УДК 621.391

Корчинский В.В.
Корчинський В.В.
Korchinsky V.V.

ОЦЕНКА СТРУКТУРНОЙ СКРЫТНОСТИ СИГНАЛЬНЫХ КОНСТРУКЦИЙ НА ОСНОВЕ ХАОТИЧЕСКИХ СИГНАЛОВ В СИСТЕМАХ ПЕРЕДАЧИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

ОЦІНКА СТРУКТУРНОЇ СКРИТНОСТІ СИГНАЛЬНИХ КОНСТРУКЦІЙ НА ОСНОВІ ХАОТИЧНИХ СИГНАЛІВ У СИСТЕМАХ ПЕРЕДАЧІ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

EVALUATION OF STRUCTURAL STEALTH SIGNAL DESIGNS BASED ON CHAOTIC SIGNALS IN THE TRANSMISSION SYSTEMS OF CONFIDENTIAL INFORMATION

Аннотация. Предложена оценка структурной скрытности методов передачи, в которых в качестве несущих колебаний используются хаотические сигналы.

Анотація. Запропоновано оцінку структурної скритності методів передачі, в яких у якості носучих коливань використовуються хаотичні сигнали.

Summary. The evaluation of structural stealth methods of transmission, in which as a carrier wave using chaotic signals was suggested.

Противодействие средствам несанкционированного доступа (НСД) к информации предприятия выдвигает всё новые требования в решение проблемы по обеспечению её защищенности. Известно [1], что защита информации от НСД осуществляется комплексом правовых, организационных и технических мероприятий непосредственно в абонентских пунктах. Не менее важной является задача по защите конфиденциальной информации от НСД на уровне физического канала, решение которой возможно за счет обеспечения скрытности передачи сигнальных конструкций [2]. Такой подход к защите информации предполагает в перспективе затруднение средствами НСД самого факта обнаружения передаваемого сигнала, распознавания его структуры и в конечном итоге раскрытия смыслового содержания перехваченного сообщения. С учетом противодействия средствам НСД различают энергетическую, структурную и информационную скрытности сигналов [2].

При условии, что сигнал обнаружен, структурная скрытность характеризует способность конфиденциальной системы связи (КСС) противостоять мерам НСД, направленным на раскрытие структуры сигнала. В этом случае задачей НСД является распознавание формы и измерение параметров сигнала, т.е. отождествление его с одним из априорно известных сигналов, принадлежащих некоторому множеству.

В [3] показана методика оценки структурной скрытности передачи для широкополосных систем связи, в которых для расширения спектра информационного сигнала используется псевдослучайная двоичная последовательность. Однако для КСС с хаотическими сигналами данная методика отсутствует, поэтому исследования и разработки по созданию соответствующей системы оценок является актуальным.

Целью статьи является разработка метода оценки структурной скрытности сигнальных конструкций, в которых хаотические сигналы применяются в качестве несущих колебаний.

Метод определения потенциальной структурной скрытности сигналов, не требующий знания алгоритмов обработки станцией НСД, изложен в работе [3]. Структурная скрытность оценивается числом двоичных измерений (дв.из), которое необходимо выполнить для задачи раскрытия структуры сигнала. Общее выражение для потенциальной структурной скрытности имеет вид [3]

$$S = \log_2 \mathrm{A}, \qquad (1)$$

где А – ансамбль реализаций, определяемый количеством всех возможных значений каких-либо параметров сигнала. Такими параметрами могут быть несущая частота, структура кода, время прихода сигнала и др. В общем случае скрытность передачи зависит от способа построения конкретного вида сигнала.

Очевидно, что для увеличения структурной скрытности передачи КСС должна манипулировать с достаточно большим ансамблем сигналов с изменяемыми во времени параметрами. Потенциально на основе хаотических сигналов можно разрабатывать методы передачи с хорошими показателями скрытности сигнальных конструкций (СК). Формирование СК на основе динамического хаоса осуществимо с помощью простейшего математического выражения [2]

$$x_{n+1} = a x_n (1 - x_n), \tag{2}$$

где a − управляющий параметр.

