нелинейных или параметрических элементов [1, 2]. Навязываемые высокочастотные колебания воздействуют на эти элементы одновременно с низкочастотными сигналами, возникающими при работе этих средств и содержащими конфиденциальную информацию. В результате этого взаимодействия высокочастотные навязываемые колебания оказываются модулированными низкочастотными (информационными) сигналами. Распространение высокочастотных колебаний, модулированных информационными сигналами, по токоведущим цепям или излучение их в свободное пространство создают реальную возможность утечки конфиденциальной информации и последующего перехвата.

Источником зондирующего сигнала может быть высокочастотный передатчик, находящийся вне контролируемой зоны, «маскируемый» под передатчик сотовых сетей связи, сетей цифрового и аналогового телевидения, радиорелейных линий, радиопередатчик FM-диапазона и т.п.

Математическое выражение, описывающее интермодуляционное излучение при зондировании широкополосным сигналом, можно представить выражением:

$$\begin{aligned} S(t) &= U_{\text{с}} \times [1+\alpha(t)] \times g(t-\tau) \times \cos(\omega_0 t + \phi(t)) \\ &+ U_{\text{с}} \times \mu \times \lambda(t) \times g(t-\tau) \times \cos(\omega_0 t + \phi(t) + \Phi), \end{aligned} \quad (1)$$

где: $U_{\text{с}}$ – средняя амплитуда принятого сигнала;

$\alpha(t), \varphi(t)$ – флуктуации амплитуды и фазы сигнала, обусловленные внутренними шумами генератора зондирующего колебания;

$\lambda(t)$ – нормированное ($|\lambda|_{\text{макс}} = 1$) сообщение, подлежащее выделению перехватывающей стороной;

$\mu = \sqrt{M^2 + m^2}$ – полный индекс амплитудно-фазовой модуляции (M – индекс амплитудной, m – фазовой модуляции);

$\Phi = \text{arctg}(m/M)$ – угол модуляции;

$g(t)$ – псевдослучайная последовательность, модулирующая зондирующий сигнал;

τ – задержка отражённого сигнала по отношению к зондирующему сигналу.

Кроме присутствия нелинейного элемента промышленного производства, в средствах связи могут присутствовать структуры с нелинейными свойствами, к ним можно отнести: неплотные контакты, присутствие на поверхностях или на контактах ржавчины (структура металл – оксид – металл МОМ).

В данной статье представлены результаты исследования ВАХ нелинейного элемента МОМ-структуры, результаты исследований облучения диода КД409А. Кроме этого, разработано математическая модель обработки сложного интермодуляционного излучения при высокочастотном навязывании и представлены меры по защите съёма информации при высокочастотном навязывании.

2. Исследование нелинейных элементов

2.1 Исследование ВАХ МОМ-структуры

Результаты экспериментального исследования нелинейности ВАХ МОМ-структуры представлены на рис. 2 – 4. Схема эксперимента представлена на рис. 1. Вольт-амперная характеристика МОМ-структуры исследовалась на платформе NI Elvis II.

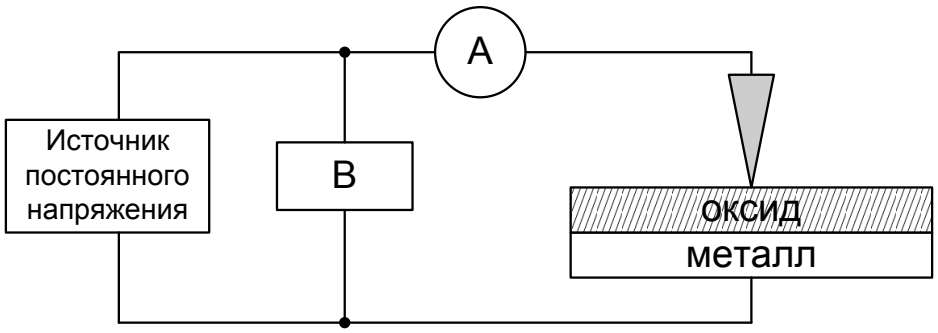

Рис. 1. Схема снятия ВАХ МОМ-структуры

На рис. 1 показан источник постоянного напряжения (от 0 до 12 В), вольтметр, амперметр и структура металл – оксид – металл. Поскольку поверхность оксида неравномерна и свойства полупроводника будут проявляться не на всей плоскости, то необходимо найти точку, в которой наиболее проявляется нелинейное свойство. В качестве второго металлического контакта использовалась металлическая игла.

По данным значениям (табл. 1) построены графики зависимости тока I от напряжения U (рис. 1 и 2) как для положительных, так и для отрицательных значений.

Таблица 1. Экспериментальные значения ВАХ МОМ-структуры

Значения положительной области	U, В	I_1, мА	I_2, мА	I_3, мА	Значения отрицательной области	U, В	I, мА
1	0	1.5	1.9	2.7	1	-0.04	-19.6
2	0.01	1.8	1.9	2.9	2	-0.05	-27.8
3	0.02	6	7	10.5	3	-0.06	-35.2
4	0.03	10.3	12.1	18.4	4	-0.07	-38.5
5	0.04	14.7	17.2	26.2	5	-0.08	-45.6
6	0.06	18.9	22.2	34.1	6	-0.09	-45.8
7	0.08	27.5	32.7	49.9	7	-0.1	-59.7
8	0.1	31.7	-	57.8	8	-0.2	-124.8
9	0.12	36	-	64.4	9	-0.3	-188.8
10	0.15	48	-	87.1	10	-0.4	-252.9
11	0.2	60	-	115	11	-0.5	-314
12	0.3	85.8	-	165.2	12	-0.6	-377.6
13	0.4	110	-	229.2	13	-0.7	-432.1
14	0.5	125	-	285.6	14	-0.8	-494.3
15	0.6	136	-	349.7	15	-0.9	-554.8
16	0.8	180	-	497	16	-1	-615
17	0.9	208	-	563	17	-	-
18	1	294	-	633	18	-	-

