УДК: 621.391.7

А. И. ЦОПА, д-р техн. наук

ОЦЕНКА ВЛИЯНИЯ КОДИРОВАНИЯ И СКРЕМБЛИРОВАНИЯ СИГНАЛА НА ЗАЩИЩЕННОСТЬ СИСТЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Введение

Современные исследования в области безопасности систем передачи информации (СПИ) ведутся в трех основных направлениях. Во-первых, идет работа по разработке защищенных протоколов на верхних уровнях модели *OSI* (*Open System Interconnect*) и на уровне приложений, базирующихся на криптографических методах преобразования информации [1]. Во-вторых, ряд исследователей ведут работы по развитию информационно-теоретического подхода в оценке безопасной связи Шеннона, с целью определения фундаментальных пределов безопасной связи по беспроводным каналам передачи информации [2]. В частности, большое внимание уделяется концепции отводного канала (*wiretap channel*) А. Вайнера [3, 4]. В третьих, в последнее время повысился интерес к методам физического уровня обеспечения безопасности связи, которые используют для повышения защищенности характеристик проводных и беспроводных каналов передачи информации [5].

Информационные методы защиты информации, которые применяются сейчас при создании защищенных беспроводных систем связи, разработаны без учета физических параметров сетей, где они используются. Однако параметры кодирования, модуляции сигнала и физические характеристики беспроводных каналов содержат специфическую информацию, которая может быть использована для повышения защищенности информации при ее передаче по каналам связи.

Для большинства систем связи вероятность битовой ошибки P_b (*BER*) используется, чтобы показать надежность (*reliability*) системы в отношении приема сигнала и декодирования информации. Например, если *BER* системы $P_b = 10^{-5}$, можно сказать, что это надежная система передачи информации (конечно, в зависимости от используемого приложения и вида передаваемой информации), а с другой стороны, если $P_b = 0,5$, то система является явно неработоспособной, так как при приеме и декодировании каждого бита информации мы будем иметь 50 % вероятности того, что это могут быть неправильные решения. Эта общепринятая мера надежности и качества системы связи приводит нас к новому определению защищенности (*security*) системы, которые можем использовать в наших дальнейших исследованиях систем с отводным каналом ОК [6].

Цель работы – оценка влияния различных методов кодирования, скремблирования и модуляции сигнала на характеристики энергетической защищенности системы передачи информации с отводным каналом.

Основная часть

При проведении численных исследований будем опираться на обобщенную структуру модели СПИ с отводным каналом, представленную на рис. 1.

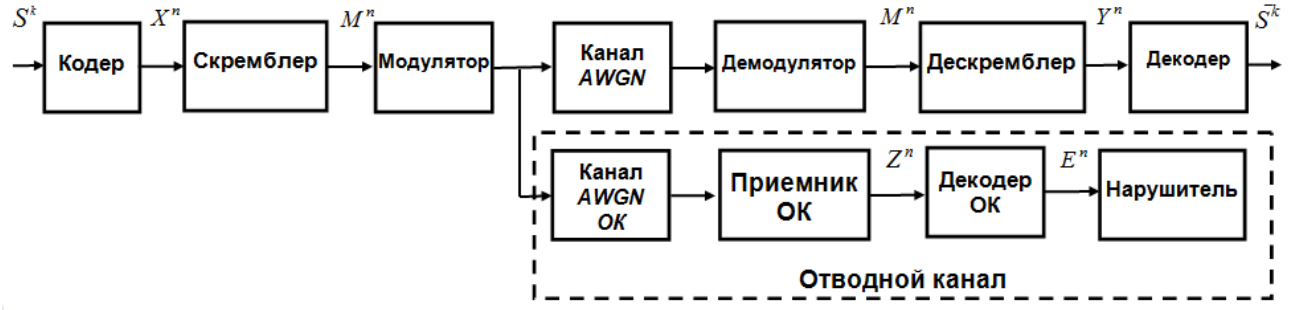

Рис. 1

Канал передачи информации от источника до получателя информации называется основным, или легитимным каналом связи *(main channel)*. Канал отвода от передатчика легитимного канала к приемнику незаконного потребителя (нарушителя) является отводным каналом ОК *(wiretap channel)*. Легитимный канал СПИ включает в себя кодер, скремблер, модулятор, канал связи с аддитивным белым гауссовским шумом (*AWGN*), демодулятор, дескремблер и декодер. Нарушитель, используя свой приемник-обнаружитель и декодер, пытается перехватить информацию, которая передается в легитимном канале связи.