На рис. 1 приведена реализация сигнала $x(t)$ на выходе генератора хаоса (2) при начальном значении $x_{n=0} =$ 0,5 и $a =$ 3,9, который по своему алгоритму функционирования является детерминированным устройством. Такой сигнал обладает всеми свойствами шумоподобного сигнала [2], так как для него характерны непериодичность траекторий во времени, быстро спадающая автокорреляционная функция, сплошной непрерывный спектр мощности. Такие свойства хаотических сигналов обосновывают их использование в современных КСС, где генераторы хаоса играют роль формирователей несущих. Возможные методы модуляции хаотического сигнала $x_{CSK}(t)$ и $x_{NRZ}(t)$ для передачи цифровой информации показаны на рис. 2.

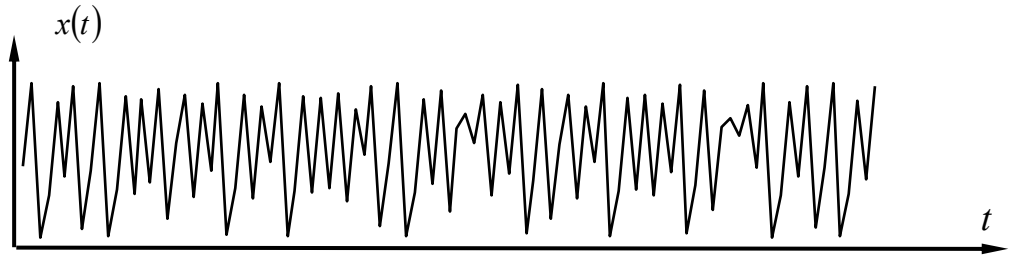

Рисунок 1 − Реализация хаотического сигнала

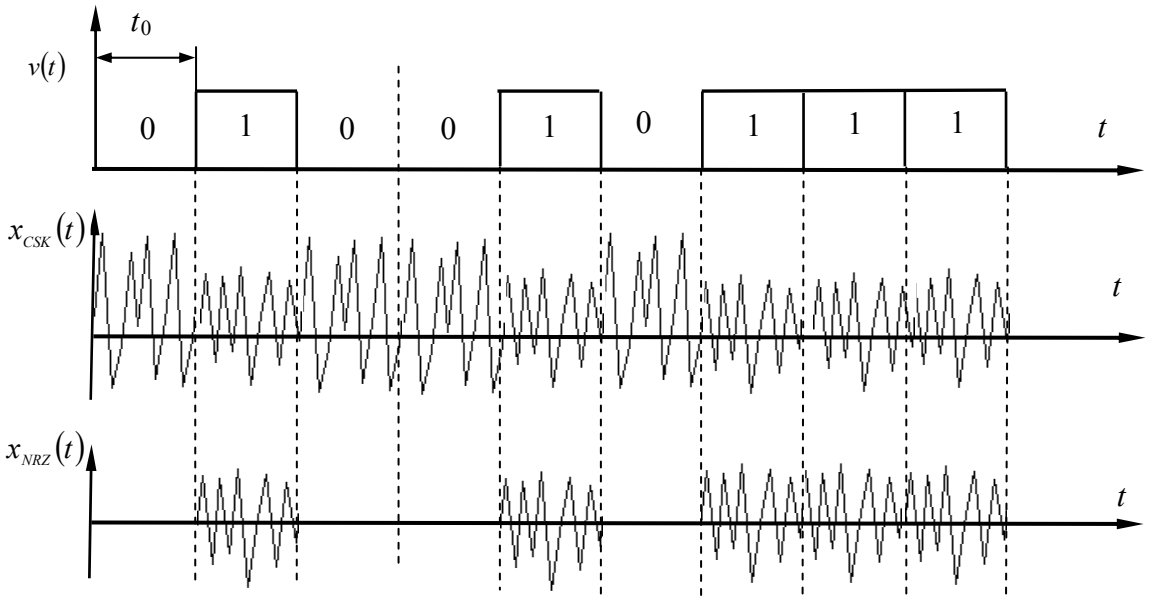

Рисунок 2 − Методы модуляции хаотического сигнала
для передачи цифровой информации

