УДК 621.372.037.372

ОЦЕНКА ЗАЩИЩЕННОСТИ ОТ УТЕЧКИ БИТОВЫХ СИМВОЛОВ ПРИ ПЕРЕДАЧЕ РЕЧЕВЫХ СИГНАЛОВ В ЦИФРОВОЙ ФОРМЕ

д-р техн. наук, проф. В.К. ЖЕЛЕЗНЯК, Д.С. РЯБЕНКО
(Полоцкий государственный университет)

Исследуется оптимальный сигнал для оценки защищенности цифровых каналов утечки информации при передаче цифровых сигналов в виде битовых символов с основанием кода m. Предложен новый оптимальный метод оценки защищенности цифровых систем передачи сигналов в каналах утечки информации при воздействии шумов высокого уровня типа белого гауссовского шума, а также выбор и обоснование оптимального сигнала, который позволит оценить защищенность цифровых каналов утечки информации.

Сущность системного подхода к оценке эффективности защиты от утечки информации системами передачи заключается в обосновании целевых функций либо основных параметров, характеризующих количественно степень достижения поставленных целей защиты информации. Важнейшими являются информационные показатели (параметры), по которым оценивают степень достижения цели по нормируемым показателям. Нормируемые показатели (параметры) устанавливают степень их приближения к научно обоснованным эталонным показателям. Согласно системному подходу методологическая составляющая защиты информации должна включать методику, математическую модель, которые реализуют возможность обоснования измерительного сигнала и его обработку и позволяют оценить степень защиты по этому сигналу каналов утечки информации. Математическая модель на основании физической модели канала утечки информации и оптимального приемника, минимизирующего вероятность ошибки, и критерий наилучшей обработки аналоговых и цифровых сигналов при взаимном их преобразовании должны быть основой для экспериментальной оценки.

Речевой сигнал преобразуют в цифровую форму, последовательно подвергая трем преобразованиям [1]: дискретизации во времени, квантованию по уровню, преобразованию в цифровой код. Каждый из этих преобразований является источником полей рассеивания информационного сигнала.

В результате преобразований формируют токовые битовые символы речевого сигнала в виде двоичных чисел с двумя возможными символами «0» и «1» [1]. Такие сигналы в виде токовых битовых символов с основанием кода m показаны на рисунке 1. Импульсы тока представляют последовательность однополярных (рис. 1, *а*) или биполярных (рис. 1, *б*) прямоугольных импульсов с постоянными параметрами. При этом положительный импульс обычно соответствует передаваемому символу «1», а пропуск или отрицательный импульс – символу «0».

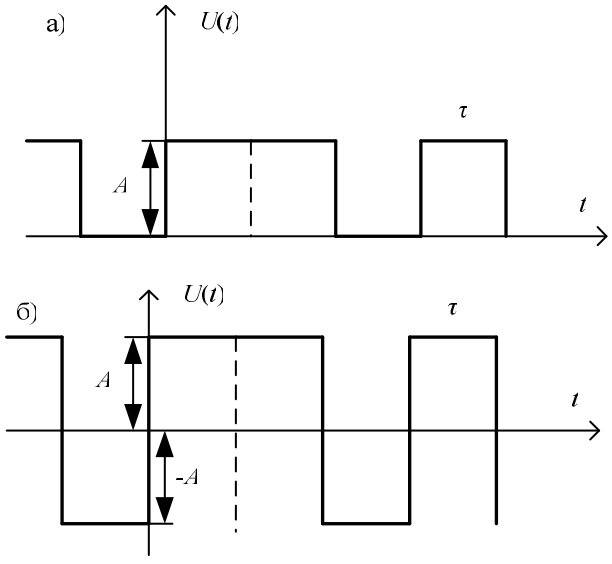

Рис. 1. Сигналы токовых битовых символов с основанием кода m

На рисунках 1 *а, б* приняты следующие обозначения: $U(t)$ – первичный сигнал в виде токовых битовых символов с основанием кода m; A – амплитуда импульсов; τ – длительность импульсов.