Одним из критериев качества работы СПИ является зависимость $P_b = f(E_b / N_O)$ – вероятность появления битовых ошибок как функция отношения энергии сигнала, приходящейся на один бит E_b, к спектральной плотности мощности аддитивного белого гауссовского шума N_0. Удобство использования отношения E_b / N_0 связано с возможностью сравнивать производительность и помехозащищенность систем связи на битовом уровне. Это важно для цифровых систем, поскольку сигнал может иметь произвольное *n*-битовое значение.

Приведенные в работе [7] выражения позволяют оценить вероятности битовой ошибки в основном канале связи $P_b^{Л}$ от отношения сигнал/шум (*SNR*) для различных методов передачи информации в канале связи, при этом для обеспечения качества передачи информации это значение должно быть ниже определенного порога $\left(P_b^{Л}\right)_{\max}$, который задается требованиями к передаче определенного вида информации (данные, речь, видео и т.п.), т.е.

$$P_b^{Л} \le \left(P_b^{Л}\right)_{\max}. \tag{1}$$

В то же время для обеспечения защищенности канала СПИ вероятность битовой ошибки в отводном канале $\left(P_b\right)_O$ от отношения сигнал/шум должна быть больше определенного порога $\left(P_b^{O}\right)_{\min}$ (близкого к 0,5), т.е.

$$P_b^{O} \ge \left(P_b^{O}\right)_{\min}. \tag{2}$$

Выполнение неравенств (1) и (2) обеспечивается соответствующими энергетическими соотношениями (E_b / N_o) в основном и отводном каналах, а разность этих значений является энергетическим критерием уязвимости системы связи от перехвата S_g, который определяется исходя из соотношений

$$\begin{cases} P_b^{Л} = f\left[\left(\dfrac{E_b}{N_O}\right)_{Л}\right], \\ P_b^{O} = f\left[\left(\dfrac{E_b}{N_O}\right)_{O}\right], \\ S_g = \left(\dfrac{E_b}{N_O}\right)_{Л} - \left(\dfrac{E_b}{N_O}\right)_{O}, [дб]. \end{cases} \tag{3}$$

Для примера рассмотрим качественную характеристику зависимости $P_b = f(E_b / N_0)$, приведенную на рис. 2. Здесь можно выделить три характерных участка, которые определяют защищенность системы связи. На участке I (*security region*) обеспечивается полная защищенность канала связи от перехвата сообщений, на участке II защищенность канала связи может быть обеспечена определенными мерами защиты информации на физическом уровне, а на участке III (*reliable region*) защита информации может быть достигнута в основном только информационными криптографическими методами.