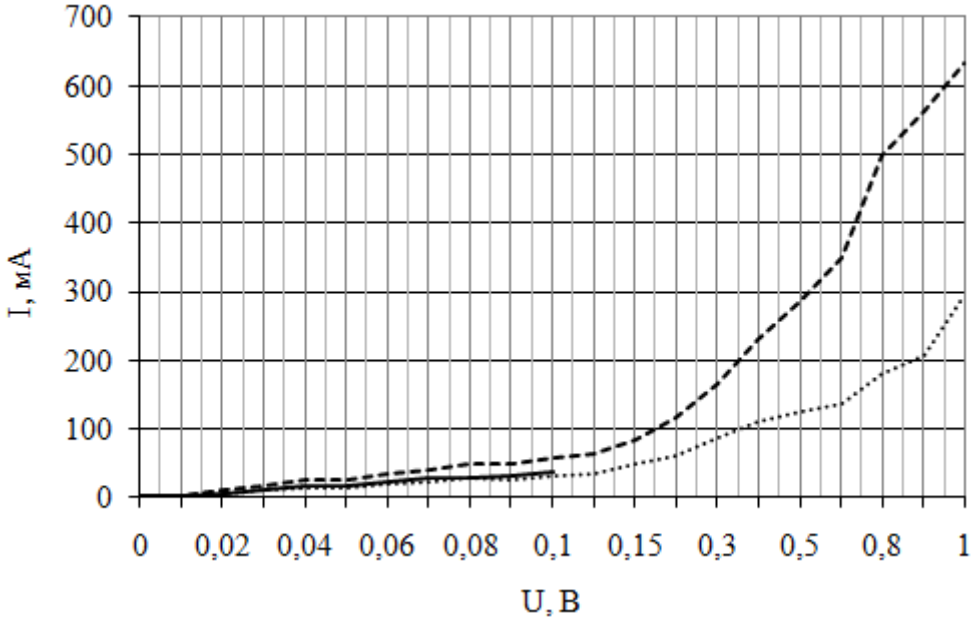

Рис. 2. Вольтамперная характеристика МОМ-структуры положительных значений

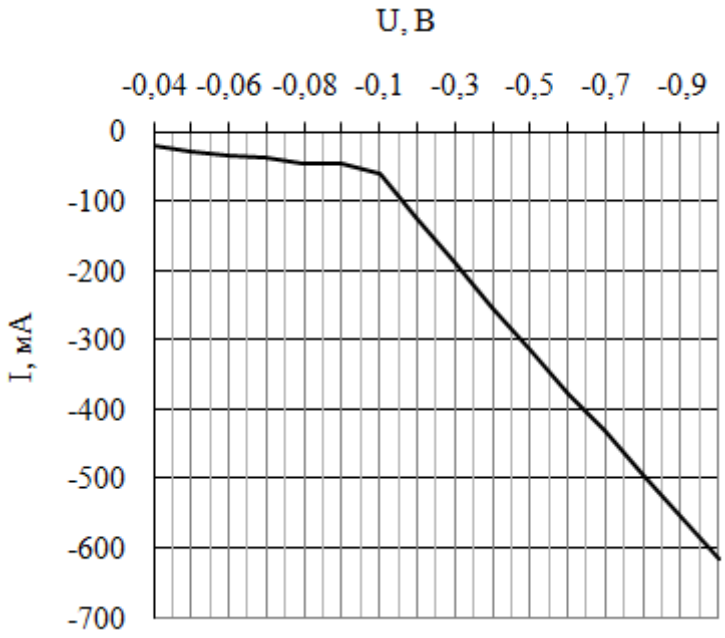

Рис. 3. Вольтамперная характеристика МОМ-структуры отрицательных значений

Как видно из рис. 2, при изменении местоположения соприкосновения второго контакта на поверхности оксида, изменяется сопротивление, при изменении напряжения, изменяется сила тока, протекающего через МОМ-структуру. В данном случае зависимость получается нелинейной. Кроме этого, нелинейную зависимость можно описать полиномом нечётной степени, что подтверждается рис. 3.

При воздействии гармонического сигнала на МОМ-структуру с частотой 1 кГц и уровнем сигнала −3 дБм, появляются гармоники, второй составляющей с частотой 2 кГц, третьей составляющей с частотой 3 кГц (рис. 4). Разница между уровнями второй и третьей гармоник составляет 3 дБм.

