11. Дідковський Р.М., Метелап В.В. Підвищення рівня захищеності даних в системах зв'язку з фазовою маніпуляцією шумового сигналу // Вісник ЧДТУ. – 2010. – № 3. – С.53-57.

12. Дідковський Р.М. Порівняльний аналіз завадостійкості бінарних систем зв'язку з протилежними шумовими сигналами // Вісник ДУІКТ. – 2010. – Т.8, №4. – С.387-407.

13. Lau F.C.M., Cheong K.Y., Tse Chi K. Permutation-Based DCSK and Multiple-Access DCSK Systems // IEEE Trans. Circuits Syst. I. – 2003. – vol. 50, no. 6. – P.733–742.

14. Демьян Н.И., Осмоловский В.А., Хорошко В.А. Линейные и нелинейные параметрические модели речевого сигнала // Захист інформації. – 2010. – №2. – С.60-64.

15. Тихонов В.И., Харисов В.Н. Статистический анализ и синтез радиотехнических устройств и систем: Учеб. Пособие для вузов. – М.: Радио и связь, 1991. – 608 с.

В роботі запропонована система зв'язку для прихованої передачі конфіденційних цифрових даних по існуючим відкритим каналам зв'язку звукового частотного діапазону. Представлені принципи побудови та функціонування системи, методи формування та обробки сигналу.

Ключові слова: прихована передача даних, широкополосна система зв'язку, шумоподібних сигнал, бінарна фазова маніпуляція.

В работе предложена система связи для скрытой передачи конфиденциальных цифровых данных по существующим открытым каналам связи звукового частотного диапазона. Представлены принципы построения и функционирования системы, методы формирования и обработки сигнала.

Ключвые слова: скрытая передача данных, широкополосная система связи, шумоподобный сигнал, бинарная фазовая манипуляция.

This paper presents a communication system for hidden transfer confidential data via the existing open communication channels in the audible frequency band. The principles of system construction and operation, methods of signal forming and signal processing are presented.

Key words: hidden data transfer, wideband communication system, noise-like signal, binary phase shift keying.

Рецензент: д.т.н., проф. Єрохін В.Ф.
Надійшла 12.01.2011

УДК 621.391.7

Шинкаренко И.В., Цопа А.И. (ХНУРЭ)

ИМИТАЦИОННАЯ МОДЕЛЬ ОТВОДНОГО КАНАЛА С ЭЛЕКТРИЧЕСКОЙ СВЯЗЬЮ ДЛЯ ПРОВОДНЫХ ЦИФРОВЫХ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ

Введение

При создании производительных ведомственных систем связи (ВСС), одним из основных требований предъявляемым к таким сетям является обеспечение не только высокой производительности, но и защищенности каналов связи. Несмотря на большое количество разработанных протоколов защиты информации на верхних ступенях семиуровневой модели взаимодействия открытых систем (*OSI*), эффективность их значительно снижается при передаче в ВСС мультимедийной информации [1]. Кроме того, при массовом внедрении цифровых технологий передачи информации обеспечить повышенные требования безопасности только одними информационными (криптографическими) методами не представляется возможным. В этих условиях необходимо искать новые пути повышения защищенности каналов связи не только на информационном, но и на физическом (энергетическом) уровне модели *OSI*.

Учитывая то, что современный этап модернизации ВСС связан лавинообразным внедрением в этих сетях цифровых методов передачи, обработки и хранения информации, то это дает повод по новому взглянуть на роль и значение технической защиты информации (ТЗИ).

Концепция технической защиты информации в Украине, которая утверждена в 1997 г. соответствующим Постановлением Кабинета Министров Украины [2], определяет основные направления развития ТЗИ и ее роли в обеспечении безопасности государства. В наше время

имеется целый ряд объективных причин в повышении угроз информации, вызванные либерализацией общественных и государственных отношений, использованием технических средств обработки (ТСО) и цифровых систем передачи информации (ЦСПИ) импортного производства, широким распространением средств для несанкционированного доступа к информации и воздействии на нее и т.п.

В этих условиях государственные интересы лежат в технической защите информации, которая циркулирует в ВСС и коммерческих сетях связи, несанкционированный доступ или ее искажение может нанести значительный ущерб государственной или экономической безопасности государства. Однако многие нормативные документы по ТЗИ подготовлены и утверждены уже давно и не отражают новых реальных угроз информации на физическом уровне и требуют обновления [3-6].

Целью работы является разработка на основе концепции отводного канала новых подходов и моделей оценки защищенности каналов связи на физическом уровне, учитывающих особенности построения проводного сегмента ВСС на основе современных цифровых систем передачи информации.

Основная часть.