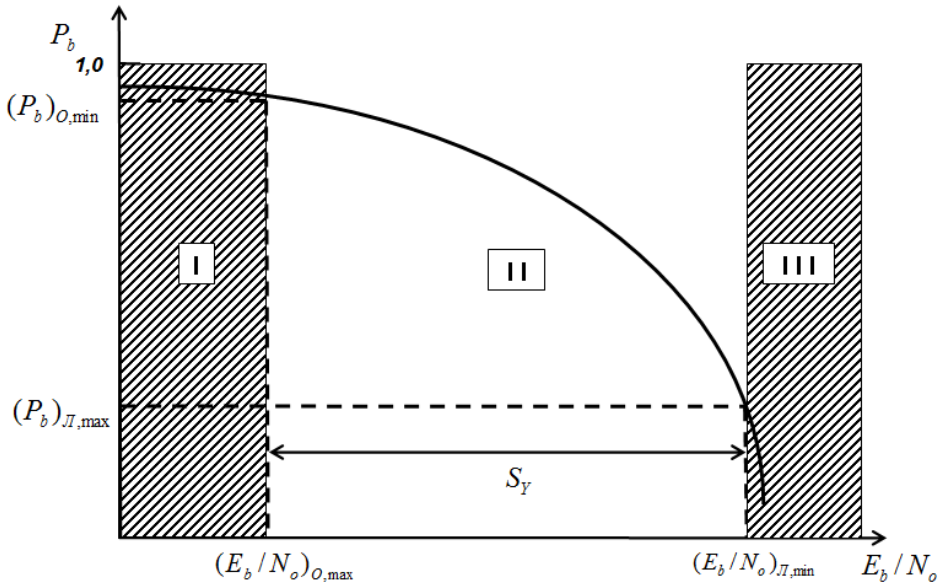

Рис. 2

Из рис. 2. также видно, чем круче склон характеристики $P_b = f(E_b/N_0)$, тем меньше зона уязвимости системы связи, которая оценивается энергетическим критерием уязвимости системы связи от перехвата информации S_g (*security gap*). Решение задачи уменьшения этой зоны перехвата информации, т.е. минимизации $\left[S_g\right]_{\min}$, как раз и связано с решением проблемы защиты информации на физическом уровне модели *OSI*.

Используя критерий S_g, можно оценить влияние тех или иных характеристик системы связи, параметров распространения сигнала и методов обработки сигналов (кодирования, скремблирования и модуляции сигнала) на физическом уровне на защищенность ВСС.

Учитывая, что современные системы передачи информации ориентированы на передачу мультимедийной информации в каналах связи с использованием пакетных протоколов передачи информации, то целесообразно использовать для оценки показателей качества и защищенности СПИ вероятность пакетной ошибки *PER* (*Packet Error Rate*), которая связана с параметром битовой ошибки *BER* следующим соотношением [9]

$$PER = (1-(1-BER)^L, \tag{4}$$

где L – длина информационного пакета.

Одним из способов обработки двоичного потока без изменения скорости передачи в канале СПИ является *скремблирование* (*scramble* – перемешивание). Это разновидность кодирования информации с целью получения свойств случайной последовательности цифрового потока и улучшения спектральных, статистических характеристик сигнала. Наиболее распространенный способ скремблирования – смешивание сигнала с генератором псевдослучайных чисел. Скремблер реализует логическую операцию суммирования по модулю два исходного и псевдослучайного двоичного сигналов. Дескремблер выделяет из принятой последовательности исходную информационную последовательность. Основным узлом скремблера является генератор псевдослучайной последовательности (ПСП), выполненный в виде линейного *n*-каскадного регистра с обратными связями (*Linear Feedback Shift Registers*), который формирует последовательность максимальной длины 2^n–1. За счет операции скремблирования улучшается синхронизация цифрового потока, выравнивается энергетический спектр передаваемого сигнала, что способствует уменьшению уровня перекрестных помех, наводимых на соседние витые пары проводов кабеля линии связи и уменьшается излучение из кабеля для проводных СПИ. Недостатком устройства скремблера является размножение ошибок, которые могут возникнуть при передаче сигнала по линии связи.

Рассмотрим сначала случай передачи информации по каналу связи *AWGN* сигналов с использованием модуляции *BPSK* (*Binary Phase Shift Key*), для которого вероятности битовой P_b и фреймовой P_f ошибки можно представить известными выражениями [9]

$$\begin{cases} P_b^{BPSK} = 1/2 \cdot erfc\left(\sqrt{\dfrac{E_b}{N_o}}\right), \\ P_f = 1-(1-P_b)^k, \end{cases} \tag{5}$$

где k – размер фрейма в цифровом потоке данных [*бит*]; $erfc$ – функция ошибок дополнительная (*error function complement*) в среде MatLab.

