УДК 621.391.7

Д. Г. ГАНШИН, В. В. МАСЛИЙ, канд. техн. наук, А. И. ЦОПА, д-р техн. наук

ИССЛЕДОВАНИЕ ЗАЩИЩЕННОСТИ СИСТЕМЫ СВЯЗИ С МНОГОЧАСТОТНЫМИ СИГНАЛАМИ

Введение

При создании производительных ведомственных систем связи (ВСС) одним из основных требований, предъявляемым к таким системам, является обеспечение не только высокой производительности, но и защищенности этих систем [1, 2]. Несмотря на большое количество разработанных протоколов защиты информации на верхних уровнях семиуровневой модели взаимодействия открытых систем *OSI (Open System Interconnect)* эффективность данных протоколов значительно снижается при передаче мультимедийной информации [3]. В связи с увеличением объемов мультимедийного трафика в ВСС появилась необходимость искать новые пути повышения защищенности каналов связи не только на информационном, но и на физическом (энергетическом) уровне модели *OSI*, с использованием концепции отводного канала (*Wiretap Channel*) [4, 5].

Учитывая то, что обычно отсутствуют данные о технических средствах нарушителя, а место подключения к легитимному каналу неизвестно, то наиболее эффективным методом анализа защищенности систем связи является моделирование отводного канала и возможных условий перехвата информации. При этом полное моделирование всех процессов преобразования информации от входа до выхода системы позволяет оценить не только параметры энергетической, но структурной защищенности канала связи.

В современных системах связи, как в проводном (*xDSL*), так и беспроводном сегментах (*Wi-Fi, WiMAX*) ВСС, широко применяются цифровые системы передачи информации (ЦСПИ), основанные на использовании многочастотных сигналов с дискретной мультитоновой модуляцией *DMT* (*Discreet Multi-Tone Modulation*) и с ортогональным частотным мультиплексированием каналов *OFDM (Orthogonal Frequency-Division Multiplexing).* Популярность таких систем связана с высокой скоростью передачи информации, хорошей работой в частотно-селективных каналах связи и эффективным использованием методов быстрого предобразования Фурье *FFT (Fast Fourier Transform)* при формировании и приеме многочастотных сигналов [6].

Цель работы – усовершенствование системной модели отводного канала и оценка защищенности системы связи с многочастотными сигналами на физическом уровне модели *OSI*.

Основная часть

Рассмотрим обобщенную структурную схему модели отводного канала для многочастотных сигналов *MCS* (*Multi-Carrier Signal*), которую можно представить в виде N независимых параллельных подканалов (рис. 1). Абонент ***A*** передает по каналу связи конфиденциальное сообщение X^n (длиной n), используя систему передачи информации с на N несущих частотах $f_1 ... f_n$, где уровень модуляции *QAM* b_i определяется отношением сигнал/шум $SNR_{M\,i}$ для каждой несущей частоты f_i. Абонент ***B*** принимает информацию Y^n. Передатчик абонента ***A*** и приемник абонента ***B*** образуют легитимный канал связи. Нарушитель ***E*** пытается перехватить информацию Z^n, используя для этого многоканальный приемник-обнаружитель.