В проводном сегменте современных ВСС доминируют широкополосные *xDSL* технологии, которые являются основой физического уровня при построении мультимедийных каналов передачи информации [7]. Использование в технологиях *xDSL* многоуровневых видов модуляции линейного сигнала, а также сигналов с множественными поднесущими частотами создают реальную основу построения не только производительных, но и защищенных систем связи. Развитие концепции отводного канала применительно к проводным ЦСПИ дает возможность достичь высокой защищенности канала на физическом уровне модели *OSI*, без применения криптографических методов защиты [8].

В известных работах [9, 10] концепция отводного канала развита для случая электромагнитной связи приемника-обнаружителя с кабельной линией связи (КЛС), проложенной в различных материальных средах (под землей, над землей и вертикальных колодцах). В этих работах получены данные о помехозащищенности и скрытности кабельных каналов связи при применении различных *xDSL* технологий. Отсутствие данных о энергетической и структурной защищенности ЦСПИ при непосредственном подключении аппаратуры нарушителя к многопарным проводам легитимного канала связи указывает на актуальность проведенных исследований.

Учитывая то, что при построении ВСС зачастую используется инфраструктура выделенных кабельных линий, то опасность подключения к таким линиям возрастает, особенно на абонентском участке КЛС. При этом нарушитель не только может снимать информацию с легитимного канала связи, но и воздействовать на него генератором помех, нарушая работу канала связи ВСС. Учитывая то, что обычно отсутствуют данные о технических средствах нарушителя, а место подключения неизвестно, то наиболее эффективным методом анализа защищенности ЦСПИ с *xDSL* технологиями является моделирование отводного канала. При этом полное моделирование всех процессов преобразования информации от входа до выхода ЦСПИ позволит не только оценить параметры энергетической, но структурной защищенности системы связи.

На рис. 1 представлена структурная схема имитационной модели в среде *MATLAB* ЦСПИ на основе *SHDSL* технологий с отводным каналом при непосредственном подключении оборудования нарушителя к каналу связи.

Рис. 1. Структурная схема имитационной модели ЦСПИ с отводным каналом

Скорость передачи информации в модели ЦСПИ задается блоком *Генератор Бернулли* (*Bernoulli Binary Generator*), который является генератором двоичных случайных сигналов с фреймовой структурой. Блок *Скремблер* (*Scrambler*) – преобразует структуру цифрового потока без изменения скорости передачи с целью получения определенных свойств случайной последовательности и реализует логическую операцию суммирования по модулю два исходного и псевдослучайного двоичных сигналов. Одна из целей скремблирования – сокращение длины строки из последовательных *0* или *1* в передаваемом цифровом потоке для повышения надежности синхронизации терминалов. Кроме того, скремблирование позволяет повысить защищенность канала связи на структурном уровне.

Для уменьшения количества ошибок, возникающих при передаче информации по каналу с помехами, используется помехоустойчивое кодирование. Блок *Треллис кодер* (*Convolution Encoder – TC*) – выполняет сверточное кодирование (со скоростью кода *3/4* и *1/2)*, которое лучше приспособлено к побитовой передаче данных и обладает хорошей исправляющей способностью, что в целом повышает энергетическую защищенность канала связи в условиях действия шумов, естественных и преднамеренных помех.

Преобразование цифрового сигнала в линейный амплитудно-модулированный сигнал (*Pulse Amplitude Modulation – PAM*) обеспечивается блоком модели *PAM модулятор* (*Modulator Baseband*). В этом блоке задается уровень модуляции *M* (*M-ary value* – количество *PAM* уровней сигнала) и тип кодировки (*Symbol Order* – двоичный либо коды Грея).

Минимизация межсимвольной интерференции (МСИ) в канале связи обеспечивается дополнительной фильтрацией сигнала в блоке *Фильтр приподнятого косинуса передатчика* (*Raised Cosine Transmit Filter*).

Блок *Канал связи* (*AWGN Channel*) моделирует характеристики проводного канала передачи. Здесь задается мощность сигнала в линии и отношение сигнал/шум (E_b/N_0) в канале связи.

В удаленном терминале происходит обратное преобразование сигнала *TC-PAM*. Сначала сигнал проходит через блок *Фильтр приподнятого косинуса приемника* (*Raised Cosine Receive Filter*), характеристики которого в легитимном канале должны совпадать с характеристиками, соответствующего фильтра передатчика. В блоке *PAM демодулятор* (*Demodulator Baseband*) выполняется операция демодуляции многоуровневого линейного сигнала.

Для декодирования сигналов используется блок *Декодер Витерби* (*Viterbi Decoding*), обеспечивающий простой и эффективный механизм гибкого декодирования методом исключения из анализа маловероятных путей на декодирующей решетке. Глубина решетки декодера Витерби является одним из показателей структурной защищенности ЦСПИ.