В работе [10] показано, что при идеальном скремблировании (*perfect scrambling*) частота ошибок при дескремблировании равно половине фреймовых ошибок в канале связи:

$$P_b^{PS} = \frac{1}{2}P_f = \frac{1}{2}\left\{1-\left[1-1/2\cdot erfc\left(\sqrt{\frac{E_b}{N_o}}\right)\right]^k\right\}. \tag{6}$$

С учетом эффекта размножения битовых ошибок при скремблировании качество скремблирования цифрового потока, зависящее от разрядности скремблера w, может быть представлено выражением

$$P_b^S(w) = \frac{1}{2}P_f \cdot \left[1-\left(1-2\frac{P_b}{P_f}\right)\right]^w. \tag{7}$$

Для примера целесообразно рассмотреть типичный случай, когда длина пакета $k = 1500$ *бит*. На рис. 3 представлены результаты численного моделирования, проведенные в среде MatLab, при нескремблированной передаче сигналов, при идеальном скремблировании и при различной разрядности скремблера $w \in [1, 60, 150, k]$.

Как видно из рис. 3, при нескремблированной передаче сигнала вероятность ошибок мала даже при низких значения *SNR*. При увеличении разрядности скремблера w вероятность ошибок повышается, приближаясь к уровню 0,5, при одновременном увеличении *SNR*. Увеличивается также крутизна наклона кривой, достигая максимального значения при идеальном скремблировании $w = k$.

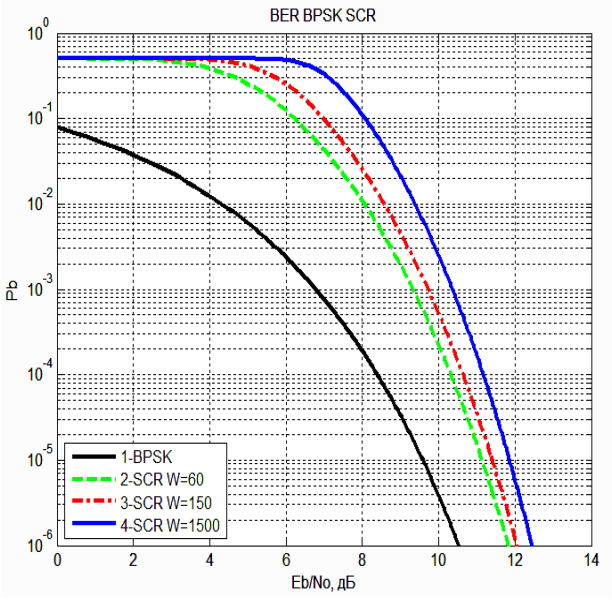

Рис. 3

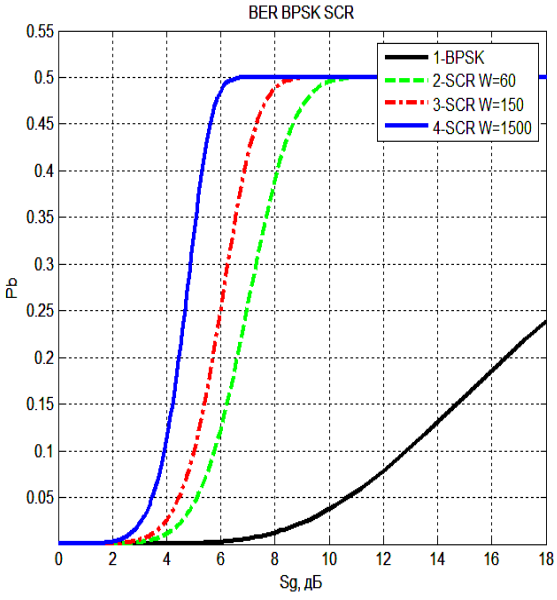

Рис. 4

Для сравнения различных методов скремблирования предположим, что в основном канале связи информация передается с вероятностью битовой ошибки $P_b^{Л} = 10^{-5}$ и это соответствует отношению сигнал/шум в канале $(E_b / N_0)_{Л}$. Тогда, используя это значение $(E_b / N_0)_{Л}$, можно оценить вероятность битовой ошибки в отводном канале P_b^O как функцию S_g:

$$P_b^O = 1/2 \cdot erfc\left(\sqrt{\frac{\left[erfcinv\left(2 \cdot 10^{-5}\right) \right]^2}{S_g}} \right), \tag{8}$$

где $erfcinv$ – обратная дополнительная функция ошибок (*inverse complementary error function*) в среде MatLab.