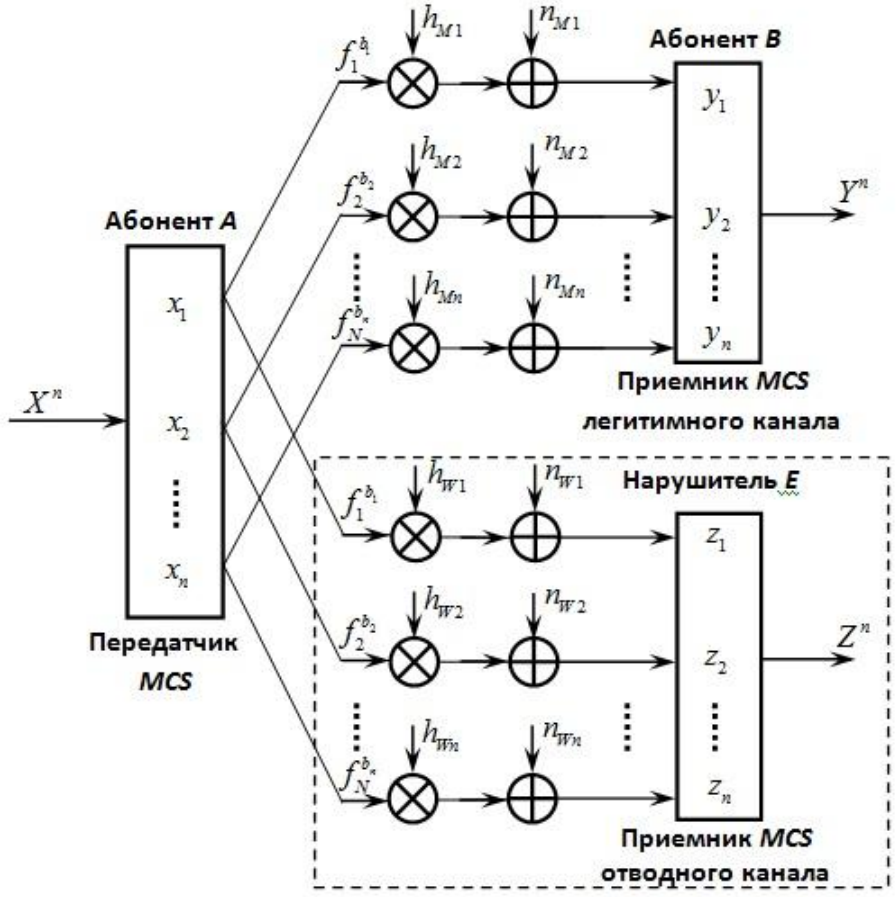


Рис. 1. Обобщенная структурная схема модели отводного канала системы связи с многочастотными сигналами

Для данного случая классическая системная модель отводного канала [7] может быть модифицирована и для каждой i-й несущей частоты в пределах $1 \le i \le N$ может быть представлена для принимаемых сигналов y_i абонентом ***B*** и z_i нарушителем ***E*** в следующем виде:

$$\begin{aligned} y_i &= h_{Mi} \cdot x_i + n_{Mi}, \quad i = 1,2...N; \\ z_i &= h_{Wi} \cdot x_i + n_{Wi}, \quad i = 1,2...N, \end{aligned} \tag{1}$$

где x_i – передаваемый сигнал абонентом ***A***; h_{Mi}, h_{Wi} – канальные коэффициенты, учитывающие затухание соответственно в легитимном и отводном каналов для каждой i-й несущей частоты легитимного и отводного каналов; n_{Mi}, n_{Wi} – характеристика шума аддитивного белого Гауссовского шума (с распределением σ^2) соответственно на каждой i-й несущей частоте легитимного и отводного каналов; N – максимальное количество несущих частот.

Задача защищенной системы связи обеспечить легальному пользователю возможность восстановления сообщения Y^n с малой вероятностью ошибки (вероятностью битовой ошибки P_b), при передаче этого сообщения по независимым параллельным каналам

$$P_b = \Pr\left\{ X^n \neq Y^n \right\} = \prod_{i=1}^{N} \Pr\left\{ x_i \mid y_i \right\} \le \varepsilon. \tag{2}$$

В то же время нарушитель при перехвате многочастотного сигнала не может получить сколько-нибудь значительной информации о сообщении X^n:

$$\frac{1}{n} I\left(X^n \wedge Z^n\right) \le \varepsilon. \tag{3}$$

При $\varepsilon = 0$ система связи обеспечивает конфиденциальность передачи информации и защиту информации в канале связи от перехвата. Одним из критериев оценки защищенности системы связи (рис. 1) может служить секретная производительность C_S [8], определяемая как разность максимальных скоростей передачи информации в легитимном C_M и отводном C_M каналах связи:

$$C_S(P^A) = \sum_{i=1}^{N} \left[\underbrace{\log_2\left(1 + \frac{\alpha_{Mi} \cdot P_i^A}{\sigma^2}\right)}_{C_M} - \underbrace{\log_2\left(1 + \frac{\alpha_{Wi} \cdot P_i^A}{\sigma^2}\right)}_{C_W} \right]^+ \text{ [бит/с]}, \tag{4}$$

где P_i^A – мощность передаваемого сигнала абонентом A для каждой i-й несущей частоты, при условии постоянной средней мощности передатчика $\sum_{i=1}^{N} P_i^A \le P$; $\alpha_{Mi} = |h_{Mi}|^2$, $\alpha_{Wi} = |h_{Wi}|^2$ – коэффициенты затухания сигнала в легитимном и отводном каналах для каждой i-й несущей частоты; N – максимальное количество несущих частот; $[a]^+ = \max(0, a)$.

Важной характеристикой защищенности системы связи является также вероятность обнаружения $P_{об}$, которая определяется как

$$P_{об}(R_S) = P(C_S \langle R_S) \tag{5}$$

где $R_S \rangle 0$ – скорость передачи информации, при которой система связи считается секретной (не обнаруживается).