Метод модуляции $x_{CSK}(t)$ в верхней части рисунка основан на переключении хаотических сигналов на интервалах времени смены полярности двоичной последовательности. Нули и единицы кодируются последовательно расположенными фрагментами хаотического сигнала двух видов. Первый сигнал кодирует нули, второй − единицы. В англоязычной терминологии этот прием называется *CSK* (*chaotic shift keying*).

В качестве модулирующего сигнала можно использовать сигналы *NRZ* (*not reset to zero*). Как и в предыдущем случае, нули и единицы кодируются последовательно расположенными фрагментами двух сигналов. Но теперь один из них, кодирующий нули, − нулевой сигнал, а второй, кодирующий единицы, − хаотический (нижняя часть рис. 2, сигнал $x_{NRZ}(t)$.

Проанализируем возможные методы приема таких сигналов средствами НСД. В системе с *NRZ* выделение цифрового сигнала $v(t)$ осуществимо по огибающей модулированного сигнала $x_{NRZ}(t)$ при условии, что соотношение сигнал/шум больше единицы. Такой метод приема не позволит распознать хаотические несущие в сигнальной конструкции $x_{NRZ}(t)$. Дешифрирование информационного сигнала из $x_{CSK}(t)$ возможно при корреляционном приеме, однако требует знание несущих составляющих хаотического сигнала. Очевидно, что для оценки эффективности того или иного метода формирования хаотических сигнальных конструкций (ХСК) требуется соответствующая методика определения потенциальной структурной скрытности.

Для оценки структурной скрытности ХСК будем использовать его квантованные по уровню отсчеты в точках реализации процесса $x(t)$ (рис. 3, *а*), полученного с помощью генератора хаоса (1) на интервале времени элементарной посылки t_0. Преобразуем сигнал $x(t)$ в отсчеты $x_{\text{отс}}(t)$ восьмиуровневого сигнала (d = 8) (рис. 3, *б*), а затем снова в аналоговый сигнал $x_{\text{кв}}(t)$ (рис. 3, *в*).

В результате такого преобразования возникнет ошибка квантования сигнала $\Delta_{\text{кв}}(t)$ (рис. 3, *г*). Для оценки степени сходства между исходным сигналом $x(t)$ и восстановленным $x_{\text{кв}}(t)$ был рассчитан взаимный коэффициент корреляции K = 0,993. Значение K близко к единице, что свидетельствует о незначительном отличии $x_{\text{кв}}(t)$ от $x(t)$. С одной стороны, очень важно не завышать число уровней квантования d, чтобы искусственно не увеличивать расчетную величину структурной скрытности хаотического сигнала, а, с другой, минимально допустимое значение d должно обеспечивать допустимую распознаваемость сигнала $x(t)$ по $x_{\text{кв}}(t)$.

Оценим возможное множество всех реализаций ХСК (табл. 1), которое можно сформировать на интервале времени t_0 с учетом d и числа отсчетов B (базы сигнала)

$$A_{\text{ХСК}} = d^B. \tag{3}$$

Таблица 1 – Количество реализаций $A_{\text{ХСК}}$ хаотического сигнала в зависимости от B и d

B	8	10	12	14	16	18
d = 2	2,560E+02	1,024E+03	4,096E+03	1,638E+04	6,554E+04	2,621E+05
d = 8	1,678E+07	1,074E+09	6,872E+10	4,398E+12	2,8147E+14	1,801E+16