Блок *Дескремблер* (*Descrambler*) восстанавливает исходную последовательность. Основной частью данного блока является генератор псевдослучайной последовательности (ПСП) в виде линейного *n*-каскадного регистра с обратными связями, формирующий последовательность максимальной длины *2n-1*. Параметры блока в легитимном канале должны соответствовать аналогичным параметрам блока *Scrambler* в ЦТ.

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

Рассмотрим более детально часть модели ЦСПИ, которая называется МОДЕМ (модулятор-демодулятор) и обеспечивает формирование и прием многоуровневого линейного сигнала *PAM*. Этот блок непосредственно определяет энергетические и спектральные характеристики сигнала в линии связи между двумя терминалами: центральным (ЦТ) и удаленным (УТ).

При передаче цифровой информации по каналу связи амплитудно-импульсный модулятор (АИМ) является устройством отображения цифровой информации в форму аналоговых сигналов (рис. 2). Отображение осуществляется посредством выбора блоков из $k = \log_2 M$ двоичных сигналов из символов информационной последовательности $\{a_k\}$ и выборе одного из $M = 2^k$ сигналов с ограниченной энергией $\{s_m(t), m = 1,2,...,M\}$, для передачи его по каналу за время передачи k информационных символов.

Цифровой многоуровневый сигнал с амплитудно-импульсной модуляцией можно представить в виде

$$x_S(t) = \sum_{k=-\infty}^{\infty} A_k \cdot \delta(t - kT), \qquad (1)$$

где A_k – амплитуда k-того импульса (символа), $A_k \in \{\pm 1, \pm 3, .., \pm(M-1)\}$ возможных уровней сигнала; M – количество уровней сигнала; $\delta(t)$ – является импульсной функцией; T – период передачи символов.

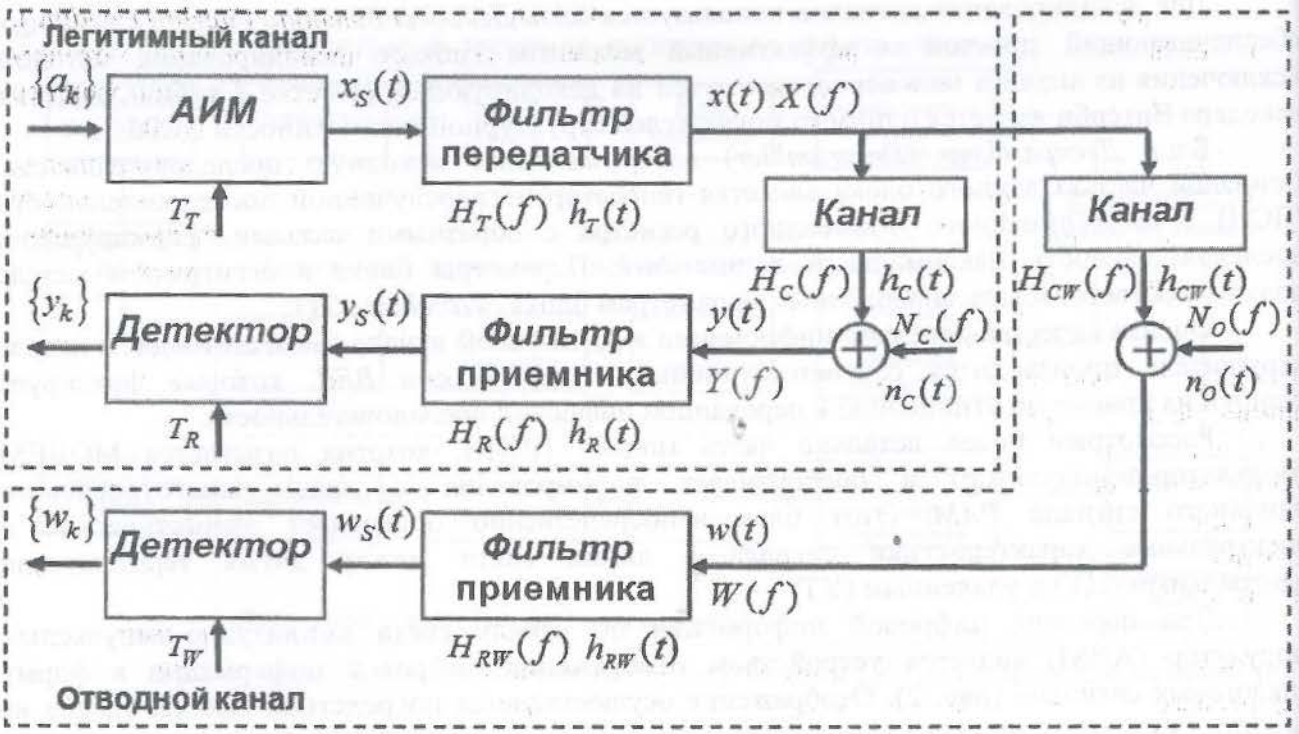


Рис. 2. Структура части модели ЦСПИ, которая называется МОДЕМ

Амплитуда сигнала A_k принимает дискретные уровни

$$A_k = \left[2 \cdot S(y_i) - M + 1\right] \cdot d, \quad 0 \le y_i \le M - 1, \tag{2}$$

где $2d$ – расстояние между соседними амплитудами сигналов (Евклидово расстояние); $S(y_i)$ – функция разметки сигнального множества.