Тогда с учетом [7] вероятность обнаружения системы связи с многочастотными сигналами можно представить в виде

$$P_{об} = \prod_{i=1}^{N} \left[1 - \frac{SNR_{Mi}}{SNR_{Mi} + 2^{R_{Si}} SNR_{Wi}} \cdot e^{\left(-\frac{2^{R_{Si}} - 1}{SNR_{Mi}}\right)} \right], \tag{6}$$

где SNR_{Mi} – отношение сигнал/шум на i-й несущей частоте легитимного канала; SNR_{Wi} – отношение сигнал/шум на i-й несущей частоте отводного канала; R_{Si} – секретная скорость передачи информации на i-й несущей частоте.

Учитывая то, что в каналах ВСС передается мультимедийная информация с высокими требованиями к качеству передачи информации, в работе [3] предложено использовать вероятность битовой ошибки $P_b = f(SNR)$ в легитимном и отводном каналах для оценки защищенности системы связи на физическом уровне модели *OSI*. Сравнительный анализ этих характеристик позволяет оценить уязвимость системы связи от перехвата и позволяет определить степень влияния параметров физического уровня системы связи (мощности передатчика, количество поднесущих частот, вида модуляции, методов обработки сигналов и т.п.) на ее помехозащищенность и скрытность.

Используя предложенную выше обобщенную модель системы связи с отводным каналом, проведем анализ защищенности системы с *DMT* модуляцией, которая широко используется в технологиях *ADSL* и *VDSL*, являющихся основой при построении проводных сегментов защищенных ВСС.

На рис. 2 представлена функциональная схема имитационной модели в среде *MATLAB* системы связи на основе *ADSL* технологий с отводным каналом при непосредственном подключении оборудования нарушителя к каналу связи.

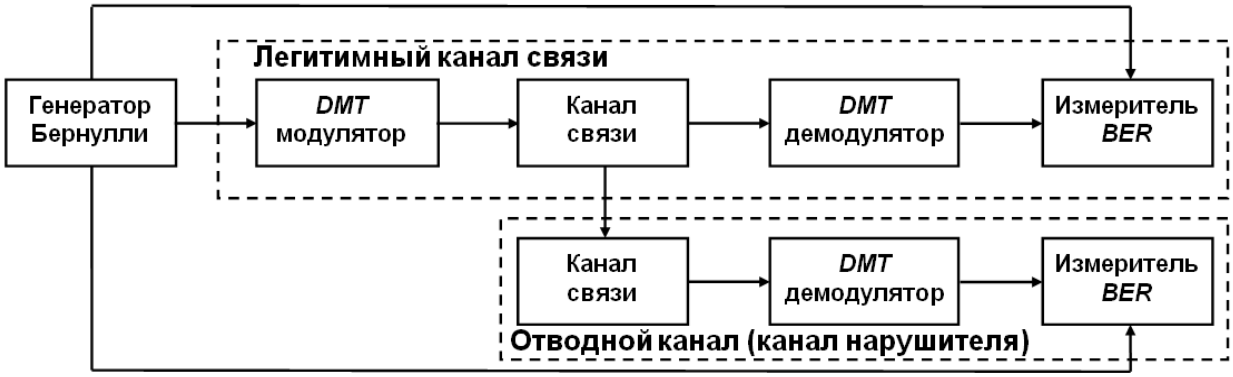


Рис.2. Функциональная схема имитационной модели *ADSL* системы с отводным каналом

Рассмотрим особенности построения некоторых блоков имитационной модели *ADSL* системы с отводным каналом. В технологии *ADSL* для передачи информации используются *QAM* модуляция 256 поднесущих частот, при полосе пропускания канала *1,1МГц*. Разность частот между соседними равномерно расположенными в полосе поднесущими частотами составляет $\Delta f = 4,3125$ *кГц*.

Генератор Бернулли является генератором двоичных случайных сигналов и задает поток данных на входе модели.

