Из (14) следует:

$$0 < n^2 - 6n + 1 = \left(n - 3 + 2\sqrt{2}\right)\left(n - 3 - 2\sqrt{2}\right). \quad (15)$$

Анализ выражения (15) показывает, что постулат Бертрана всегда справедлив при $n > 5$. Простой дополнительный анализ при $1 < n \le 5$ свидетельствует о том, что названный постулат выполняется для всех $n > 1$.

Из доказательства гипотезы Лежандра легко выводится утверждение, названное гипотезой Брокарда: между квадратами подряд идущих простых чисел, за исключением первых двух, всегда найдется хотя бы четыре простых числа.

Обозначим $\pi(p_{i+1}^2)$ число простых чисел в интервале $(0, p_{i+1}^2)$ и $\pi(p_i^2)$ – число простых чисел в интервале $(0, p_i^2)$, где p_i и p_{i+1} – подряд идущие простые числа. Тогда гипотеза Брокарда формулируется как

$$\Delta\pi_B = \pi\left(p_{i+1}^2\right) - \pi\left(p_n^2\right) \ge 4. \quad (16)$$

Пусть $p_n^2 = m^2$. Докажем справедливость соотношения (16) для простых чисел-«близнецов», когда расстояние между подряд идущими простыми числами $p_{i+1} - p_i = 2$ минимально. В случае, когда соседние простые числа не «близнецы», доказательство очевидно.

Итак, вводя определение Δ_B

$$\Delta_B = (p_i + 2)^2 - p_i^2 = 4p_i + 4 = 4(m + 1), \quad (17)$$

имеем

$$\Delta_B = 4m + 4 = 2(\Delta + 1), \quad (18)$$

т. е. $\Delta = 2m + 1$ включен в интервал Δ_B.

Из (18) следует, что $\Delta\pi_B > 0$ всегда, ибо на большем, чем Δ, интервале, как было показано при доказательстве гипотезы Лежандра, всегда есть простое число.

Учитывая, что при $p_i^2 = m^2$ на интервале $(p_i^2,\ p_{i+1}^2)$ МСЧ и ПСЧ образуются такими же простыми числами, как и на интервале $(m^2, (m + 1)^2)$, справедливо следующее соотношение:

$$\Delta\pi_B = \frac{4(m+1)}{6}\left\{\left(1 - z'\right)^2 + \left(1 - \rho'\right) + \frac{1}{3}\left(1 - \frac{z'}{2}\right)\right\}. \quad (19)$$

Покажем, что даже при минимуме выражения в фигурных скобках гипотеза Брокарда подтверждается.

На самом деле минимум выражения $\left(1 - z'\right)^2 + \frac{1}{3}\left(1 - \frac{z'}{2}\right) = 0{,}16,$ а минимум $(1 - \rho') = 0{,}908$ достигается при максимуме $\rho' = 0{,}0919$.

Тогда необходимо найти m, при котором выполняется неравенство

$$\frac{4(m+1)}{6}(0{,}908 + 0{,}16) \ge 4. \quad (20)$$

Очевидно, что при $n \ge 5$, неравенство (20), а значит и (16), выполняется всегда. Таким образом, гипотеза Брокарда подтверждена.

Найденное новое, более точное соотношение для оценки количества простых чисел, содержащихся в интервале $(0, n)$, дало возможность решить открытую проблему математики – доказать гипотезу Лежандра, а также доказать гипотезу Брокарда и по-новому подойти к подтверждению постулата Бертрана, что выступает фундаментальным достижением как в области математики, так и в области разработки вычислительных процедур в сфере обеспечения информационной безопасности.

УДК 621.391

В.М. Чертков, В.К. Железняк

ИДЕНТИФИКАЦИОННЫЙ ПОРТРЕТ КАК ОСНОВНОЙ ПАРАМЕТР ИДЕНТИФИКАЦИИ РАДИОЭЛЕКТРОННЫХ СРЕДСТВ

Высокая скрытность и помехоустойчивость радиоэлектронных средств (РЭС) съема информации в различных режимах работы обусловливает необходимость совершенствования их обнаружения, оценки демаскирующих признаков и идентификации в условиях значительной неопределенности.

Нелинейный локатор (НЛ) является одним из самых эффективных технических средств по выявлению радиоэлектронных средств съема информации.

Анализ литературных источников показал, что термин «идентификация» часто воспринимается как распознавание типа нелинейности (искусственный или естественный полупроводник) элементов в составе РЭС скрытого съема информации. Авторами предложено использовать термин «идентификация» как установление тождественности неизвестного объекта известному, находящемуся в базе данных, на основании сравнения полученных характеристик в результате приема переизлученного зондирующего сигнала.

Процедура идентификации РЭС с помощью НЛ включает три основных последовательных процесса:

PDF created with pdfFactory Pro trial version www.pdffactory.com

1. Обнаружение РЭС по присутствию нелинейности. Осуществляется классическим подходом: по наличию второй и третьей гармоник, а также определением их уровня в спектре перезолоченного сигнала.

2. Получение идентификационного портрета. Авторами предложено использовать идентификационный портрет (ИП) как основной параметр поиска в экспериментально наполненной базе данных. ИП состоит из эффективной площади рассеяния (ЭПР) и вида нелинейности вольтамперной характеристики (ВАХ) исследуемого объекта. ЭПР определяет характер изменения уровней на второй, третьей и удвоенной восстановленной несущей гармониках в зависимости от угла облучения зондирующим сигналом.