Для того, чтобы устранить межсимвольную интерференцию (МСИ) в канале связи импульсный сигнал $\delta(t - kT)$ необходимо пропустить через специальный фильтр передатчика с передаточной характеристикой $h_T(t)$ для придания ему характеристик, удовлетворяющих условию Найквиста.

Тогда выходной сигнал на выходе фильтра передатчика будет иметь вид

$$x(t) = \sum_{k=-\infty}^{\infty} A_k \cdot h_T(t - kT) \tag{3}$$

Класс импульсов Найквиста – это множество импульсов, форма которых может быть описана функцией $\sin c(\frac{t}{T})$, умноженной на другую временную функцию. Наиболее популярными являются сигналы с характеристикой типа приподнятого косинуса или корня из приподнятого косинуса. Несмотря на близкие характеристики именно импульс типа приподнятого косинуса дает нулевую межсимвольную интерференцию (МСИ) при взятии выборок сигнала в моменты времени T, $2T$, $3T$... $n \cdot T$.

Передаточная общесистемная функция $H(f)$ типа приподнятого косинуса описывается выражением [11]

$$H(f)=\begin{cases}1, & для\ |f|<2\cdot W_0-W\\ \cos^2\left(\frac{\pi}{4}\cdot\frac{|f|+W-2W_0}{W-W_0}\right), & для\ 2W_0-W<|f|<W\\ 0, & для\ |f|>W\end{cases}, \quad (4)$$

где W – максимальная ширина полосы; $W_0=\frac{1}{2\cdot T}$ – минимальная ширина полосы по Найквисту.

Разность частот $W-W_0$ определяет дополнительную ширину полосы по сравнению необходимым минимумом, для оценки которого можно использовать коэффициент сглаживания r

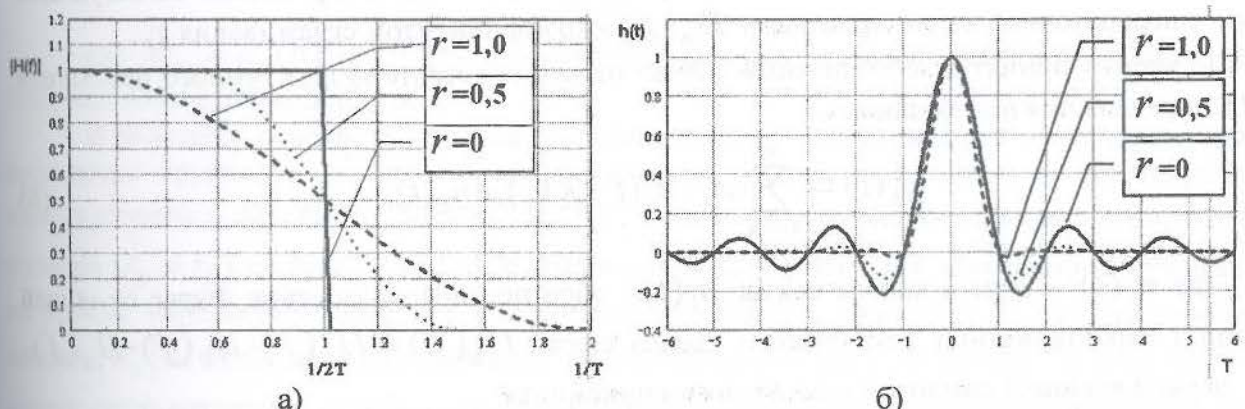
$$r=\frac{W-W_0}{W_0}. \quad (5)$$

Для лучшего понимания дальнейших результатов на рис. 3,а показана характеристика фильтра типа приподнятого косинуса при различных значениях коэффициента сглаживания r ($r=0$, $r=0{,}5$ *и* $r=1$). Из рис. 3,а видно, что для данной величины W_0 коэффициент сглаживания r характеризует крутизну фронта характеристики фильтра.

Импульсный отклик, соответствующий функции $H(f)$, описываемой выражением (4), можно определить так [11]:

$$h(t)=2\cdot W_0(\sin c2W_0\cdot t)\cdot\frac{\cos(2\pi\cdot r\cdot W_0\cdot t)}{1-(4\cdot r\cdot W_0\cdot t)^2}. \quad (6)$$

Импульсный отклик $h(t)$ при разных коэффициентах сглаживания r приведен на рис. 3,б. Импульсная характеристика имеет максимальное значение при $T=0$ и переходит через ноль при всех других значениях $n\cdot T$ кратных длительности символа. Чем больше коэффициент сглаживания фильтра r, тем короче «хвосты» импульсов и меньше их амплитуда, а значит меньше искажения вследствие МСИ.