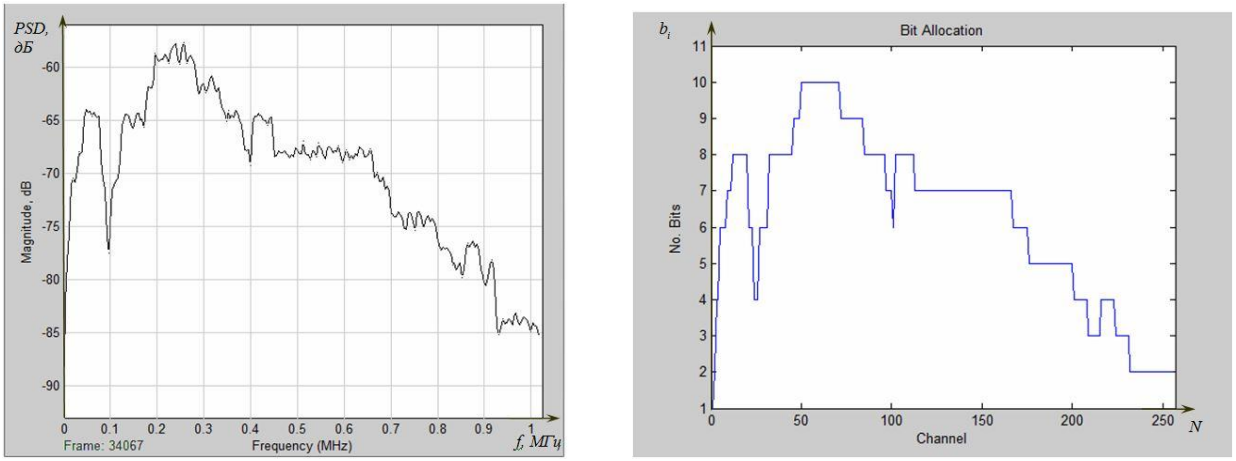
DMT модулятор формирует $N = 256$ поднесущих частот (тонов), каждая из которых имеет свой уровень модуляции *QAM* в зависимости от отношения сигнал/шум SNR_i в канале связи для каждой i-й несущей частоте и частотной характеристики кабельной линии связи (КЛС), которая определяет загрузку b_i. Максимальное количество бит информации b_i, которые могут передаваться в течение одной посылки на *i*-й поднесущей частоте, связано с отношением сигнал/шум SNR_i на этой частоте и заданной величиной вероятности битовой ошибки P_b на выходе приемника легитимного канала [9]:

$$b_i = floor\left\{\log_2\left(1+\frac{3SNR_i}{k^2}\right)\right\} \tag{7}$$

где $b(i)$ – битовая загрузка *i*-й поднесущей частоты; $floor\{x\}$ – операция отбрасывания дробной части числа x; $k = Q^{-1}(P_b/1,7)$ – отношение между самыми близкими точками сигнального созвездия к среднеквадратическому значению белого Гауссовского шума в *i*-м канале, где $Q^{-1}(x)$ – функция, обратная к интегралу ошибок $Q(x)$, $Q(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} e^{-\frac{y^2}{2}} dy$.

По стандарту технологии *ADSL* [10] нормированная вероятность битовой ошибки в легитимном канале связи составляет $P_b = 10^{-7}$, а значит – $k \approx 5,3$.

На рис. 3, *а* представлена типовая частотная характеристика КЛС, по которой был определен уровень *QAM модуляции* для каждой i-й поднесущей частоты, а значит и битовая загрузка b_i в легитимном канале связи (рис. 3, *б*).



а *б*

Рис. 3. Частотная характеристика КЛС (*а*) и битовая загрузка b_i (уровень *QAM* модуляции) (*б*) – для 256 частотных каналов

Блок *Канал связи* моделирует характеристики проводного канала передачи. В этом блоке задается мощность сигнала в линии и отношение сигнал/шум *SNR* в канале связи.

В блоке *DMT демодулятор* выполняется операция демодуляции полученного сигнала.

Оценка качества передачи информации в легитимном канале связи и отводном канале нарушителя производится соответствующими *Измерителями BER*, которые фиксируют ошибки на приеме по отношению к переданной цифровой последовательности.

Упрощенная блок-схема *модулятора* и *демодулятора DMT* на основе модулей обратного (*IFFT*) и прямого (*FFT*) быстрого преобразования Фурье представлена на рис. 4.

