УДК 621.396

ОЦЕНКА БЕЗОПАСНОСТИ ПЕРЕДАЧИ ИНФОРМАЦИИ ЦИФРОВОЙ СИСТЕМОЙ УПЛОТНЕНИЯ СИГНАЛОВ С ИСКУССТВЕННО СОЗДАВАЕМЫМИ ГРЕБЕНЧАТЫМИ СПЕКТРАМИ

к.т.н., проф. Л.С. Сорока, к.т.н. Д.Н. Воронов,
к.т.н. А.Г. Снисаренко, к.т.н. С.Г. Рассомахин

В статье проведена оценка безопасности передачи информации цифровой системой уплотнения сигналов с применением нового класса сигналов.

Введение. В настоящее время очень важное значение приобретает проблема безопасности передачи информации в смысле сохранения ее конфиденциальности. От решения проблемы безопасности информации зависит и успех военной операции, и успех политиков и глав мировых держав, безопасность страны и даже исход войны. Мнение многих ведущих специалистов в области безопасности информации однозначно: третья мировая война будет информационной. Не лишены смысла и слова известного философа: кто владеет информацией – тот владеет миром. Значение информации, а тем более ее безопасности в наше время трудно переоценить.

Анализ литературы и последних исследований. Сигналы с гребенчатыми спектрами – это новый перспективный класс сигналов [2], сравнимых по помехозащищенности с широкополосными сигналами, но значительно превосходящими их по показателю эффективности использования частотного ресурса [2, 3]. В [1, 4, 5] был предложен способ объединения сигналов с гребенчатым спектром, а в [3] оценена энергетическая эффективность использования данного класса сигналов. Особый интерес представляет оценка безопасности передачи информации цифровой системой уплотнения сигналов с использованием нового класса сигналов – сигналов с гребенчатыми спектрами, поскольку ранее этот вопрос не рассматривался в научных публикациях. С практической точки зрения очень важно оценить уровень безопасности передачи информации, который может обеспечить система уплотнения и какими методами это можно реализовать, вскрыть возможные слабые места системы уплотнения в плане обеспечения конфиденциальности передачи информации. В связи с этим целесообразно провести оценку безопасности передачи информации с использованием нового класса сигналов, которая, возможно, позволит подняться на новый уровень безопасности передачи инфор-

© к.т.н., проф. Л.С. Сорока, к.т.н. Д.Н. Воронов, к.т.н. А.Г. Снисаренко, к.т.н. С.Г. Рассомахин, 2004

мации благодаря исключительным свойствам нового класса сигналов.

Основная часть. Цифровая система уплотнения сигналов с искусственно создаваемыми гребенчатыми спектрами (ЦСУС СГС) представляет собой приемное и передающее звенья. Принцип работы ЦСУС СГС подробно описан в [1]. Основным элементом системы уплотнения является цифровой фильтр (ЦФ) [4, 5]. Структурная схема цифрового фильтра представлена на рис. 1, где $a_0 - a_n$ – аттенюаторы с коэффициентом передачи $a_0 - a_n$, τ – линия задержки на время τ, Σ – сумматор, $n + 1$-канальная ЦСУС СГС состоит из $n + 1$ цифровых фильтров, каждый из которых характеризуется индивидуальным набором характеристик аттенюаторов, соответствующих определенному каналу ЦСУС СГС.

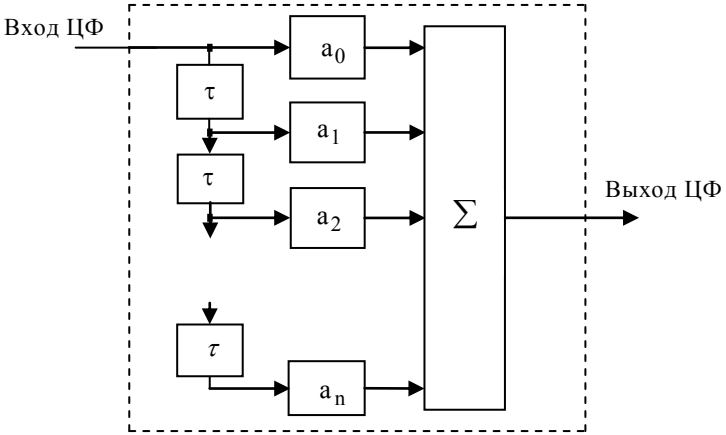

Рис. 1. Структурная схема цифрового фильтра

Коэффициенты передачи аттенюаторов $a_0 - a_n$ ЦФ каналов определяются элементами строк матрицы А:

$$A = \begin{vmatrix} a_0^0 & a_1^0 & \dots & a_n^0 \\ a_0^1 & a_1^1 & \dots & a_n^1 \\ \vdots & \vdots & \dots & \vdots \\ a_0^n & a_1^n & \dots & a_n^n \end{vmatrix}. \qquad (1)$$