а) б)

Рис. 3. Характеристики фильтра типа приподнятого косинуса при различных значениях коэффициента сглаживания r

При передаче, например, нескольких импульсов последовательности $\{+3,-3,+1,+3\}$ с разными уровнями амплитуды МСИ будет отсутствовать при взятии отсчетов во время кратное длительности символа $n \cdot T$ (рис. 4).

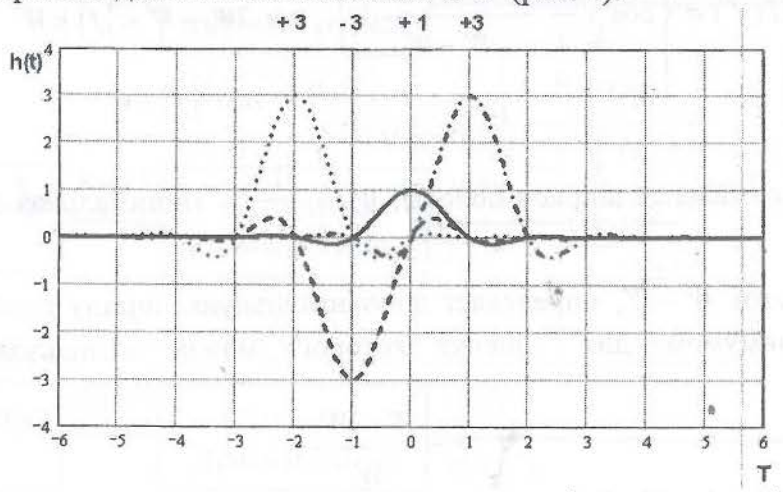


Рис. 4. Передача импульсов последовательности $\{+3,-3,+1,+3\}$ без МСИ

С учетом (6) цифровой поток в линии связи без МСИ можно представить в виде [12]

$$x(t) = \sum_{n}^{\infty} A_n \cdot \sin c[2W_0 \cdot (t - n \cdot T_T)] \cdot \frac{\cos[2\pi \cdot r_T \cdot W_0 \cdot (t - n \cdot T_T)]}{1 - [4 \cdot r_T \cdot W_0 \cdot (t - n \cdot T_T)]^2}, \quad (7)$$

где A_n – многоуровневая дискретная случайная переменная; r_T – коэффициент сглаживания фильтра передатчика; T_T – период выдачи символов в передатчике.

Этот сигнал передатчика ЦСПИ одновременно поступает в легитимный канал связи и отводной канал (ОК), который образуется за счет непосредственного подключения к линии связи приемника-обнаружителя.

Блок канала связи моделирует затухание сигнала в легитимном канале связи $H_C(f)$ и воздействие гауссовского белого шума $N_C(f)$ на линейный многоуровневый сигнал. Для коррекции сигнала на входе легитимного приемника установлен приемный согласующий фильтр с передаточной характеристикой $H_R(f)$ и коэффициентом сглаживания r_R.

С учетом принятых обозначений сигнал на входе детектора легитимного приемника $y_S(t)$ определяется выражением

$$y_S(t) = \sum_{k=-\infty}^{\infty} A_k \cdot h_L(t - kT_R) + n_L(t), \quad (8)$$

где $n_L(t)$ – шум в канале связи; $h_L(t)$ – обратное преобразование Фурье от общей частотной характеристики легитимного канала связи $H_L(f) = H_T(f) \cdot H_C(f) \cdot H_R(f)$; T_R – период выборки символов в легитимном приемнике.

Выборка сигнала $y_S(t)$ в детекторе легитимного канала происходит в определенные моменты времени $t_R = nT_R + t_d$, обеспечивающие оптимальное определение принимаемого символа

$$y_n = y(nT_R + t_d) = \sum_{k=-\infty}^{\infty} A_k \cdot h_L((n-k)T_R + t_d) + \vartheta_n, \quad (9)$$

где $\vartheta_n = n_L(nT_R + t_d)$ – дискретная выборка шума в канале; t_d – оптимальная задержка компаратора детектора.

При условии полной синхронизации легитимного канала связи обеспечивается когерентный прием и детектирование многоуровневого линейного сигнала ($T_T = T_R$). Согласованная настройка передающего и приемного фильтра ($r_T = r_R$) создает оптимальные возможности для правильного определения на приеме переданных символов, т.е. последовательность символов на выходе ЦСПИ $\{y_k\}$ равна последовательности символов $\{a_k\}$, поступившим на вход системы передачи.