Основная часть. Защита сигналов цифровой манипуляции приобретает особую важность в связи с переходом на помехоустойчивые системы передачи информации. Особенностями каналов утечки цифровых сигналов являются их широкополосность, высокий уровень шумов и несимметричность. Это ограничивает возможности измерительных сигналов при оценке их защищенности в шумах высокого уровня.

Общепринятое состояние дискретных и цифровых сигналов, маскируемых помехой, решается их обнаружением, классификацией и оцениванием [2]. Дискретные и цифровые каналы передачи оценивают вероятностью ошибок [3].

Мерой оценки качества аналоговой системы передачи сигналов и данных является отношение сигнал/шум, для дискретных систем передачи – вероятность ошибки в символе [4].

При различном числе символов алфавит содержит $\log_2 M$ бит информации.

Для выбора сигнала важной характеристикой выступают количество символов M и их взаимная зависимость, т.е. энергия символов $E(1 - \rho)$. Вероятность ошибки является функцией коэффициента взаимной корреляции $\rho_{ij} = \rho$, отношения энергии бита E_b к спектральной плотности мощности шума N_0.

При $\rho = -1$ минимизируется вероятность ошибки только для $M = 2$.

При $M > 2$ коэффициент ρ для алфавита из M символов ограничен снизу величиной $-\frac{1}{M-1}$, в частности, если $\rho_{ij} = \rho$ для всех $i, j,\ i \neq j$, то $\rho \geq -\frac{1}{N-1}$.

Цель настоящей работы – обоснование и выбор оптимального сигнала для оценки защищенности каналов утечки информации цифровой модуляции для $M = 2$ и $M > 2$, т.е. многопозиционных, на основании нормированного показателя; повышение достоверности оценки защищенности информации при передаче ее в цифровой форме; анализ защищенности информации при ее передаче.

Впервые предложен и обоснован новый метод оценки защищенности от утечки цифровых речевых сигналов в виде битовых символов с основанием кода m.

Измерительным сигналом для оценки защищенности от утечки цифровых речевых сигналов в виде битовых символов с основанием кода m может служить периодическая последовательность прямоугольных импульсов (рис. 2, 3).

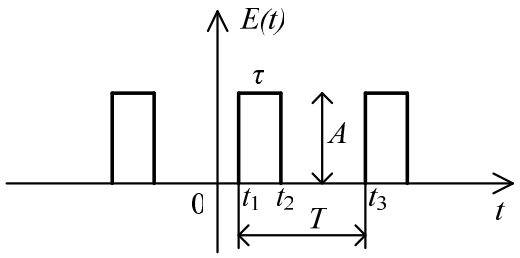

Рис. 2. Периодическая последовательность прямоугольных импульсов:
A_0 – амплитуда импульсов; t – длительность импульса;
T – период следования импульсов

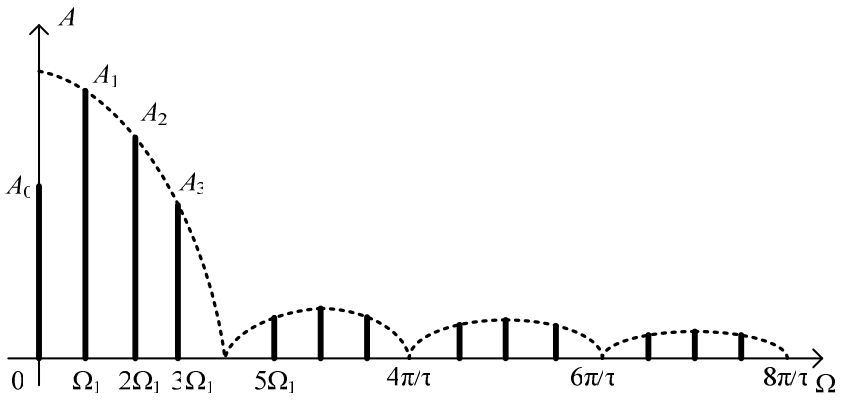

Рис. 3. Спектр периодической последовательности прямоугольных импульсов

Огибающая линия спектра определяется следующим образом [7]:

$$A(\Omega) = \frac{2A\tau}{T}\left(\frac{\sin\frac{\Omega\tau}{2}}{\frac{\Omega\tau}{2}}\right). \quad (1)$$

Амплитуды гармоник такого сигнала имеет вид [7]

$$A_n = \frac{2A\tau}{T}\cdot\frac{\sin\frac{n\Omega_1\tau}{2}}{\frac{n\Omega_1\tau}{2}}\cdot e^{-jn\Omega_1\left(t_1+\tau/2\right)}, n = 1,2,3... \quad (2)$$

Фазы гармоник зависят от выбора начала отсчета времени, которым определяется значение величины t_1 (рис. 4).