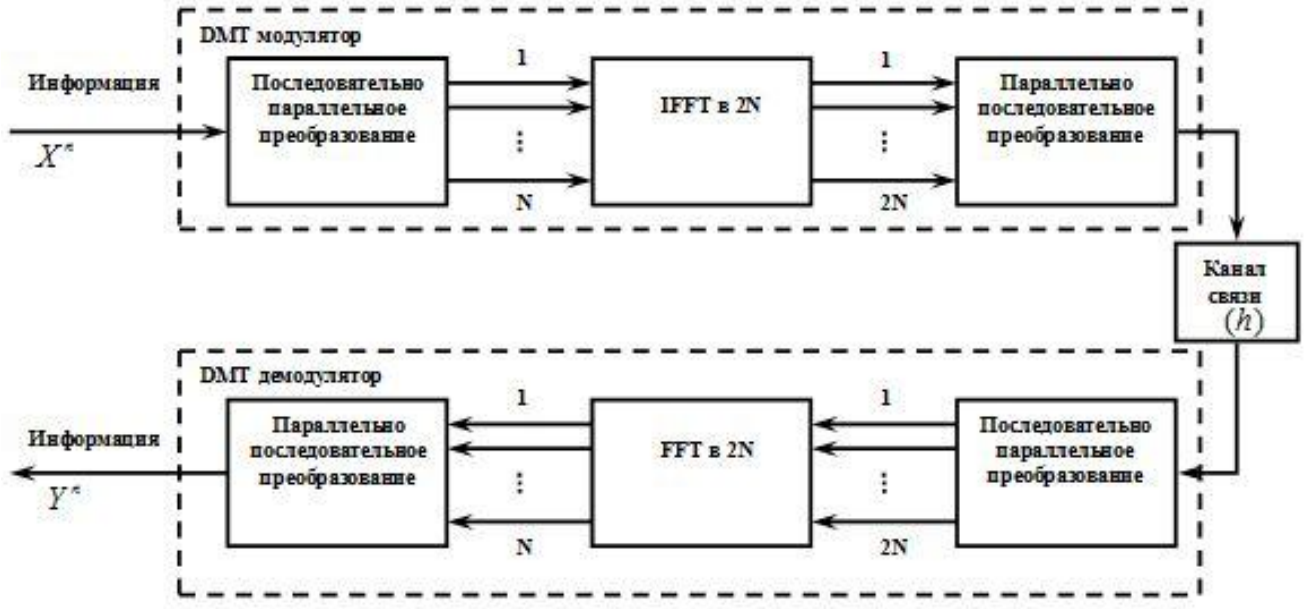


Рис. 4. Блок-схема модулятора и демодулятора *DMT* сигнала

Модулятор в модели реализован с помощью *IFFT*, который имеет *2N* выходов. Схема формирования *N* тонов в *DMT* модуляторе представлена на рис. 5.

Для реализации *QAM* модуляции нужно иметь количество тонов *N+1,…,2n-1*, и комплексно сопряженных по уровню модуляции тонов *N-1,…,1*, что может быть выражено следующими условиями:

$c_k = a_k + jb_k$ – совокупность модулирующих символов в тонах *k*, *k=1,2,…,N-1*;

$c_{2N-k} = (c_k)^* = a_k - jb_k$ – совокупность модулирующих символов в тонах;

$$N+1,\ldots,2N-1 \qquad (8)$$

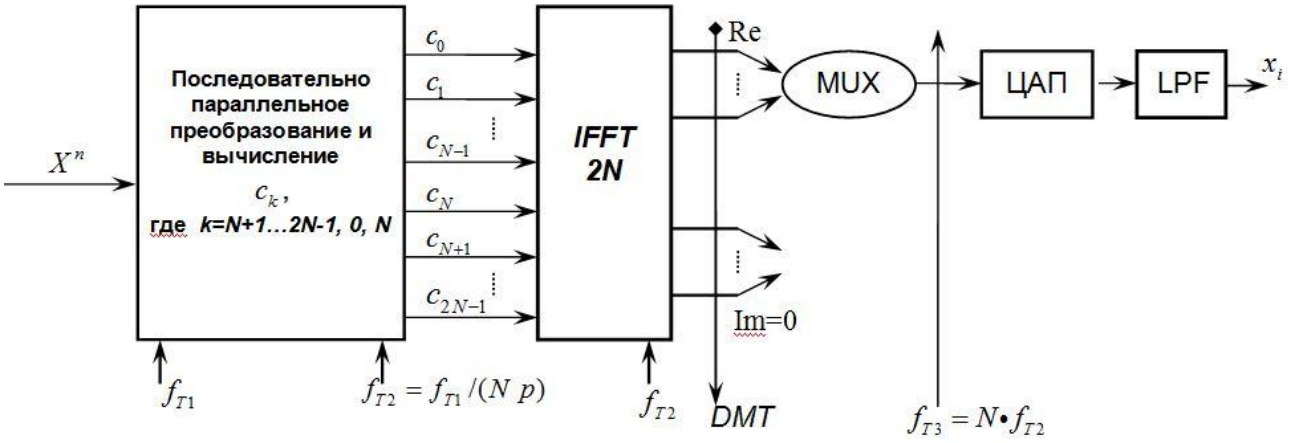


Рис. 5. Схема формирования *N* тонов в *DMT* модуляторе

Тоны *0* и *N* имеют специальный режим. Модуляционный уровень на этих тонах должен быть нулевым $c_0 = c_N = 0$, в добавление к этому в соотношении (8) составляющая мнимой части сигнала на выходе блока *IFFT* должна быть равна нулю, независимо от вида модуляции данных.

На рис. 5 показаны тактовые частоты, на которых работают отдельные части модели: f_{T1} – символьная тактовая частота; f_{T2} – частота *N*-го тона, f_{T3} – частота выборки данных, p – коэффициент, который принимает значение от *1* до *N-1*.