На рис. 4 приведены графики этой функции $P_b^O(S_g)$ в зависимости от разрядности скремблера w. Увеличение разрядности скремблера w приводит к уменьшению зоны уязвимости S_g на 4 – 6 *дБ* по сравнению с передачей нескремблированного цифрового потока. Также наблюдается увеличение наклона кривой, а значит и рост вероятности ошибок в отводном канале нарушителя к максимальному пределу $P_b^O = 0{,}5$.

Используя предложенную выше методику, можно определить размер зоны уязвимости СПИ S_g при применении в канале связи многоуровневых видов модуляции *M-QAM*, для которых вероятность битовой ошибки определяется выражением [11]

$$P_b^{QAM} = 2 \cdot \left(1 - \frac{1}{\sqrt{M}}\right) \cdot erfc\left(\sqrt{\frac{3\log M}{2(M-1)} \cdot \frac{E_b}{N_o}} \right), \tag{9}$$

где M – уровень модуляции *QAM*.

На рис. 5 представлены результаты численного моделирования зависимости P_b^{SQAM} от *SNR* при передаче сигналов с модуляцией 16-*QAM* по основному каналу связи *AWGN* при нескремблированной передаче сигналов и при различной разрядности скремблера $w \in [1, 60, 500, k]$. При увеличении разрядности скремблера w вероятность ошибок также повышается, приближаясь к уровню 0,5. Увеличивается также крутизна наклона кривой, достигая максимального значения при идеальном скремблировании $w = k$.

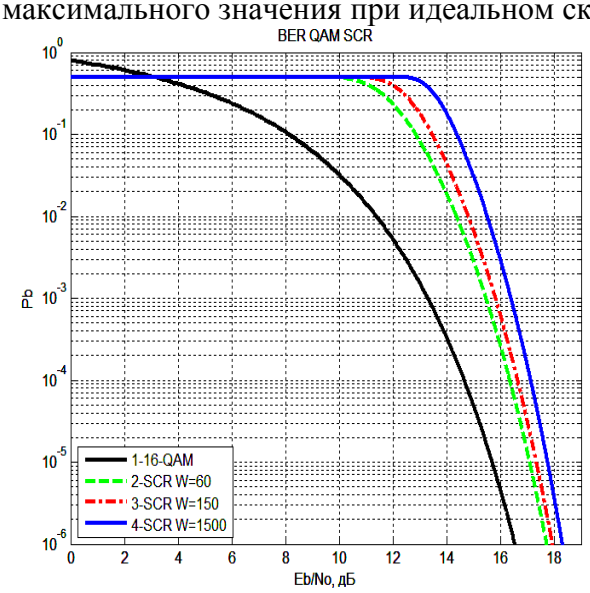

Рис. 5

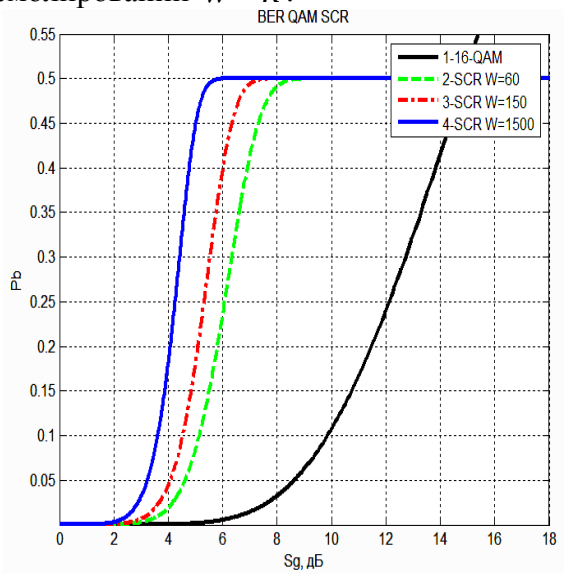

Рис. 6

На рис. 6 представлены результаты численного моделирования вероятности битовой ошибки в отводном канале P_b^O как функцию S_g при нескремблированной передаче сигналов с модуляцией *16-QAM* по основному каналу связи *AWGN* и при различной разрядности скремблера w. Результаты показывают, что увеличение разрядности скремблера вплоть до идеальной ($w = k$) приводит к уменьшению зоны уязвимости S_g.