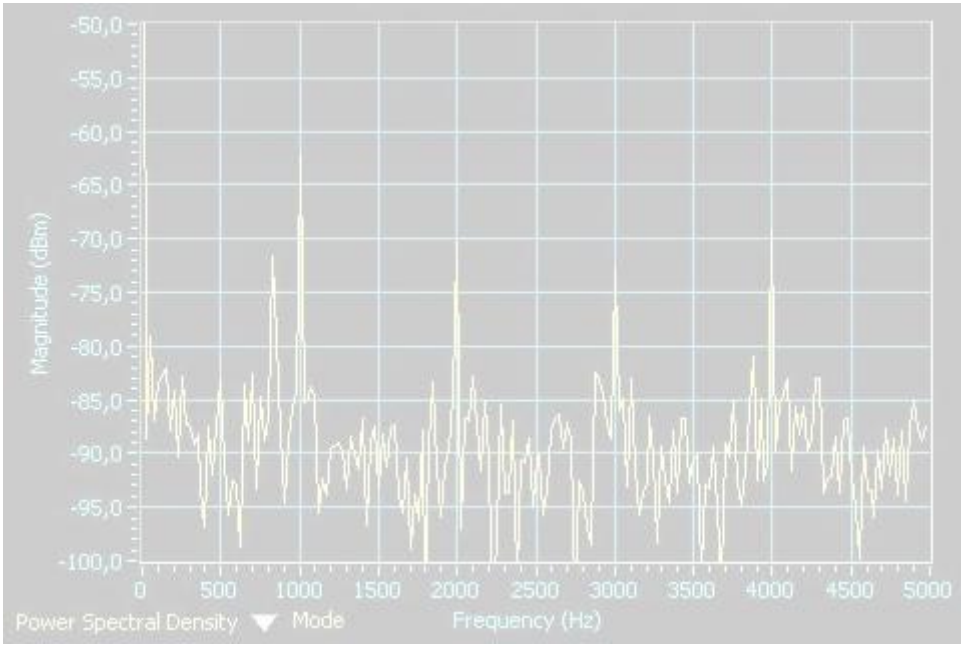

Рис. 4. Спектр сигнала на выходе МОМ-структуры при воздействии гармонического сигнала

2.1 Воздействие высокочастотного сигнала на нелинейный элемент

На рис. 5 показана схема исследования интермодуляционного излучения антенного модулятора, облучаемого узкополосным ВЧ-сигналом. Антенный модулятор выполнен на основе антенны «бабочки», между лепестками впаян диод КД409А.

Источником зондирующего сигнала является FM-трансивер. Частота зондирующего сигнала $f_з$ = 433.45 МГц (тип модуляции – частотная) мощностью 1 мВт, частота информационного сигнала $f_и$ = 100 кГц. Приёмником интермодуляционного излучения является векторный анализатор PXI-5661 платформы PXIe - 1065.

На рис. 6 показан спектр интермодуляционного излучения антенного модулятора, облучаемого узкополосным высокочастотным сигналом.

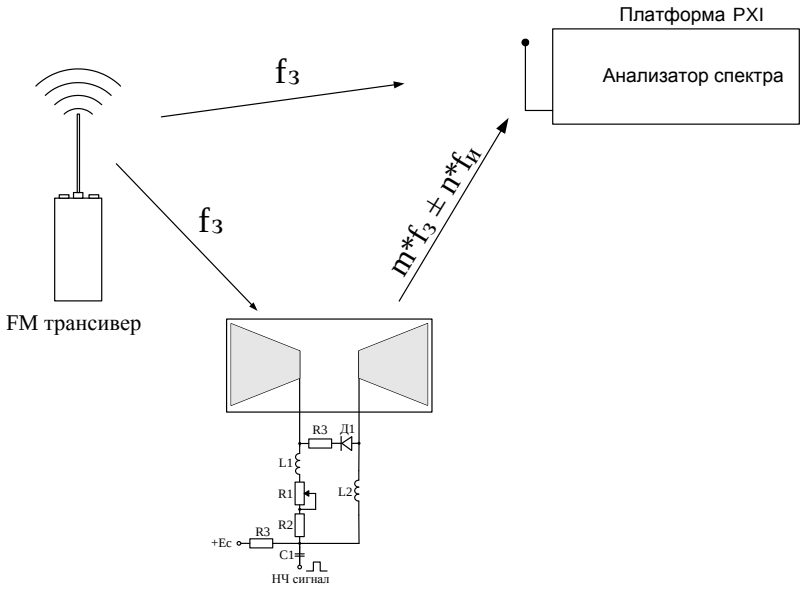

Рис. 5. Схема исследования интермодуляционного излучения антенного модулятора, облучаемого узкополосным ВЧ-сигналом

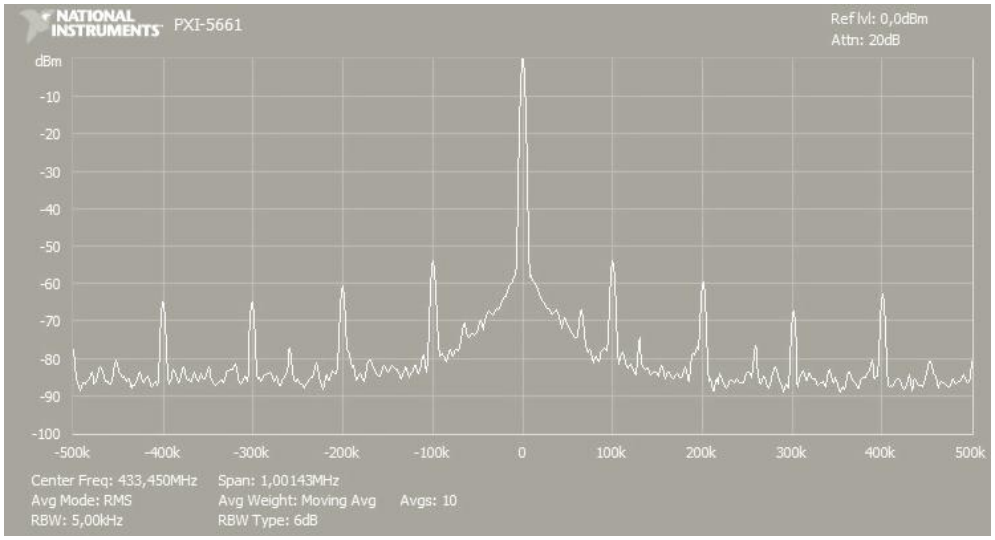

Рис. 6. Спектр интермодуляционного излучения антенного модулятора, облучаемого ВЧ-сигналом

На спектрограмме (рис. 6) показаны гармоники первого, второго, третьего и четвёртого порядка, на центральной частоте 433.45 МГц показана несущая зондирующего сигнала FM-трансивера.