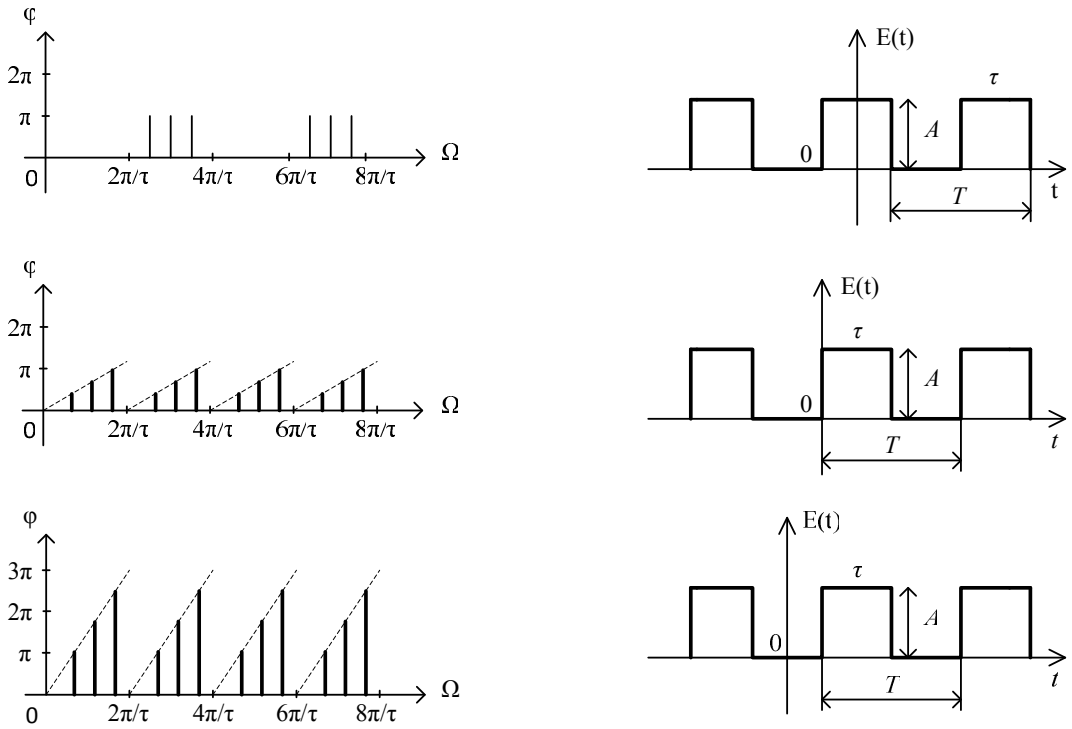

Рис. 4. Спектры фаз и их огибающие при различных началах отсчета времени [7]

Выражение для фазы гармоники [7] выглядит следующим образом:

$$\varphi_n = n\Omega_1\left(t_1+\tau/2\right)+(k-1)\pi, \quad (3)$$

где k – порядковый номер интервала $\Delta\Omega = 2\pi/\tau$ на шкале частот, отсчитываемый от нулевой частоты.

На основе этого предложено модулирующее колебание представить в виде последовательности N прямоугольных с одинаковыми энергиями импульсов (рис. 5) длительностью τ и периодом $T = 2\tau$ [7].