DMT сигнал, модулированный как функция *k* (индекс тона кратный частоте f_{T2}), и *n* (индекс дискретизации по времени) можно записать в виде [11]:

$$x(n) = \sum_{k=0}^{2N-1} c_k e^{j\frac{2\pi kn}{2N}}, \tag{9}$$

С учетом соотношения (8) и особенности тонов *0* и *N*, *DMT* модулированный сигнал можно записать как:

$$\begin{aligned} x(n) &= \sum_{k=0}^{2N-1}(a_k + jb_k)e^{j\frac{2\pi kn}{2N}} = \sum_{k=1}^{N-1}(a_k + jb_k)e^{j\frac{2\pi kn}{2N}} + \sum_{k=N+1}^{2N-1}(a_k + jb_k)e^{j\frac{2\pi kn}{2N}} = \\ &= \sum_{k=1}^{N-1}(a_k + jb_k)e^{j\frac{2\pi kn}{2N}} + \sum_{k'=1}^{N-1}(a_{k'} - jb_{k'})e^{j\frac{2\pi(2N-k')n}{2N}} = \\ &= \sum_{k=1}^{N-1}a_k(e^{j\frac{2\pi kn}{2N}} + e^{j2\pi n} + e^{-j\frac{2\pi kn}{2N}}) + j\sum_{k=1}^{N-1}b_k(e^{j\frac{2\pi kn}{2N}} - e^{j2\pi n}e^{-j\frac{2\pi kn}{2N}}), \end{aligned} \tag{10}$$

где $k = 2N - k',\ k' = 1,\ldots N-1 \Rightarrow a_k = a_{k'},\quad b_k = -b_{k'}$

Так как *n* является индексом дискретизации по времени, то есть натуральным числом, $\Rightarrow e^{j2\pi n} = \cos(2\pi n) + j\sin(2\pi n) = 1$. Используя соотношение Эйлера [12] для синуса и косинуса, соотношение (10) примет вид

$$\begin{aligned} x(n) &= \sum_{k=1}^{N-1}a_k(e^{j\frac{2\pi kn}{2N}} + e^{-j\frac{2\pi kn}{2N}}) + j\sum_{k=1}^{N-1}b_k(e^{j\frac{2\pi kn}{2N}} - e^{-j\frac{2\pi kn}{2N}}) = \\ &\sum_{k=1}^{N-1}2a_k\cos\left(\frac{2\pi kn}{2N}\right) + j\sum_{k=1}^{N-1}2jb_k\sin\left(\frac{2\pi kn}{2N}\right) \Rightarrow s(n) = 2\sum_{k=1}^{N-1}\left[a_k\cos\left(\frac{2\pi kn}{2N}\right) - b_k\sin\left(\frac{2\pi kn}{2N}\right)\right], \end{aligned} \tag{11}$$

Для реализации *DMT* сигнала после преобразования *IFFT* реальная часть результата обработки подается через мультиплексор (*MUX*) и цифроаналоговый преобразователь (ЦАП) в линию связи. Для формирования выходного сигнала с нужными параметрами используется выходной фильтр (*LPF*).

Используя выражение Эйлера, опишем демодуляцию данных на каждом тоне l (l-индексом тона в приемном блоке *FFT*) в виде

$$c_l = \frac{1}{2N}\sum_{n=0}^{2N-1}\left[\sum_{k=0}^{2N-1} 2\left(a_k \cos\left(\frac{2\pi kn}{2N}\right) - b_k \sin\left(\frac{2\pi kn}{2N}\right)\right)\right] e^{j\frac{2\pi l\,n}{2N}} =$$
$$= \frac{1}{2N}\sum_{n=0}^{2N-1}\left[\sum_{k=0}^{2N-1}\left(a_k\left(e^{j\frac{2\pi(k-1)n}{2N}} + e^{-j\frac{2\pi(k+1)}{2N}}\right) + jb_k\left(e^{j\frac{2\pi(k-1)}{2N}} - e^{-j\frac{2\pi(k+1)n}{2N}}\right)\right)\right], \quad (12)$$

Демодулированный сигнал в канале c_{l-1} можно представить заменой индекса $k=l$ в выражении (12) :

$$c_{l-1} = \frac{1}{2N}\sum_{n=0}^{2N-1} a_l\left(e^{j\frac{2\pi n\,0}{2N}} + e^{-j\frac{2\pi 2l\,n}{2N}}\right) + jb_l\left(e^{j\frac{2\pi n\,0}{2N}} - e^{-j\frac{2\pi 2ln}{2N}}\right) =$$
$$= \frac{1}{2N}\sum_{n=0}^{2N-1} a_l\left(1 + e^{-j\frac{2\pi 2l\,n}{2N}}\right) + jb_l\left(1 - e^{-j\frac{2\pi 2ln}{2N}}\right) = \quad (13)$$
$$= \frac{1}{2N}\sum_{n=0}^{2N-1}(a_l + jb_l) + \frac{1}{2N}a_l\sum_{n=0}^{2N-1} e^{-j\frac{2\pi 2l\,n}{2N}} - j\frac{1}{2N}b_l\sum_{n=0}^{2N-1} e^{-j\frac{2\pi 2l\,n}{2N}},$$