Элементы соответствующей строки матрицы являются коэффициентами передачи аттенюаторов, соответствующих определенному каналу и представляют собой координаты ортогональных векторов $n+1$-мерного пространства, выходящих из начала координат. Каждый вектор характеризует своими элементами один из каналов системы уплотнения. Обязательное условие для элементов матрицы – ортогональность векторов, т.е. ска-

лярное произведение любых двух строк матрицы должно быть равно нулю:

$$a_0^0 \cdot a_0^1 \cdot \ldots \cdot a_0^n + a_1^0 \cdot a_1^1 \cdot \ldots \cdot a_1^n + \ldots + a_n^0 \cdot a_n^1 \cdot \ldots \cdot a_n^n = 0. \qquad (2)$$

Условие (2) определяет независимость каналов системы. Это значит, что на приемной стороне соответствующий ЦФ выделяет цифровую последовательность только “своего” канала, совершенно не реагируя на последовательности других каналов.

Сумма квадратов элементов каждой строки матрицы должна быть равна 1 для создания равномощного нормированного сигнала:

$$\left(a_0^0\right)^2 + \left(a_1^0\right)^2 + \ldots + \left(a_n^0\right)^2 = 1; \quad \left(a_1^1\right)^2 + \left(a_1^1\right)^2 + \ldots + \left(a_n^1\right)^2 = 1 \qquad (3)$$

и т.д. до

$$\left(a_1^n\right)^2 + \left(a_1^n\right)^2 + \ldots + \left(a_n^n\right)^2 = 1.$$

Размерность матрицы зависит от числа каналов, используемых в системе. Коэффициент сжатия k равен n + 1. Задержка τ определяется допустимой задержкой при передаче информации и требованиями помехозащищенности.

Для того, чтобы вскрыть исходный сигнал, противнику требуется: определить количество каналов в системе уплотнения; определить задержку τ; определить коэффициенты строки матрицы A, используемые в цифровом фильтре (для одного канала, затем последующих каналов).

Решение первой и второй задачи (они взаимосвязаны) для противника не составляет особого труда (занимает мало времени), основную трудность для противника представляет решение третьей задачи.

При условии, что наиболее эффективным методом является лобовое вскрытие, противнику требуется определить коэффициенты одной из строк матрицы методом полного перебора для вскрытия одного из n каналов. Определение коэффициентов других строк облегчается, т. к. мера неопределенности с каждым вскрытым каналом уменьшается.

Для матрицы размерности n + 1 необходимо определить коэффициенты строки матрицы, учитывая число степеней свободы каждого коэффициента. Число степеней свободы определяется минимальным числом возможных значений коэффициента, необходимых для определения коэффициентов матрицы размерности n + 1 с заданной степенью точности. Число степеней свободы зависит от числа n + 1 (размерность матрицы), а также от уровня помех, задаваемых проекциями мешающих неортогональных векторов. Фактически число n определяет n + 1-мерное пространство, в котором существует n + 1 ортогональных векторов или n векторов, ортогональных данному.

Число степеней свободы определяется соотношением

$$\nu = 180 \Big/ \arcsin \frac{p}{n} \cdot \frac{90}{\pi}, \qquad (4)$$

где p – проекция мешающего неортогонального вектора; n – размерность матрицы.

Цифровая последовательность, передаваемая в канал связи, обладает свойствами случайности. Это подтверждается принципом ее формирования [1, 2] при условии, что все каналы (даже в отсутствие информации) передают цифровую последовательность, близкую к случайной. Вероятность вскрытия каналов системы уплотнения в этом случае подчиняется нормальному закону распределения, и, следовательно, вероятность вскрытия одного канала системы может быть оценена выражением [6]:

$$P = 1 \Big/ \nu^{n+1}, \qquad (5)$$

где ν – число степеней свободы; n – число каналов в системе.

Результаты вычислений вероятностей вскрытия каналов системы уплотнения для разных уровней порога шумов неортогональности (уровня мощности спектральной плотности помехи по отношению к мощности полезного сигнала) $Y = p^2 = 0{,}1; 0{,}2; \ldots 0{,}9$ приведены в табл. 1.

Зависимости вероятности лобового вскрытия (полного перебора коэффициентов матрицы) от n для различных порогов шумов неортогональности приведены на рис. 2.