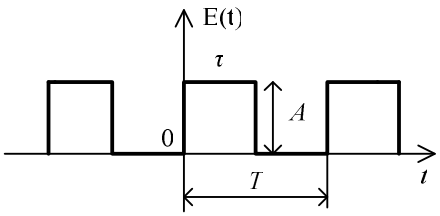

Рис. 5. Измерительный сигнал – последовательность прямоугольных импульсов (меандр)

Спектр амплитуд рассматриваемой последовательности импульсов изображен на рисунке 6.

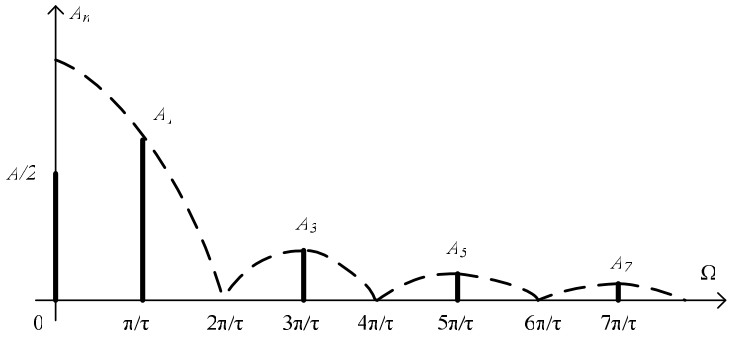

Рис. 6. Спектр последовательности прямоугольных импульсов (меандра) [5]

При условии, что $\Omega_1\tau = 2\pi\tau / T = \pi$, получено следующее выражение [7]:

$$f_1(t) = \frac{A}{2} + \frac{2A}{\pi}\sum_{n=1,3,5...}^{\infty}\frac{\sin\left(\frac{n\pi}{2}\right)}{n}\cos\left(n\Omega_1 t - \frac{n\pi}{2}\right) = \frac{A}{2} + \frac{2A}{\pi}\sum_{n=1,3,5...}^{\infty}\frac{\sin\left(n\Omega_1 t\right)}{n}. \quad (4)$$

В этом случае начальные фазы всех гармоник одинаковы и равны 0. Применение последовательности прямоугольных импульсов с одинаковыми энергиями импульсов длительностью τ и периодом $T = 2\tau$ в качестве измерительного сигнала позволяет обнаруживать и восстанавливать сигнал в шумах высокого уровня.

Оценка защищенности от утечки цифровых речевых сигналов в виде битовых символов с основанием кода m выполняется следующим образом: устанавливают источник испытательного сигнала в точке размещения источника полей рассеивания сигнала цифровой системой передачи информации; в точке приема полей рассеивания, образованных передаваемым сигналом, – оптимальный приемник. Далее испытательный сигнал в виде периодической последовательности однополярных прямоугольных импульсов с одинаковыми энергиями импульсов длительностью τ и периодом $T = 2\tau$ n-кратно подают на вход цифровой системы передачи информации. В точке приема полей рассеивания передаваемого сигнала принимают и обрабатывают сигнал, измеряют энергию бита E_b сигнала и спектральную плотность мощности шума N_0, вычисляют отношение сигнал/шум и пропускную способность $C_ц$ канала утечки информации, образованного полями рассеивания испытательного сигнала. Полученные значения данных параметров сравнивают с нормированными значениями и по допустимому порогу различия устанавливают защищенность информации от утечек.