Второй и третий элемент выражения (13) больше 0, поскольку две суммы можно рассмотреть как две геометрические прогрессии с первым элементом $a_0 = 1$ и нормировать $r = e^{-j\frac{2\pi 2l}{2N}}$, получим выражение:

$$\sum_{n=0}^{2N-1}\left(e^{-j\frac{4\pi l}{2N}}\right)^n = \frac{e^{-j\frac{4\pi 2lN}{2N}} - 1}{e^{-j\frac{4\pi l}{2N}} - 1} = \frac{1-1}{e^{-j\frac{4\pi l}{2N}} - 1} = 0, \qquad r = e^{-j\frac{2\pi 2l}{2N}}, \quad (14)$$

После этого выражение (13) можно записать так:

$$c_{l-1} = \frac{1}{2N}(a_l + jb_l)\,2N = a_l + jb_l, \quad (15)$$

Таким образом, после демодуляции получим точный уровень модуляции, который был передан по каналу l.

Общую модель системы связи с отводным каналом для *DMT* модуляции, при условии, что нарушитель также использует для приема и обработки многочастотных сигналов блоки *FFT*, можно представить в следующем виде

$$y_{k,m} = \underbrace{\sum_{n=0}^{2N_c-1}\underbrace{\left(\frac{1}{2N_c}\sum_{k=0}^{2N_c-1}\left(\sum_{\eta=0}^{N_c} h_M(\eta)e^{-\frac{j2\pi k\eta}{N_c}}\right)x_{k,m}e^{\frac{j2\pi kn}{2N_c}}\right)}_{IFFT_M} e^{-\frac{j2\pi kn}{2N_c}}}_{FFT_M} + n_{k,m} - \text{легитимный канал;} \quad (16)$$

$$z_{w,k,m} = \underbrace{\sum_{n=0}^{2N_c-1}\underbrace{\left(\frac{1}{2N_c}\sum_{k'=0}^{2N_c-1}\left(\sum_{\eta=0}^{N_c} h_W(\eta)e^{-\frac{j2\pi k\eta}{N_c}}\right)x_{k,m}e^{\frac{j2\pi kn}{2N_c}}\right)}_{IFFT_M} e^{-\frac{j2\pi k'n'}{2N_c}}}_{FFT_W} + n_{k,m} - \text{отводной канал.} \quad (17)$$

Вероятность появления битовой ошибки, в зависимости от отношения сигнал/шум *SNR* в канале связи, рассчитывается с использованием следующего соотношения:

$$BER = \frac{\sum_{i=1}^{N} P_{bi}}{M \cdot \sum_{i=1}^{N} b_i}, \qquad (18)$$

где P_{bi} – вероятность битовой ошибки на каждой i-й поднесущей; b_i – битовая загрузка на каждой i-й поднесущей; N – количество несущих; M – общее количество пакетов данных переданных от *генератора Бернулли* через модель.

С использованием приведенной выше модели была исследована защищенность системы связи *ADSL* при изменении параметров физического уровня. Учитывая то, что в многочастотных системах связи точность установки частоты и фазы в легитимном приемнике определяет качество передачи мультимедийной информации, с помощью модели оценивались возможности нарушителя при приеме *DMT* сигналов.

На рис. 6 приведены зависимости *BER* от *SNR* для легитимного и отводного каналов в зависимости от сдвига фаз в демодуляторе нарушителя на 0.1, 0.05, 0.02, 0.01 рад для каждого вида модуляции несущей. Величина BER_0 определяет допустимый уровень ошибок в канале связи при передаче мультимедийной информации.