Результаты практических исследований наглядно подтверждаются разработанной математической моделью обработки сложного интермодуляционного излучения, несущего конфиденциальную информацию. Математическая модель моделирует ситуацию, представленную на рис. 7.

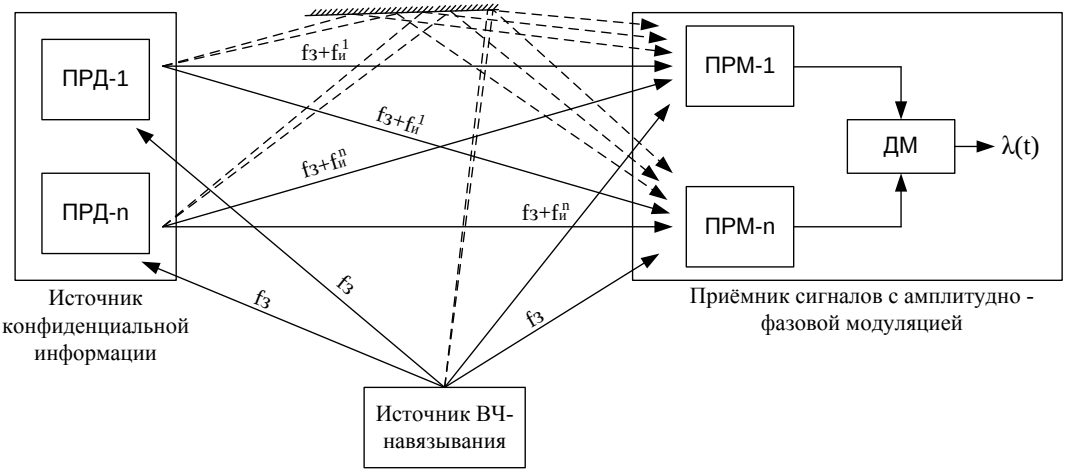

Рис. 7. Схема съёма информации методом ВЧ-навязывании

На рис. 7 показано несколько источников конфиденциальной информации, которые подвержены высокочастотному навязыванию с частотой $f_з$. Передатчики выступают в качестве «случайных антенн», в которых наводится ЭДС зондирующего сигнала, этот сигнал поступает на нелинейный элемент, модулируется по амплитуде информационным сигналом и переизлучается «случайной антенной» в окружающее пространство. В точку приёма поступает смесь сигналов с частотами $f_з$, $f_з + f_и^1$ и $f_з + f_и^n$, а также отражённые сигналы, показанные на рис. 7 штриховой линией. Сигналы поступающие от других объектов конфиденциальной информации, являются помеховыми.

3. Математическая модель обработки сигнала, модулируемого по амплитуде и фазе двумя низкочастотными сигналами

Для моделирования выбран язык программирования NI LabVIEW. Лицевая панель представлена на рис. 8. Блок-диаграмма состоит из виртуальных подприборов:

– узкополосного и широкополосного зондирующего генератора;
– генератора белого гауссова шума с нормальным законом распределения;
– двух источников информации; линейной части приёмника;
– когерентной и некогерентной части приёмника.

Блок-диаграмма когерентного и некогерентного квазиоптимального приемника смоделирована по структурной схеме, представленной в статье [3].

Результаты математического моделирования представлены графически, зависимостью коэффициента ошибок BER от отношения сигнал/шум SNR (рис. 9 - 13) и отношение сигнал/шум SNR от индекса амплитудной модуляции M (рис. 14 и 15).

В реальном режиме времени имеется возможность наблюдать форму сигнала на лицевой панели виртуального прибора, в каждой точки смоделированного приемника.