Из таблицы видно, что с увеличением базы сигнала B существенно растет число реализаций, что усложняет задачу распознавания структуры ХСК. Число d можно считать основанием системы счисления, служащего для формирования хаотического сигнала. Значение потенциальной структурной скрытности $S_{\text{хск}}$ определяется с учетом максимального ансамбля реализаций $\text{A}_{\text{хск}}$, который требуется проанализировать методом полного перебора с целью нахождения отсчетов последовательности $x_{\text{кв}}$ при несанкционированном доступе

$$S_{\text{хск}} = \log_2 d^B. \tag{4}$$

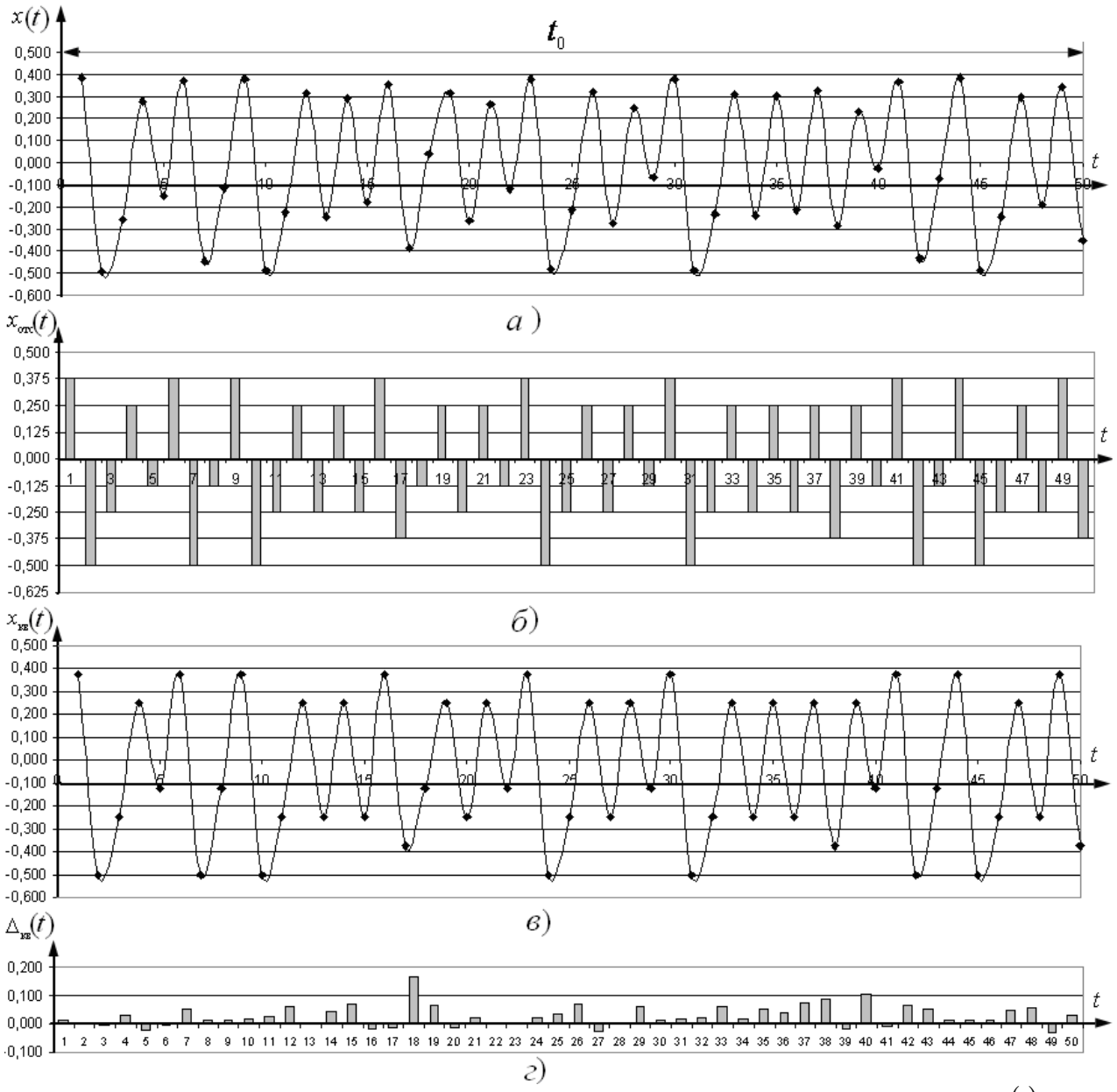

Рисунок 3 – Преобразование хаотического сигнала x в квантованные отсчеты $x_{\text{отс}}(t)$