Увеличение уровня модуляции сигнала *M* в основном канале связи приводит к уменьшению зоны уязвимости S_g на 4 – 6 *дБ* для нескремблированного цифрового потока и на 2 – 3 *дБ* при идеальном скремблировании. Также увеличивается наклон кривой и рост вероятности ошибок в ОК к пределу $P_b^O = 0{,}5$.

Далее рассмотрим случай передачи информации по основному каналу связи *AWGN* сигналов при применении в кодере легитимного канала линейного блочного кодирования для коррекции ошибок в СПИ. При использовании кодовой схемы с жестким декодированием, демодулятор принимает решение по каждому из принятых символов кода и на вход декодера поступают кодовые комбинации в виде двоичных символов. Если в процессе декодирования произошла ошибка в приеме кодового слова, то в блоке из *k* декодированных символов часть их будет принята с ошибками, а другая часть без них.

Вероятность фреймовой ошибки P_f для блокового кода структуры (*n, k*), исправляющего *t* ошибок, можно определить, с учетом вероятности битовой ошибки в канале связи P_b, используя следующие выражения [12]:

$$\begin{cases} P_b^{COD} = 1/2 \cdot erfc\left(\sqrt{\dfrac{E_b}{N_o} \cdot \dfrac{k}{n}}\right), \\ P_f = \sum\limits_{i=t+1}^{n} C_n^i \cdot P_b^i \cdot (1-P_b)^{n-i}, \end{cases} \tag{10}$$

где n – размер кодового слова; k – число информационных символов в кодовой комбинации; t – количество исправляемых ошибок; P_b – вероятность битовой ошибки в канале связи; $r = k/n$ – кодовая скорость; C_n^i – биноминальный коэффициент, определяемый выражением $C_n^i = n!/i!(n-i)!$.

Используя выражения (7) и (10), можно провести численное моделирование для различной структуры блочного кодера БЧХ (*n, k*), исправляющего *t* ошибок.

На рис. 7, 8 представлены результаты численного моделирования зависимости $P_b(E_b/N_0)$ и $P_b(S_g)$ при различной структуре кодера БЧХ и его возможностей по коррекции ошибок: 1 – БЧХ(63, 30), $t = 6$; 2 – БЧХ(127, 64), $t = 10$; 3 – БЧХ(255, 123), $t = 19$.

Применение блокового кодирования БЧХ (скорость кодирования во всех случаях *r*=½) приводит к значительному уменьшению зоны уязвимости S_g на 2 – 3 *дБ* по сравнению с сопримененением скремблирования и увеличением уровня модуляции. Также увеличивается наклон кривой, а значит и рост вероятности ошибок в отводном канале нарушителя к максимальному пределу $P_b^O = 0{,}5$.

Представленная выше методика оценки уровня защищенности СПИ на физическом и канальном уровнях модели взаимодействия *OSI* с использованием понятия энергетической зоны уязвимости системы от перехвата S_g, позволяет проводить сравнительную оценку различным методам модуляции, кодирования и скремблирования сигнала в канале связи, с целью обеспечения требований защиты информации.