Второй блок канала связи моделирует затухание сигнала в отводном канале связи $H_{CW}(f)$ и воздействие гауссовского белого шума $N_O(f)$ на линейный многоуровневый сигнал. Для коррекции сигнала на входе приемника-обнаружителя установлен приемный фильтр с передаточной характеристикой $H_{RW}(f)$ и коэффициентом сглаживания r_W.

С учетом принятых обозначений сигнал на входе детектора приемника-обнаружителя $w_S(t)$ определяется выражением

$$w_S(t) = \sum_{k=-\infty}^{\infty} A_k \cdot h_O(t - kT_W) + n_O(t), \quad (10)$$

где $n_O(t)$ – шум в отводном канале; $h_O(t)$ – обратное преобразование Фурье от общей частотной характеристики отводного канала $H_O(f) = H_T(f) \cdot H_{CW}(f) \cdot H_{RW}(f)$; T_W – период выборки символов в приемнике-обнаружителе.

Выборка сигнала $w_S(t)$ в детекторе приемника-обнаружителя происходит в определенные дискретные моменты времени $t_w = nT_W + t_{wd}$, необходимые для идентификации принимаемого символа

$$w_n = w(nT_W + t_{wd}) = \sum_{k=-\infty}^{\infty} A_k \cdot h_O((n-k)T_W + t_{wd}) + \vartheta_{wn}, \quad (11)$$

где $\vartheta_{wn} = n_O(nT + t_{wd})$ – дискретная выборка шума в отводном канале; t_{wd} – задержка компаратора детектора.

В условиях перехвата сигнала добиться полной синхронизации в отводном канале достаточно трудно, а значит, не обеспечивается когерентный прием и детектирование многоуровневого линейного сигнала ($T_W \neq T_T$). Разная настройка передающего и приемного фильтра ($r_W \neq r_T$) также не создает оптимальные возможности для правильного определения на приеме переданных символов, т.е. последовательность символов на выходе отводного канала $\{w_k\}$ не будет равна последовательности символов $\{a_k\}$, поданных на вход ЦСПИ. В канале связи возникают ошибки, уровень которых в модели определяется измерителем *BER*.

На рис. 5 приведены результаты численного моделирования с использованием предложенной модели и показаны зависимости битовой ошибки *BER* от отношения сигнал/шум (E_b/N_0) в легитимном и отводном каналах при разных значениях коэффициента сглаживания фильтра r_W и при разных видах модуляции *TC-PAM 16* и *TC-PAM 32*.

Из приведенных графиков видно, что несогласованный прием многоуровневого линейного сигнала *TC-PAM* в отводном канале при $r_W \le r_T$ приводит к увеличению ошибок *BER* в (*10-100*) раз, что не дает возможность нарушителю возможность перехватить мультимедийную информацию, которая передается в легитимном канале. Увеличение уровня модуляции M еще больше увеличивает защищенность ЦСПИ от перехвата сообщений.

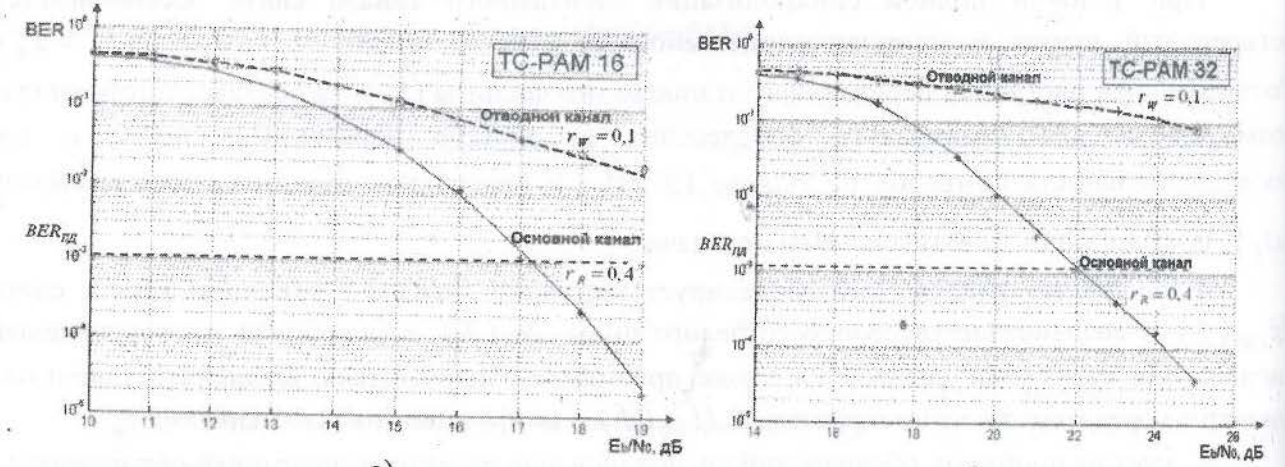
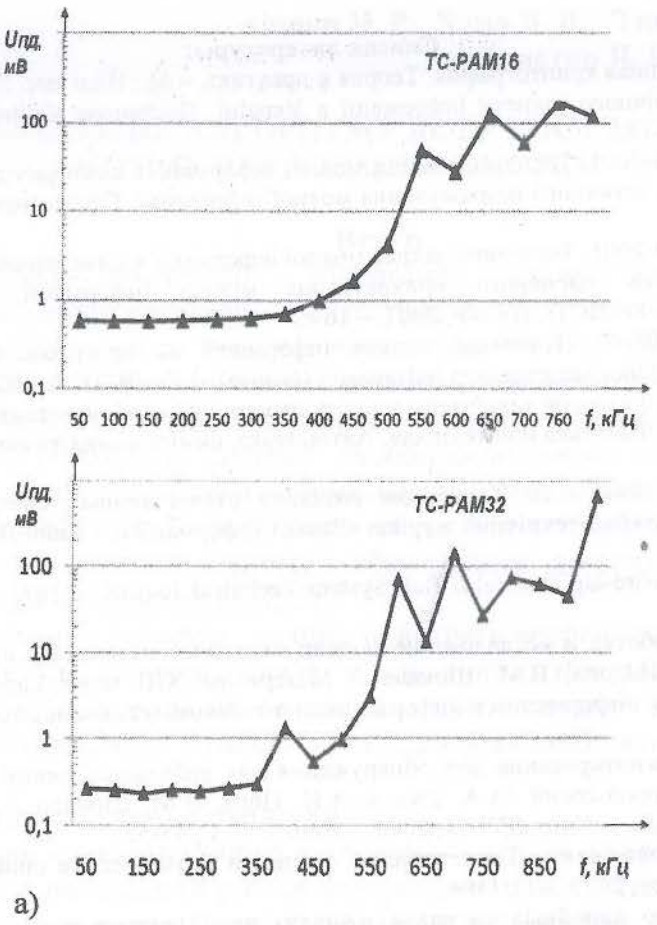