Оценим структурную скрытность для квантованного по уровню хаотического сигнала $x_{\text{кв}}$. Для сравнительного анализа будем использовать широкополосные сигналы [4], в которых для расширения спектра информационного сигнала используются двоичные псевдослучайные последовательности (ПСП).

На рис. 4 показаны зависимости потенциальной структурной скрытности ХСК и ПСП от базы сигнала B. Как видно из рисунка потенциальная скрытность $S_{\text{хск}}$ хаотического сигнала существенно увеличивается по сравнению с $S_{\text{псп}}$ псевдослучайной последовательности и для $B = 64$ превышает её уже в три раза.

Предложенный метод позволят оценивать потенциальную структурную скрытность ХСК на интервале t_0. Для сравнительного анализа таких конструкций целесообразно выбирать оптимальное значение d и учитывать особенности алгоритма формирования ХСК. Полученные результаты сравнительного анализа показывают целесообразность использования хаотических сигналов для задачи повышения скрытности передачи конфиденциальной информации.

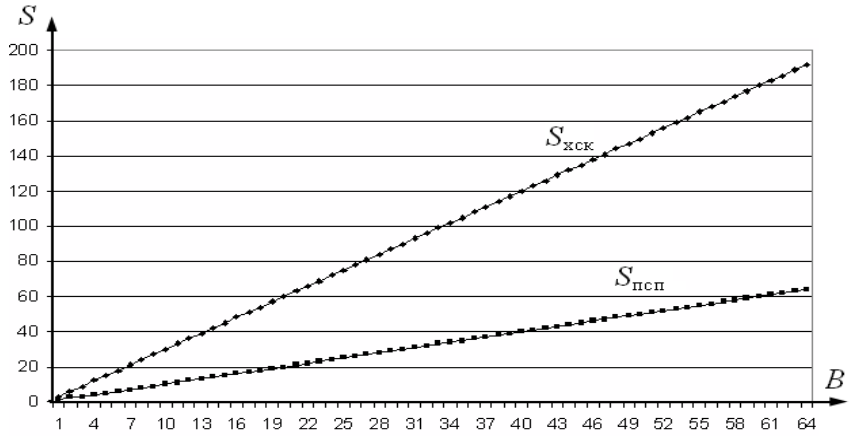

Рисунок 4 − Зависимости структурной скрытности ХСК и ПСП от базы B

В заключение можно сделать следующие выводы.

В данной статье разработан метод оценки структурной скрытности ХСК. Метод позволяет проводить сравнительный анализ различных алгоритмов формирования ХСК.

Литература

1. *Куприянов А.И.* Теоретические основы радиоэлектронной борьбы / А.И. Куприянов, А.В. Сахаров. – М.: Вузовская книга, 2007. – 356 с.
2. *Гуляев Ю.В.* Информационные технологии на основе динамического хаоса для передачи, обработки, хранения и защиты информации / [Ю.В. Гуляев, Р.В. Беляев, Г.М. Воронцов и др.] // Радиотехника и электроника. – 2003. – Т. 48. – № 10. – С. 1157–1185.
3. *Каневский З.М.* Теория скрытности / З.М. Каневский, В.П. Литвиненко. – Воронеж: ВГУ, 1991. – 144 с.
4. *Помехозащищенность* систем радиосвязи с расширением спектра сигналов модуляцией несущей псевдослучайной последовательностью / [Борисов В.И., Зинчук В.М., Лимарев А.Е. и др.]; под ред. В.И. Борисова. – М.: Радио и связь, 2003. – 640 с.