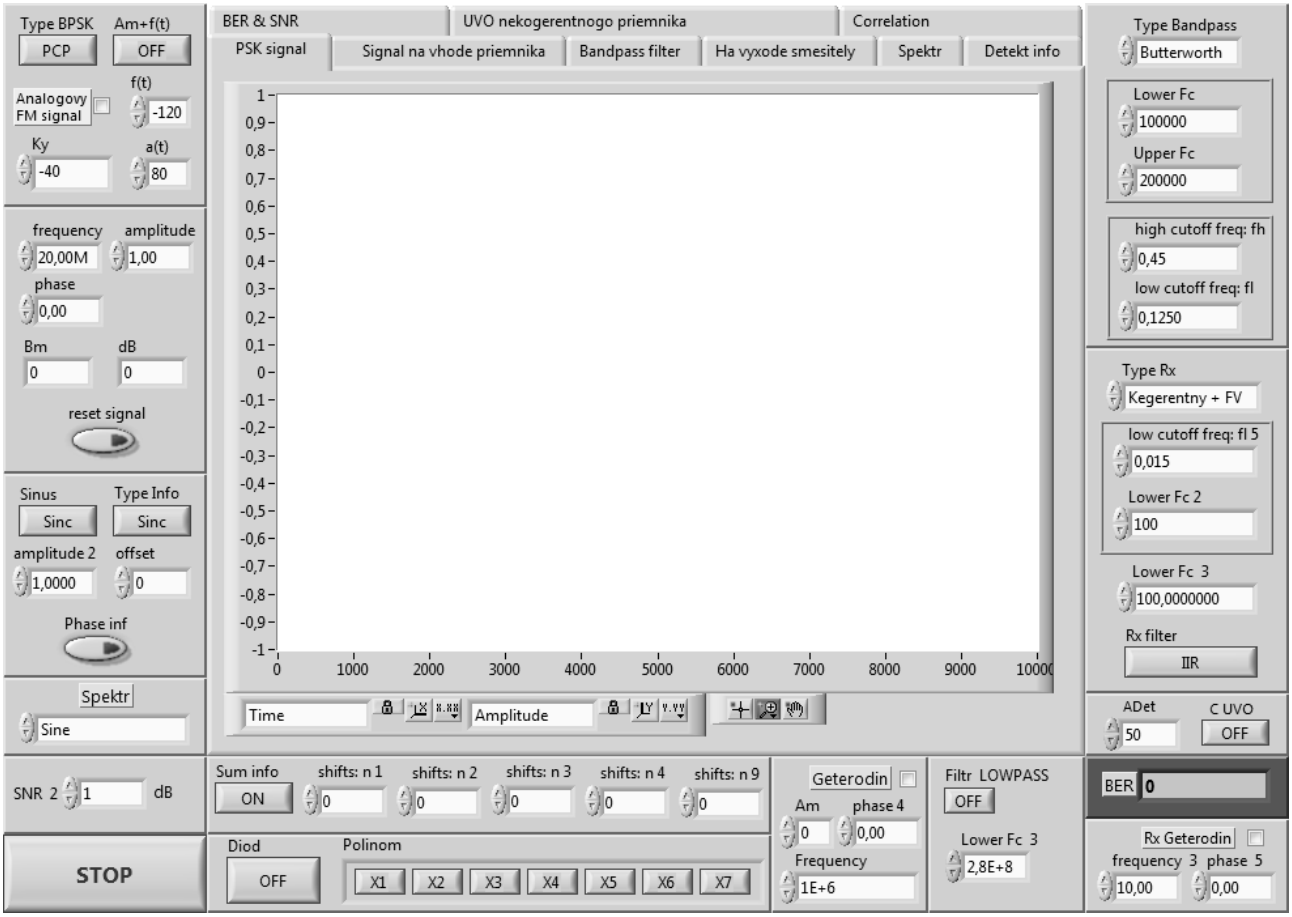

Рис. 8. Лицевая панель ВП обработки интермодуляционного излучения

Элементы управления на лицевой панели позволяют выбрать тип информационного сигнала (гармонический или бинарный), тип источника зондирующего сигнала, параметры фильтров, линии задержки и фазовращателей.

Результаты экспериментального моделирования показывают, что для выделения информационного сигнала из интермодуляционного излучения, вызванного высокочастотным навязыванием широкополосным или узкополосным сигналом, необходимо поддерживать значение SNR более 30 дБ, если приёмник находится на большом расстоянии (в эксперименте

расстояние составляло 100 метров). Это условие позволит детектировать сигнал с коэффициентом амплитудной модуляции при облучении широкополосным сигналом M = 10^{-2}, при зондировании узкополосным сигналом M = 10^{-5} как когерентным, так и некогерентным приёмником. Также необходимо учитывать мощность зондирующего сигнала. Для шумоподобного сигнала максимальное значение уровня сигнала составляло 20 дБ, для узкополосного сигнала – 0 дБ. Следует отметить, что уровень сигнала задаётся на входе нелинейного элемента.

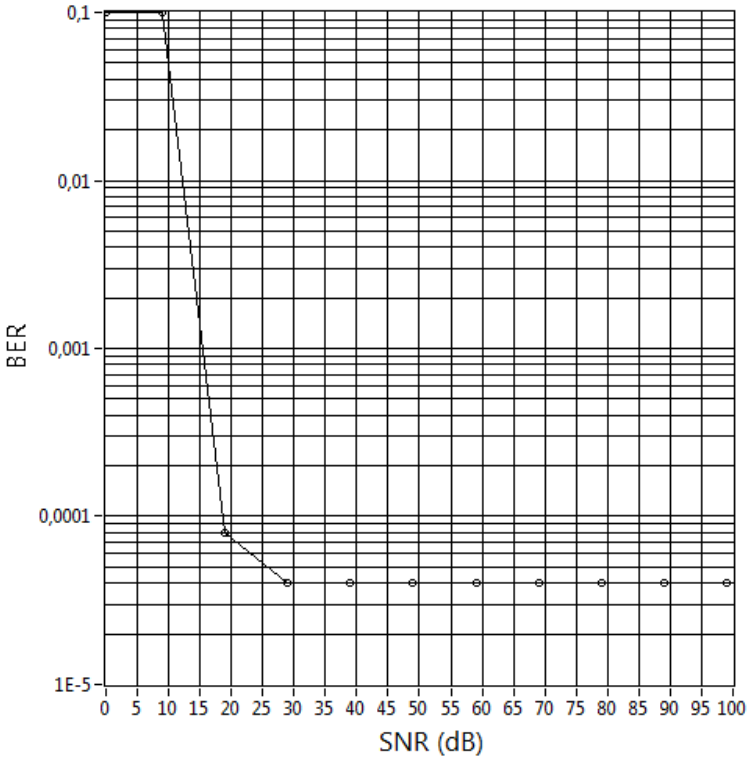

Рис. 9. График зависимости BER от SNR для когерентной обработки сигнала с индексом амплитудной модуляции M = 0.04 при зондировании широкополосным сигналом