На рис. 1 и 2 представлены экспериментальные данные измерения уровней гармоник в зависимости от мощности излучения зондирующего сигнала при различных углах облучения. Анализ рисунков показывает, что ЭПР простых нелинейных объектов (одиночных диодов) по форме совпадают при различных углах. Это обстоятельство дает возможность рассматривать ЭПР в виде вектора данных, полученных только при одном угле излучения.

Авторами предложен принципиально новый способ получения вида нелинейности ВАХ объекта исследования на основе использования специального зондирующего сигнала с подавленной несущей, который позволяет установить вид нелинейности по полученным данным гармоник в коэффициенты полинома, аппроксимирующего ВАХ.

Таким образом, идентификационный портрет простого нелинейного объекта состоит из трех векторов значений уровней второй, третьей и удвоенной восстановленной несущей гармоник.

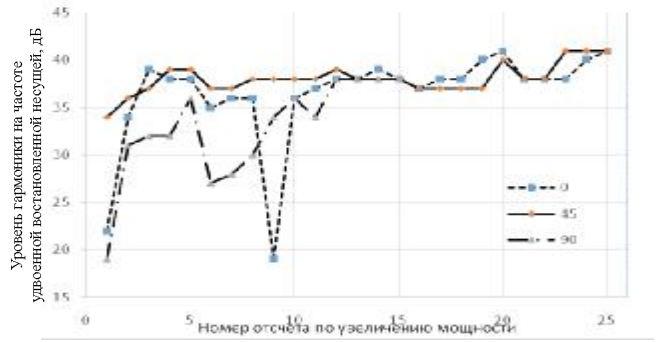


Рис. 1. Уровень гармоники удвоенной восстановленной несущей принятого переизлученного зондирующего сигнала от диода Д18

Рис. 2. Уровень второй гармоники принятого переизлученного зондирующего сигнала от диода Д18

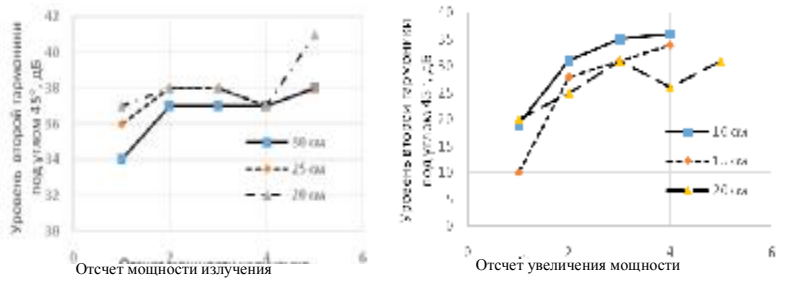
3. Идентификация РЭС (принадлежность к определенному классу на основе алгоритма поиска в экспериментально заполненной базе данных идентификационных портретов) осуществляется по алгоритму, представленному на рис. 3. Полученный идентификационный портрет поочередно сравнивается с имеющимися в базе данных для определения степени подобия. После сравнения всех записей в базе данных находится максимально похожий идентификационный портрет. Если степень подобия окажется меньше 70 %, то принимается решение о внесении новой записи в базу данных после детального дополнительного исследования. Если степень подобия выше 70 %, то процедура идентификации завершается.

Особенностью алгоритма является построение векторов из значений разности соседних уровней для каждой гармоники и вычисления их нормы и метрики. Степень подобия определяется суммой коэффициентов корреляции векторов соответствующих векторов гармоник и корреляции коэффициентов полинома, аппроксимирующего ВАХ.

PDF created with pdfFactory Pro trial version www.pdffactory.com

Рис. 3. Алгоритм идентификации РЭС

На рис. 4 представлены данные, полученные в результате измерения уровня второй гармоники от мощности излучения при разных расстояниях облучения во время проведения эксперимента по определению достоверности идентификации. В эксперименте участвовало три диода Д18, Д2, Д220. Достоверность идентификации составила 95 % при проведенных пяти экспериментах для разных значений расстояний и угла облучения, т. е. для каждого диода по 45 экспериментов: три различных значений расстояния и три значения угла облучения.



а *б*

Рис. 4. Результаты измерения уровня второй гармоники от мощности излучения на разных расстояниях от диода: *а* – диод Д18; *б* – диод Д220

УДК 004.056.5

С.А. Шабанов

СПЕЦИФИКА ЗАЩИТЫ ИНФОРМАЦИИ В ЦИФРОВЫХ РАДИОСТАНЦИЯХ СТАНДАРТА DMR

На вооружении в подразделениях внутренних войск МВД Республики Беларусь до недавних пор в основном состояли аналоговые радиостанции ОВЧ-диапазона. Основные недостатки аналоговых средств радиосвязи хорошо известны: это ограниченная функциональность, дальность связи и качество звука. Особого внимания заслуживает такой фактор, как недостаточная защищенность радиосвязи, т. е. возможность бесконтрольного прослушивания переговоров.

Для непрофессиональной радиосвязи это, конечно, не имеет существенного значения. Но учитывая те требования, которые предъявляются к управлению во внутренних войсках, как и во всех силовых структурах, утечка информации при проведении служебных мероприятий недопустима.

В соответствии с Уставом служебно-боевой деятельности внутренних войск скрытность – одно из требований, которое предъявляется к управлению войсками. Одним из важнейших способов достижения скрытого управления войсками является ограничение использования открытых каналов связи и широкое применение средств шифрования информации.

PDF created with pdfFactory Pro trial version www.pdffactory.com