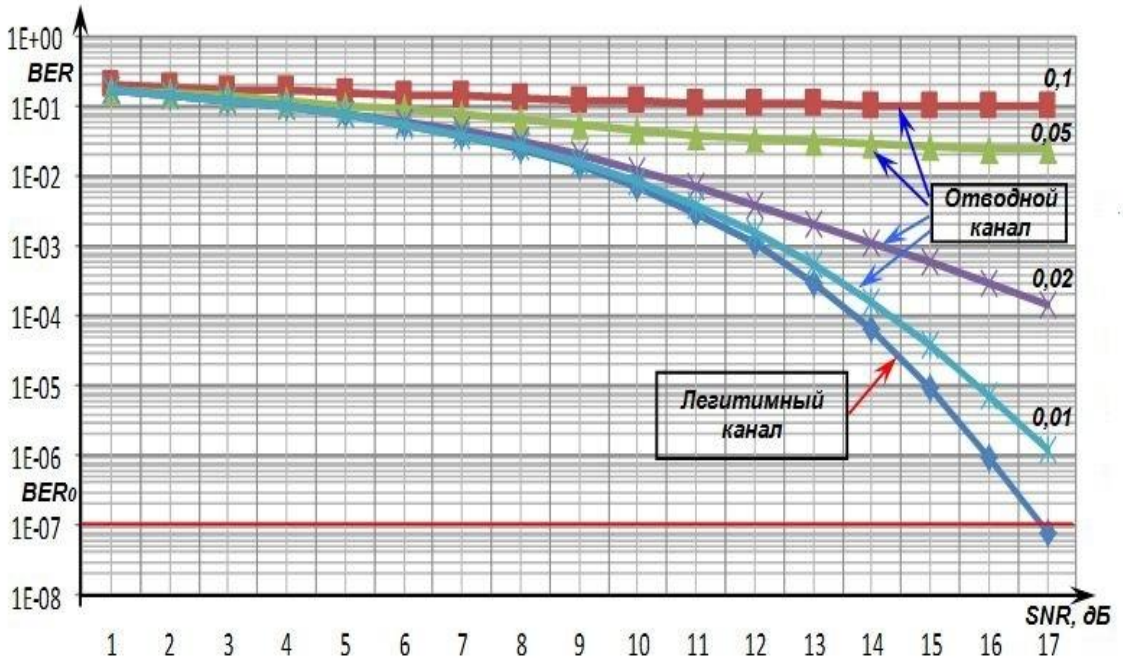


Рис. 6. График зависимости битовой ошибки *BER* от *SNR*
при разных параметрах настройки *DMT* демодулятора

По результатам полученных данных видим, что вероятность успешного перехвата информации легитимного канала связи возможна при сдвиге фазы на 0.01 *рад*. в демодуляторах приемной части канала нарушителя. При увеличении сдвига фаз нарушителю не удастся распознать принятую информацию с требуемым уровнем *BER*.

Заключение

Представлена обобщенная модель отводного канала для систем связи, использующих многочастотные сигналы. Для оценки защищенности (помехозащищенности и скрытности) системы связи предложены соответствующие критерии.

Детально рассмотрено математическое описание процессов цифровой обработки сигналов и описана модель отводного канала для системы связи с *ADSL* технологией передачи информации с использованием *DMT* модуляции.

Получены графики зависимости битовой ошибки *BER* от *SNR* при разных параметрах настройки *DMT* демодулятора, показывающие влияние параметров физического уровня (сдвига фазы в демодуляторе нарушителя) на защищенность системы связи.

Список литературы: 1. *Концепція* технічного захисту інформації в Україні. Постанова Кабінету Міністрів України від 8 жовтня 1997 року № 1126. 2. *Хорошко В.А., Чекатков А.А.* Методы и средства защиты информации. – К. : ЮНИОР, 2003. – 504 с. 3. *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. 4. *Wyner A.D.* The wire-tap channel // Bell System Technical Journal. – 1975. – Vol. 54, № 8. – pp. 1355 -1387. 5. *Цопа А.И.* Разработка и исследование модели отводного канала для проводных цифровых систем передачи информации / А.И.Цопа, В.М. Шокало // Материалы XIII междунар. науч.-практ. конф. «Безопасность информации в информационно-телекоммуникационных системах». – Київ, 2010. – С. 64. 6. *Прокис Д.* Цифровая связь ; пер. с англ. под ред. Д.Д. Кловского. – М. : Радио и связь, 2000. – 800 с. 7. *Barros J., Rodrigues Miguel R. D.* Secrecy Capacity of Wireless Channels // Proc. of the IEEE International Symposium on Information Theory (ISIT'06), Seattle, WA, July 2006. – P.356-360. 8. *Jorswieck E., Wolf A.* Resource allocation for the wire-tap multi-carrier broadcast channel // Proc. International Workshop on Multiple Access Communications (MACOM). – St. Petersburg, Russia, 2008. – P.45–51. 9. *SERIES G: TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS.* Digital transmission systems – Digital sections and digital line system – Access networks Asymmetric digital subscriber line (*ADSL*) transceivers // ITU-T Recommendation G.991.1. 06/1999. 10. *Лашко А. Г., Ляховецкий Л. М., Раду В. В.* Моделирование характеристик цифровых абонентских линий, построенных по *ADSL* технологии // Наукові праці ОНАЗ ім. Попова. – 2005. – №1. – С. 67-74. 11. *Сергиенко А.Б.* Цифровая обработка сигналов : учебник для вузов. 2-е изд. – СПб. : Питер, 2006. – 751 с. 12 *Корн Г., Корн Т.* Справочник по математике (для научных работников и инженеров). – М. : Наука, 1973. – 832 с.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 12.02.2013