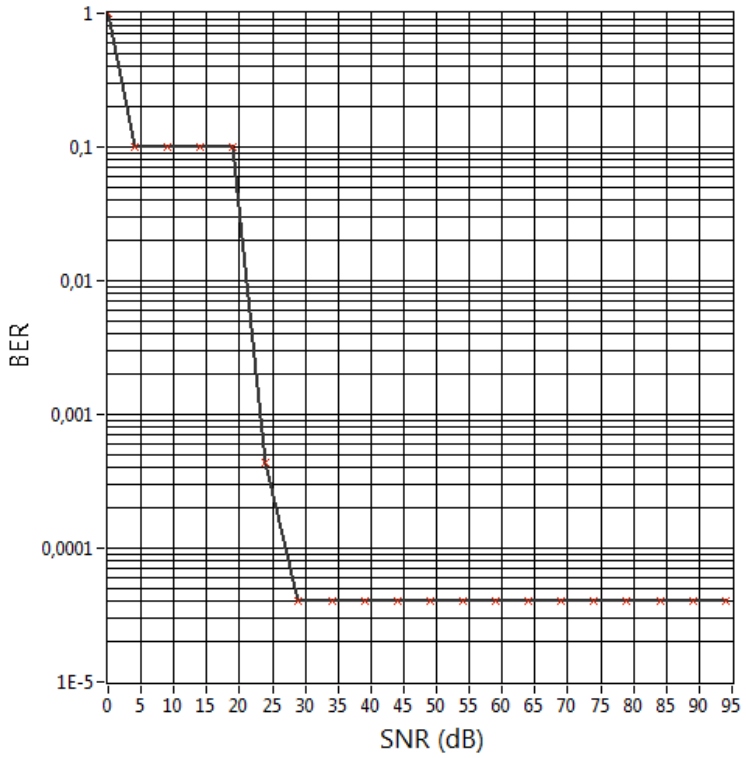

Рис. 10. График зависимости BER от SNR для некогерентной обработки сигнала
с индексом амплитудной модуляции M = 0.02
при зондировании широкополосным сигналом

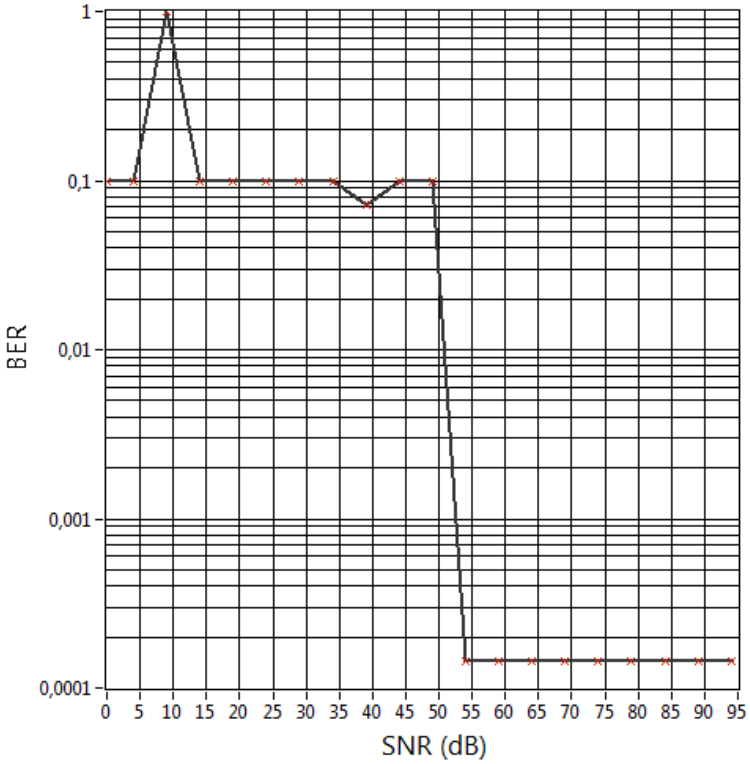

Рис. 11. График зависимости BER от SNR для когерентной обработки сигнала
с индексом амплитудной модуляции M = 0.0005
при зондировании узкополосным сигналом

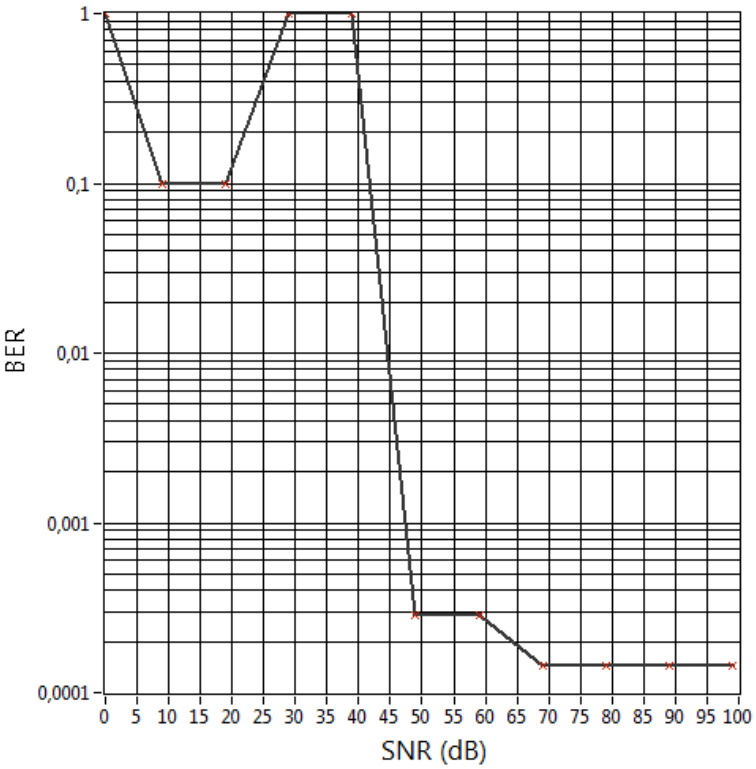

Рис. 12. График зависимости BER от SNR для некогерентной обработки сигнала с индексом амплитудной модуляции M = 0.0025 при зондировании узкополосным сигналом

На графиках (рис. 13 и 14) представлена зависимость отношения сигнал/шум от индекса амплитудной модуляции, показывающая возможность выделения информационного сигнала при различных значениях SNR и M. Зависимость SNR от M снималась для случайного бинарного сигнала при зондировании узкополосным и широкополосным высокочастотным сигналом.