Рис. 5. Зависимости битовой ошибки *BER* от отношения сигнал/шум (E_b/N_0) в легитимном и отводном каналах при разных значениях коэффициента сглаживания фильтра r

На представленной модели были также проведены численные исследования помехозащищенности ЦСПИ при воздействии одночастотных искусственных помех, созданных генератором нарушителя и определены значения предельного напряжения помех $U_{ПД}$, при которых система связи перестает функционировать, т.е. не обеспечивается доступность информации в ВСС.

На рис. 6 приведены результаты численного моделирования зависимости $U_{ПД}$ от частоты одночастотных помех при различных видах модуляции *TC-PAM 16* (рис. 6,а) и *TC-PAM 32* (рис. 6,б). Авторами экспериментально установлено, что критерием разрыва канала связи при воздействии одночастотной помехи служил уровень пакетной ошибки *PER=0,1* при длине пакета $L = 512$, который может быть пересчитан в величину $BER_{ПД}$ по известному соотношению $PER \approx BER^L \approx L \cdot BER$ при $BER \ll 1$[10].

На рис. 5 величина $BER_{ПД}$ отмечена горизонтальной штрих пунктирной линией. Эти данные показывают, что превышение уровня BER_W в отводном канале выше уровня $BER_{ПД}$ приводит к разрыву связи в канале нарушителя и не дает ему возможности перехватывать сообщения, которые передаются в легитимном канале связи.



а) б)

Рис. 6. Результаты численного моделирования зависимости $U_{ПД}$ от частоты одночастотных помех при различных видах модуляции: а) *TC-PAM16*; б) *TC-PAM 32*

Результаты моделирования показывают, что уровень помехозащищенности ЦСПИ на основе *SHDSL* технологий существенно зависит от частоты одночастотной помехи. Особенно заметно влияние помех в частотном диапазоне, в котором расположен главный лепесток спектральной плотности мощности линейного сигнала *TC-PAM*. При повышении уровня модуляции *M* помехозащищенность ЦСПИ уменьшается.

Выводы

1. В статье предложена новая имитационная модель отводного канала для проводных систем связи на основе *SHDSL* технологий, позволяющая оценить как скрытность и помехозащищенность ЦСПИ на физическом уровне.

2. Получены новые данные о влиянии согласованной фильтрации линейного многоуровневого сигнала на скрытность системы связи на основе *SHDSL* технологий. Увеличение уровня модуляции *M* повышает скрытность системы связи.

3. Проведена оценка помехозащищенности ЦСПИ при воздействии искусственных помех при непосредственном подключении нарушителя к кабельной линии связи. При увеличении уровня модуляции *M* помехозащищенность ЦСПИ на основе *SHDSL* технологий снижается. Это связано с ограничением на мощность сигнала передаваемого по КЛС, а как следствие уменьшение абсолютного значения напряжения квантованного уровня линейного сигнала на приеме.