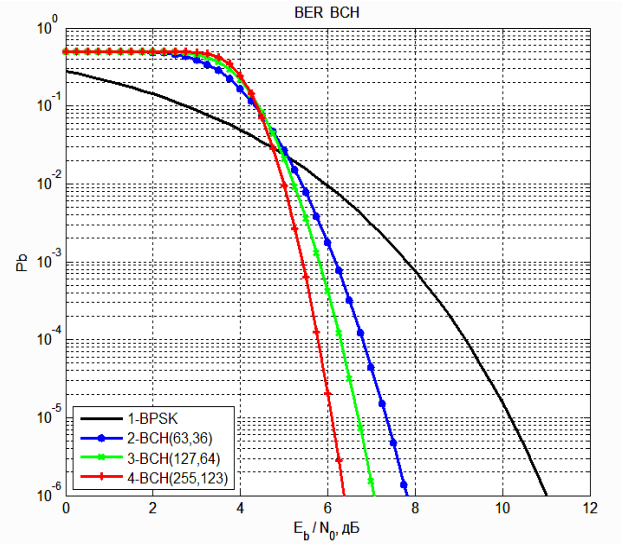

Рис. 7

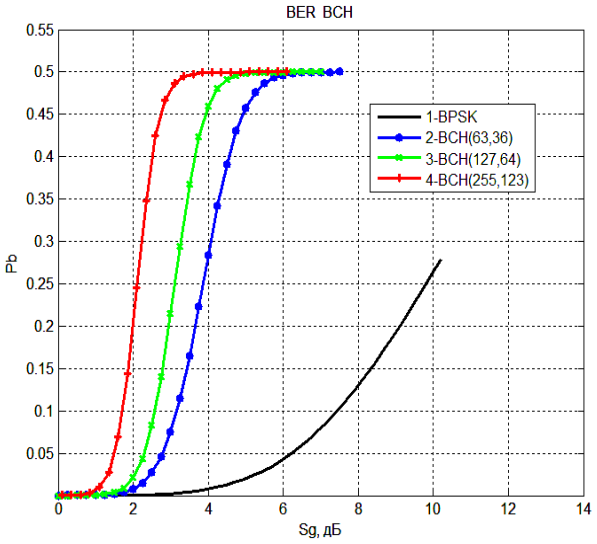

Рис. 8

Выводы

1. В работе рассмотрены особенности применения информационно-теоретических методов для оценки параметров защищенности систем передачи информации на канальном и физическом уровне модели взаимодействия систем связи *OSI*.

2. Рассмотрены примеры оценки защищенности СПИ с отводом для различных видов модуляции (*BPSK*, 16-*QAM*), скремблирования и блочного кодирования БЧХ(*n*, *k*) сигналов в канале связи. Показана универсальность и эффективность предложенного метода оценки защищенности на основе параметра вероятности битовой ошибки в основном и отводном каналах.

3. Получены сравнительные оценки защищенности СПИ при различных методах обработки цифрового потока на основе критерия энергетической уязвимости системы S_g.

Список литературы: 1. *Mao, B.* Современная криптография. Теория и практика. – М. : Вильямс, 2005. – 768 с. 2. *Yingbin Liang, H. Vincent Poor, Shlomo Shamai.* Information Theoretic Security. – Boston : Publishers Inc, 2009. – p. 233. 3. *Wyner A. D.* The wire-tap channel // Bell System Technical Journal. – 1975. – Vol. 54, № 8. – pp. 1355-1387. 4. *Csisz´ar I., K¨orner J.* Broadcast Channels with Confidential Messages // IEEE Trans. Inform. Theory. –1978. –Vol. 24, № 3. – pp. 339–348. 5. *R. Liu and W. Trappe.* Securing Wireless Communications at the Physical Layer. New York: Springer, 2010. 6. *Методы* прогнозирования защищенности ведомственных систем связи на основе концепции отводного канала ; под ред. А. И. Цопы, В. М. Шокало. – Харьков : КП «Городская типография», 2011. – 502 с. 7. *Цопа, А. И.* Критерии оценки и пути повышения защищенности каналов связи цифровых систем передачи информации на физическом уровне // Радиотехника. – 2010. – Вып. № 161. – С. 87-96. 8. *Волков, Л. Н., Немировский, М. С., Шимаков, Ю. С.* Системы цифровой радиосвязи: базовые методы и характеристики. – М. : Эко-Трендз, 2005. – 392 с. 9. *Слепов, Н. Н.* Оценка показателей ошибок цифровых линий связи // Электроника: Наука, Технология, Бизнес. – 2002. – № 5. – С. 22-31. 10. *Шевкопляс, Б. В.* Скремблирование передаваемых данных // Схемотехника. – 2004. – №12. – С. 24 – 27. 11. *Волков, Л.Н., Немировский, М.С., Шинаков, Ю.С.* Системы цифровой радиосвязи. Базовые методы и характеристики. – Эко-Трендз, 2005. – 392 с. 12. *Золотарев, В. В., Овечкин, Г. В.* Помехоустойчивое кодирование. Методы и алгоритмы : справочник. – М. : Горячая линия – Телеком, 2004. – 126 с.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 09.11.2013