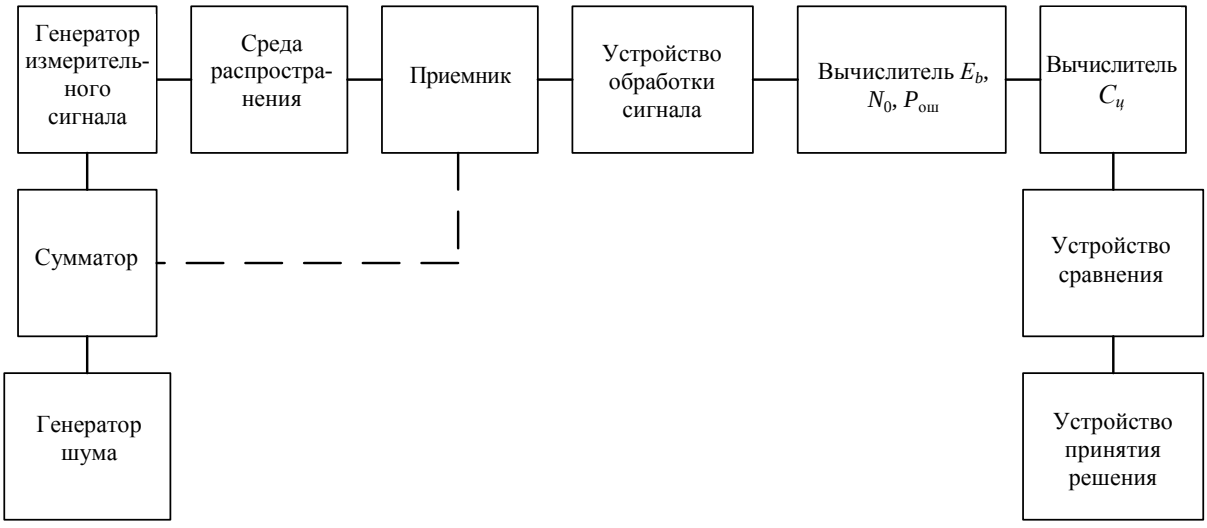

Рис. 7. Структурная схема устройства оценки защищенности цифровых речевых сигналов в виде битовых символов с основанием кода m

Сущность способа заключается в передаче информации цифровой системой передачи информации, а именно в моделировании передачи информации измерительным сигналом с одинаковыми энергиями импульсов длительностью τ и периодом $T = 2\tau$, приеме в точке приема полей рассеивания передаваемого сигнала, обработке путем n-кратного запоминания, накапливания, нормирования делением амплитуды накапливаемых импульсов на n, перемножения принятого измерительного сигнала с пачкой счетных импульсов, считывания. Далее измеряют энергию бита E_b сигнала и спектральную плотность мощности шума N_0, вычисляют параметры, необходимые для сравнения с нормированными.

Ниже рассматривается функционирование системы передачи информации и определение защищенности передаваемой информации, где в качестве передатчика используется источник измерительного сигнала, приемника – приемник сигнала вместе с элементами запоминания, накопления, нормирования, а линия связи в данном случае моделируется подачей на вход приемника просуммированного испытательного сигнала с белым гауссовым шумом. Устройство обработки такого сигнала (рис. 8) должно выполнять функцию восстановления полезного сигнала из шумов высокого уровня и содержать элементы запоминания, накопления и нормирования.

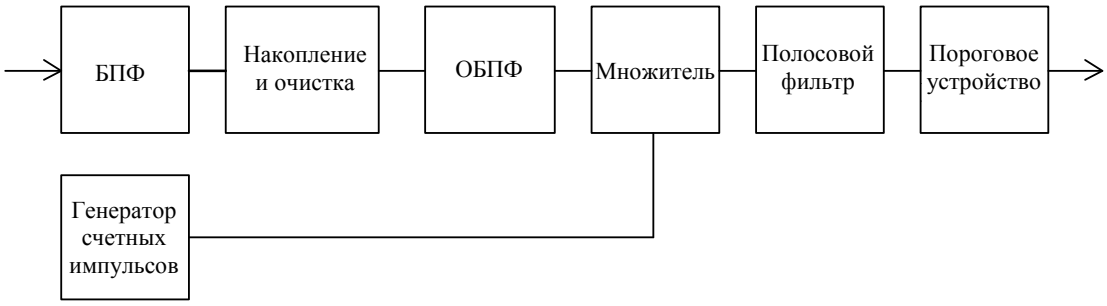

Рис. 8. Устройство обработки принимаемого сигнала

Принятый сигнал подается на вход устройства обработки сигнала, а именно в устройство, выполняющее функцию быстрого преобразования Фурье (БПФ), устройство n-кратного запоминания, накапливания, нормирования делением амплитуды накапливаемых импульсов на n, устройство, выполняющее функцию обратного быстрого преобразования Фурье (ОБПФ). После выполнения спектрального выделения гармоник принятого сигнала обнуления (очистки) шумовых составляющих между гармониками сигнала последовательность прямоугольных импульсов перемножается с пачкой счетных импульсов. Обнуляются шумовые составляющие между импульсными последовательностями с помощью полосового фильтра, и восстанавливается исходная импульсная последовательность с помощью порогового устройства.