На рис. 13 представлены два графика: график зависимости SNR от M (сплошная линия) снимался при статичных параметрах приёмника, график, показанный штриховой линией, снимался при изменении (подстройке) параметров фильтров нижних частот, что позволило добиться смещения линии в область 70 дБ.

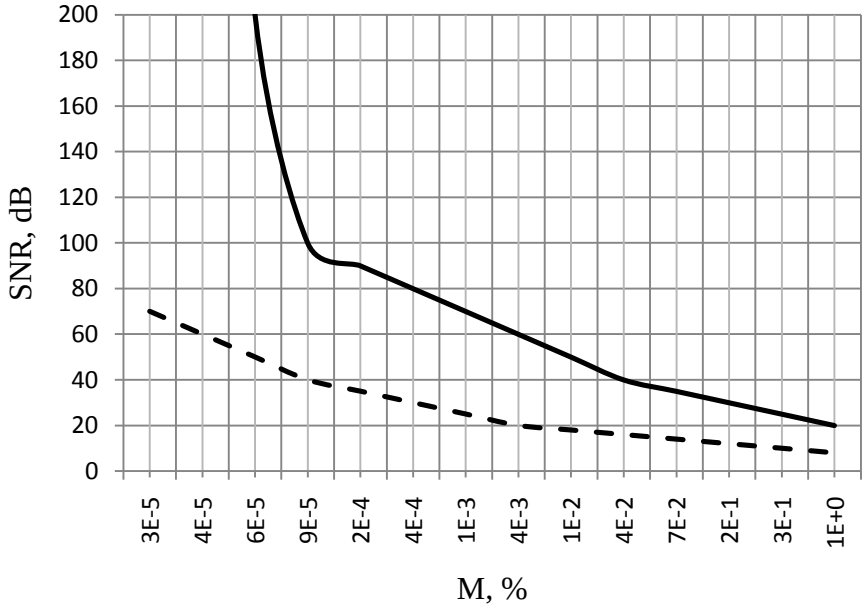

Рис. 13. График зависимости величины SNR от индекса амплитудной модуляции при зондировании узкополосным сигналом

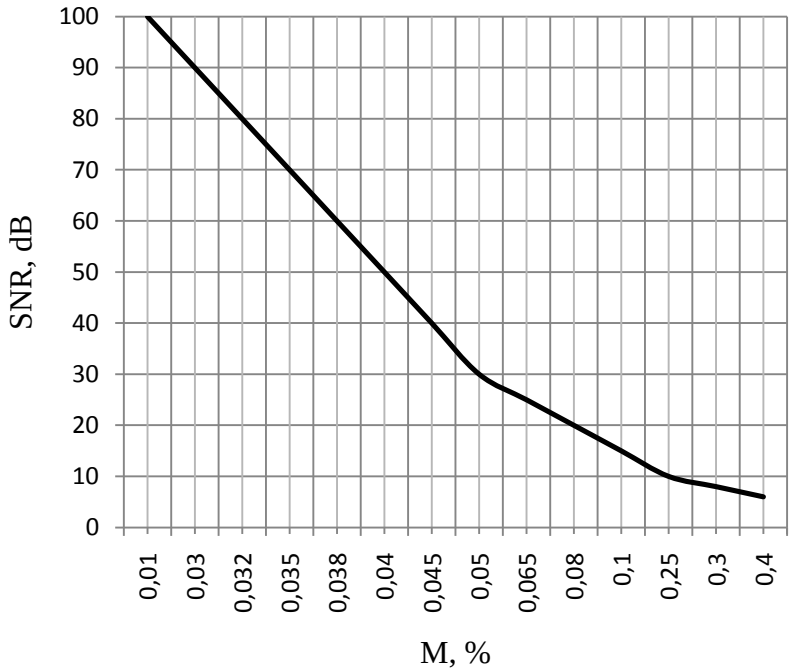

Рис. 14. График зависимости величины SNR от индекса амплитудной модуляции при зондировании широкополосным сигналом

Результат имитационного моделирования обработки двух сигналов, модулированных по амплитуде и фазе двумя независимыми процессами, представлен на рис. 15. При снятии зависимости BER от SNR, полный индекс амплитудно-фазовой модуляции помехового процесса был на порядок выше индексов модуляций информационного сообщения, что позволило повысить вероятность ошибки выделения конфиденциальной информации на один порядок. Низкочастотные процессы носили случайный характер, при этом, их верхняя частота была приблизительна одинакова.