Различимость принятого сигнала зависит от заданного порога шумов неортогональности при вскрытии системы. Для цифрового и для аналогового сигнала порог будет разный, поскольку избыточность у них разная. Необходимо отметить, что для цифрового сигнала значение $Y = 0{,}5$ является предельным, выше которого понятия различимости цифрового сигнала просто не существует. Для аналогового сигнала значение Y может превышать 0,5. Значение Y в этом случае зависит от избыточности аналоговой информации.

Вероятность вскрытия следующих каналов системы будет каждый раз увеличиваться по мере того, как мера неопределенности вскрытия оставшихся каналов уменьшается с каждым вскрытым каналом.

Время вскрытия канала T рассчитывалось как частное числа возможных комбинаций коэффициентов цифровых фильтров на производительность машины C, реализующей алгоритм вскрытия, соотношение (6)

$$T = \nu^n \Big/ C, \qquad (6)$$

где n – число каналов в системе; ν – число степеней свободы; C – производительность машины, реализующей алгоритм вскрытия, оп./сек.

В табл. 2 – 4 приведены результаты расчета вероятности и времени вскрытия одного канала системы одной машиной, осуществляющей про-

верку 1 млн. комбинаций в секунду, и тысячей таких машин, работающих параллельно.

Для приближения структуры группового сигнала к случайной, необходимо, чтобы по всем каналам передавалась информация. В отсутствие передачи информации по одному или нескольким каналам необходимо “заполнять” неработающий канал непрерывной случайной последовательностью (например, рекуррентной). Пренебрежение этим требованием может сильно облегчить задачу противника по вскрытию исходного сигнала.

Для 8-канальной системы уплотнения существует 10^{12} комбинаций перебора коэффициентов матрицы с порогом Y = 0,5.

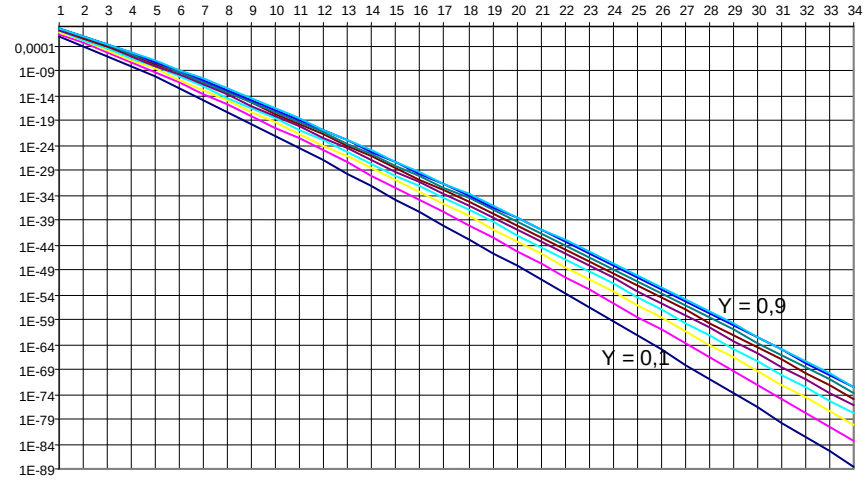

Рис. 2. Семейство зависимостей вероятности полного перебора коэффициентов одной строки матрицы от числа каналов системы для разных уровней порога шумов неортогональности Y = 0,1; … ; 0,9

Таблица 2

Оценка среднего времени лобового вскрытия одного канала ЦСУС СГС в зависимости от числа каналов в системе, Y = 0,1

Кол-во каналов в системе	Вероятность вскрытия “в лоб” Y = 0,1	Время вскрытия “в лоб” одной машиной	Время вскрытия “в лоб” тысячей машин, раб. параллельно
2	$1,1*10^{-2}$	-	---
3	$1,3*10^{-4}$	---	---
4	$1,3*10^{-6}$	---	---
5	$1,0*10^{-8}$	1,7 мин.	---
6	$6,7*10^{-11}$	4 часа	15 сек.
7	$3,7*10^{-13}$	1 месяц	45 мин.

8	$1,8*10^{-15}$	17 лет	6 суток
9	$7,9*10^{-18}$	31 107 лет	32 года
10	$3,1*10^{-20}$	3 170 979 лет	3 170 лет

Таблица 3

Оценка среднего времени лобового вскрытия одного канала ЦСУС СГС в зависимости от числа каналов в системе, Y = 0,5

Кол-во каналов в системе	Вероятность вскрытия “в лоб” Y = 0,5	Время вскрытия “в лоб” одной машиной	Время вскрытия “в лоб” тысячей машин, раб. параллельно
2	$6,2*10^{-2}$	---	---
3	$1,5*10^{-3}$	---	---
4	$3,3*10^{-5}$	---	---
5	$5,8*10^{-7}$	---	---
6	$8,5*10^{-9}$	1,7 мин	---
7	$1,1*10^{-10}$	3 часа	1,2 сек
8	$1,2*10^{-12}$	12 суток	20 мин
9	$1,1*10^{-14}$	3 года	1,2 суток
10	$9,7*10^{-17}$	317 лет	4 месяца
11	$7,6*10^{-19}$	41 723 года	42 года
12	$5,4*10^{-21}$	5 872 183 года	5 872 года