Проводятся оценка превышения отношения сигнал/шум $h = \left(2E/N_0\right)^{1/2}$ на входе порогового устройства при его наличии над относительным уровнем порога $h_0 = z_0\left(N_0E/2\right)^{1/2}$ и сравнение с оценкой превышения отношения сигнал/шум по новому методу оценки защищенности от утечки битовых речевых сигналов в цифровой форме с основанием кода m.

Выражение для вероятности ошибочного приема бита имеет вид

$$P_{\text{ош}} = 0,5\exp\left(-0,5\frac{E_b}{N_0}\right), \tag{5}$$

где E_b / N_0 – отношение энергии бита к спектральной плотности мощности шума.

Далее производят определение и вычисление таких параметров сигнала, как вероятность ложного срабатывания, энергия сигнала, отношение сигнал/шум, пропускная способность. В сравнивающем устройстве производят вычисление отличия данных параметров от нормированных значений. По разнице между полученными при измерении параметрами и нормированными значениями параметров в устройстве принятия решения производят оценку защищенности информации, передаваемой по цифровым системам передачи информации.

Использование предлагаемого способа позволит получить повышение достоверности оценки защищенности информации при передаче ее в цифровой форме и проанализировать защищенность информации при ее передаче в виде битовых символов с основанием кода m.

Заключение. Выбрана и обоснована предпочтительная и актуальная альтернатива применительно к сложной решаемой задаче оценки защищенности цифровой речевой информации, передаваемой в виде битовых символов с основанием кода m. Метод сигнала в виде последовательности прямоугольных импульсов с одинаковыми энергиями импульсов, длительностью τ и периодом $T = 2\tau$ для оценки защищенности от утечки битовых символов при передаче цифровой речевой информации повышает точность оценки и восстановления измерительного сигнала за счет возможности восстановления сигнала по единичным гармоникам в спектре принимаемого сигнала.

ЛИТЕРАТУРА

1. Гольдберг, Л.М. Цифровая обработка сигналов: справочник / Л.М. Гольдберг, Б.Д. Матюшкин, М.Н. Поляк. – М.: Радио и связь, 1985. – 312 с.
2. Блох, Э.Л. Модели источника ошибок в каналах передачи цифровой информации / Э.Л. Блох, О.В. Попов, В.Я. Турин. – М.: Связь, 1971. – 312 с.
3. Стиффлер, Дж.Дж. Теория синхронной связи / Дж.Дж. Стиффлер; пер. с англ. Б.С. Цыбакова под ред. Г.М. Габидулина. – М.: Связь, 1975. – 488 с.
4. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр: пер. с англ. – 2-е изд. – М.: Издат. Дом «Вильямс», 2007. – 1104 с.
5. Витерби, А.Д. Принципы цифровой связи и кодирования / А.Д. Витерби, Дж.К. Омура; пер. с англ. под ред. К.Ш. Зигангирова. – М.: Радио и связь, 1982. – 536 с.
6. Железняк, В.К. Основы теории модулированных колебаний: учеб. пособие / В.К. Железняк, С.В. Дворников. – СПб.: ГУАП, 2006. – 160 с.
7. Фельдбаум, А.А. Теоретические основы связи и управления / А.А. Фельдбаум. – М.: 1963. – 932 с.

Поступила 04.03.2014

ESTIMATION OF SECURITY FROM BIT SYMBOL LEAKAGE DURING DIGITAL VOICE DATA TRANSMISSION

V. ZHELEZNYAK, D. RYABENKO

Optimal signal for estimation of security of digital information leakage channels during transmission of digital signals as bit symbols with code base m is analyzed. New optimal method of estimation of security of signal transmission digital systems in information leakage channels under the influence of high level noise like white Gaussian noise was suggested. Choice and substantiation of optimal signal which allows to evaluate the security of digital channels of information leakage was offered.