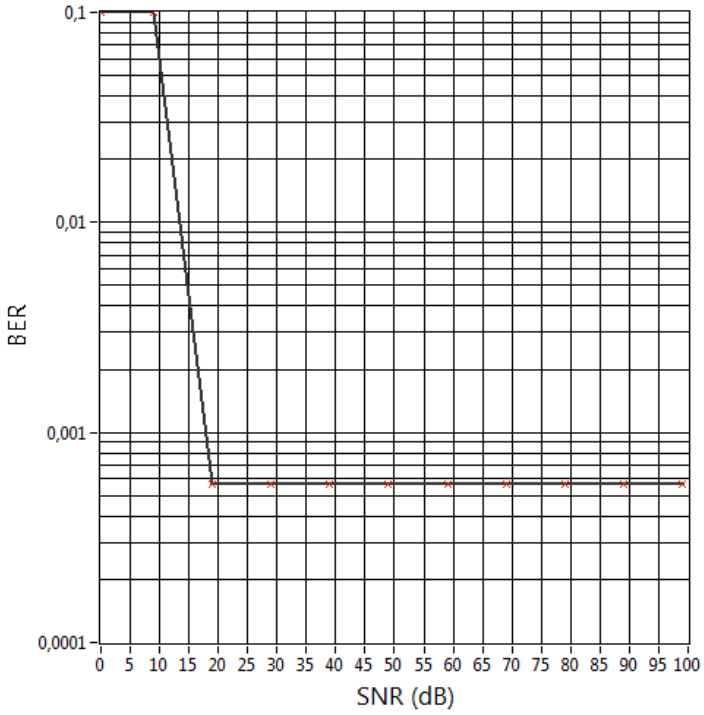

Рис. 15. График зависимости BER от SNR когерентной обработки двух сигналов в присутствии одной мультипликативной помехи

Полученный результат моделирования выделения информационного сообщения, при приеме совокупности двух интермодуляционных сигналов, наблюдаемых в смеси с одной мультипликативной помехой и аддитивным широкополосным шумом, подтверждает выражение дисперсии ошибки выделения информационного сообщений (формула 2):

$$\sigma_1^2 = \frac{1}{q_1^2 \times \mu_{11}^2 \times \sin^2 \Delta\Phi_1}, \tag{2}$$

где μ_{11} – полные индексы модуляции первого сигнала, соответственно, первым сообщением;

$\Delta\Phi_1 = \Phi_{11} - \Phi_{12}$ – разность углов модуляции сигнала сообщением $\lambda_1(t)$ и мультипликативной помехой $\lambda_2(t)$;

q_1^2 – отношение сигнал/шум в первом канале.

Также, имитационным моделированием подтверждается выражение для вероятности ошибки при обработке интермодуляционного сигнала, модулированного по амплитуде и фазе одним низкочастотным процессом:

$$P_{\text{ош}} = F\left(-q \times \mu^2 \frac{1}{\sqrt{2 \times (1 - \mu^2)}}\right), \tag{3}$$

где $F(x)$ – функция Лапласа.

4. Заключение

Для обеспечения информационной безопасности при высокочастотном навязывании объектов связи необходимо обеспечивать комплексную защиту от утечки информации. Все методы защиты от информативных побочных электромагнитных излучений и наводок делятся на пассивные и активные.

Пассивные методы (экранирование, снижение мощности излучений и наводок, снижение информативности) обеспечивают уменьшение уровня опасного сигнала или снижение информативности сигналов.

Активные методы защиты направлены на создание помех в каналах побочных электромагнитных излучений и наводок, затрудняющих приём и выделение полезной информации из информативных ПЭМИ. Этот метод является актуальным и подтверждается результатами моделирования. Из рис. 15 видно, что наличие мультипликативной помехи позволит увеличить коэффициент ошибок на один порядок. Данный вид помехи создается «искусственно», не используя широкополосных генераторов шума. Причина тому – генерация новых интермодуляционных излучений переносящих конфиденциальную информацию.

Для реализации метода дополнительной модуляции информативных интермодуляционных излучений, вызванных высокочастотным облучением технических средств связи, необходимо использовать антенный модулятор, подключенный к генератору низкочастотного сигнала, причём этот сигнал должен быть случайным. В результате этого зондирующий сигнал будет модулирован по амплитуде шумовым процессом. В точке приёма будем наблюдать сумму переизлученных сигналов, модулированных по амплитуде и фазе информационным и помеховым сообщением. Уровень мешающей помехи должен быть таким, чтобы индекс амплитудной модуляции помехового сигнала был на порядок выше информационного сообщения.

Чтобы затруднить процесс обработки сигналов, модулированных по амплитуде и фазе информационным сообщением, его необходимо дополнительно модулировать четырьмя – пятью шумовыми процессами.

Литература

1. Корнеев И.К., Степанов Е.А. Защита информации в офисе. – М.: ТК Велби, 2008.
2. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. Технические средства и методы защиты информации. – М.: ООО «Издательство Машиностроение», 2009.
3. Астрецов Д.В., Шестаков И.И., Тарасов Е.С. Анализ возможности перехвата информации при зондировании объектов широкополосными сигналами. Научные труды международной научно-практической конференции «СВЯЗЬ-ПРОМ 2009» в рамках 7-го Международного форума «СВЯЗЬ-ПРОМЭКСПО 2009», посвящённого 150-летию со дня рождения изобретателя радио А.С. Попова: в 2-х томах. Том 1. – Екатеринбург: УрТИСИ ГОУ ВПО «СибГУТИ», 2010. – С. 86-89.

Статья поступила в редакцию 26.09.2011

Шестаков Иван Игоревич
заведующий лабораториями, преподаватель кафедры многоканальной электрической связи Уральского технического института связи и информатики (филиал) ГОУ ВПО «СибГУТИ»
тел. (343) 359-91-08

Noise Immunity Isolation of Information Signal from Intermodulation Radiation at High-Frequency Imposing

I.I. Shestakov

In this article we present practical research of MOM (metal–oxide–metal) structure volt-ampere characteristics and influence of signal on nonlinear element. The mathematical model of processing intermodulation radiation at high-frequency imposing is developed.

Keywords: intermodulation, high-frequency imposing, noise immunity, noise-like signal, coherent processing, not coherent processing.