Таблица 4

Оценка среднего времени лобового вскрытия одного канала ЦСУС СГС в зависимости от числа каналов в системе, Y = 0,9

Кол-во каналов в системе	Вероятность вскрытия “в лоб” Y = 0,9	Время вскрытия “в лоб” одной машиной	Время вскрытия “в лоб” тысячей машин, раб. параллельно
2	$1,6*10^{-1}$	---	---
3	$3,8*10^{-3}$	---	---
4	$1,1*10^{-4}$	---	---
5	$2,6*10^{-6}$	---	---
6	$5,0*10^{-8}$	1,7 мин	---
7	$8,4*10^{-10}$	20 мин	---
8	$1,2*10^{-11}$	23 часа	1,5 мин
9	$1,6*10^{-13}$	2,5 месяца	2 часа
10	$1,8*10^{-15}$	17 лет	6 суток
11	$1,9*10^{-17}$	1 669 лет	1,7 лет
12	$1,8*10^{-19}$	176 165 лет	176 лет

При условии, что наиболее эффективным методом является лобовое вскрытие, и программа, реализующая алгоритм взлома, может проверить миллион комбинаций в секунду, поиск правильной комбинации займет 12 дней. Тысяча машин, работающих параллельно, сможет восстановить пра-

вильную комбинацию за 20 минут, табл. 3. Анализируя данные табл. 2 – 4 можно утверждать, что ЦСУС СГС способна обеспечить закрытие информации с временной стойкостью, начиная уже с 8 каналов. Выбор уровня безопасности будет зависеть только лишь от назначения системы.

Выводы. ЦСУС СГС способна обеспечить безопасность информации с временной стойкостью, которая тем выше, чем больше каналов в системе, однако не исключает возможность навязывания противником старой информации, что требует дополнительных исследований по данной теме и, при необходимости, введения в систему дополнительных средств обеспечения имитозащиты.

Следует заметить, что наряду с повышением числа каналов в системе уплотнения растет усложнение программно-аппаратной части и требования к быстродействию цифрового процессора обработки сигналов.

ЛИТЕРАТУРА

1. *Рассомахин С.Г., Лученко С.В. Способ объединения сигналов с гребенчатыми спектрами // Изв. ВУЗов. Радиоэлектроника. – 1994. – 37, № 11. – С. 19 – 27.*
2. *Рассомахин С.Г., Горбачёв В.В., Ильченко М.Е. Метод формирования системы сигналов с гребенчатым спектром // Вестник науки и техники.– Х. – 2003.– Вып. 1. – С. 87.*
3. *Рассомахін С.Г., Горбачов В.В., Авдєєв В.Г. Енергетична ефективність сигналів з гребінчастим спектром // Вестник науки и техники. – Х. – 2003. – № 2 – 3(13 – 14). – 66 с.*
4. *Рассомахин С.Г., Лученко С.В. Поэтапный алгоритм расчета формирующих фильтров для цифровой системы объединения сигналов // Электронное моделирование. – 1985. – Вып. 6. – С. 35 – 36.*
5. *Лученко С.В. Синтез рекурсивных цифровых фильтров на основе метода условной оптимизации // Радиотехника. – 1993. – Вып. 102. – С. 21.*
6. *Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Изд. ТРИУМФ, 2002. – 816 с.*

Поступила 10.03.2004

***СОРОКА Леонид Степанович**, канд. техн. наук, профессор, ведущий научный сотрудник отдела научного центра при ХВУ. В 1974 году окончил ХВВКИУ. Область научных интересов – подсистемы передачи и отображения информации в АСУ.*

***ВОРОНОВ Дмитрий Николаевич**, канд. техн. наук, научный сотрудник научного центра при ХВУ. В 1995 году окончил ХВУ. Область научных интересов – защита информации в системах передачи данных.*

***СНИСАРЕНКО Андрей Георгиевич**, канд. техн. наук, с.н.с., начальник отдела научного центра при ХВУ. В 1985 году окончил ХВВКИУ РВ. Область научных интересов – подсистемы передачи информации в АСУ.*

***РАССОМАХИН Сергей Геннадиевич**, канд. техн. наук, доцент, ведущий научный*

сотрудник отдела научного центра при ХВУ. В 1980 году окончил ХВВКИУ РВ. Область научных интересов – исследование частотных характеристик сложных сигналов.