4. Развитие теории отводного канала позволяет определить новые возможности повышения защищенности каналов связи на физическом уровне и найти механизмы их интеграции с информационными методами защиты информации.

Список литературы:

1. *Мао В.* Современная криптография. Теория и практика. – М.: Вильямс, 2005. – 768 с.
2. Концепція технічного захисту інформації в Україні. Постанова Кабінету Міністрів України від жовтня 1997 року № 1126.
3. НД СТЗІ 2.3-003-2001. Технічний захист мовної інформації в симетричних абонентських аналогови телефонних лініях. Засоби активного приховування мовної інформації. Генератори спеціальних сигналів. – К ДСТСЗІ СБУ, 2001. – 22 с.
4. НД СТЗІ 2.3-003-2001. Технічний захист мовної інформації в симетричних абонентських аналогови телефонних лініях. Засоби пасивного приховування мовної інформації. Нелінійні атенюатори т загороджувальні фільтри. – К.: ДСТСЗІ СБУ, 2001. – 16 с.
5. НД ТЗІ 3.7-002-99. Технічний захист інформації на програмно-керованих АТС загальног користування. Методика оцінки захищеності інформації (базова). – К.: ДСТСЗІ СБУ, 1999.
6. *Хома В.В.* Методі і засоби технічного захисту інформації на абонентських телефонних лініях // Вісник Нац. університету «Львівська політехніка». Автоматика, вимірювання та керування. – 2009. – Вип. № 639. – С. 97–93.
7. *Шокало В.М., Цопа А.И.* Концепция создания отечественных специальных цифровых систе передачи информации // Науково-технічний журнал «Захист інформації». – Київ: ДУІКТ, 2006. – Вип. № 3. – С 51-57.
8. *Wyner A.D.* The wire-tap channel // Bell System Technical Journal. – 1975. – Vol. 54, № 8. – pp. 1355 1387.
9. *Цопа А.И.* Разработка и исследование модели отводного канала для проводных цифровых систе передачи информации /А.И.Цопа, В.М. Шокало // Материалы XIII международной научно-практическої конференции «Безопасность информации в информационно-телекоммуникационных системах». – Київ, 2010. С. 64.
10. *Цопа А.И.* Прогнозирование зон обнаружения для кабельных линий связи в сети абонентского доступа на основе *VDSL* технологий /А.А. Дудка, А.И. Цопа, В.М. Шокало // Науково-технічний журнал «Сучасний захист інформації». – Київ: ДУІКТ, 2010. – Вип. 3. – С. 45-53.
11. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение. 2-е издание. – М.: Издательский дом «Вильямс», 2003. – С. 1104.
12. *Цопа А.И.* Выбор линейных сигналов и анализ их спектральных характеристик в системах передачи информации с использованием *xDSL* технологий // Радиотехника. Всеукраинский межведомственный научно-технический сборник. – 2006. – Выпуск № 146, – С. 66-74.

В статье предложена новая имитационная модель отводного канала для проводных систем связи на основе *SHDSL* технологий, позволяющая оценить как скрытность и помехозащищенность ЦСПИ на физическом уровне. Получены новые данные о влиянии согласованной фильтрации линейного многоуровневого сигнала на скрытность системы связи на основе *SHDSL* технологий. Проведена оценка помехозащищенности ЦСПИ при воздействии искусственных одночастотных помех при непосредственном подключении нарушителя к кабельной линии связи.

Ключевые слова: имитационная модель, цифровая система передачи информации, легитимный канал, отводной канал, вероятность битовой ошибки.

У статті запропонована нова імітаційна модель відвідного каналу для проводових систем зв'язку на основі *SHDSL* технологій, що дозволяє оцінити як скритність, так і завадозахищеність ЦСПИ на фізичному рівні. Отримані нові дані про вплив погодженої фільтрації лінійного багаторівневого сигналу на скритність системи зв'язку на основі *SHDSL* технологій. Проведена оцінка завадозахищеності ЦСПИ при дії штучних одночастотних завад при безпосередньому підключенні порушника до кабельної лінії зв'язку.

Ключові слова: імітаційна модель, цифрова система передачі інформації, легітимний канал, відвідний канал, вірогідність бітової.

In the article the new simulation model of wiretap channel is offered for wire communication networks on the basis of *SHDSL* of technologies, allowing to estimate as secrecy and immunity noise systemof DTS at physical level. New data are got about influence of the concerted filtration of linear multilevel signal on secrecy of communication network on the basis of *SHDSL* of technologies. The estimation of immunity noise DTS is conducted at influence of artificial frequency hindrances during the direct connecting of violator to the cable line.

Keywords: simulation model, digital transmission system, legitimate channel, wiretap channel, bit error probability.

Рецензент: д.т.н., проф. Хорошко В.О.
Надійшла 28.01.2011