УДК 621.391.7

И.В. ШИНКАРЕНКО, А.А. ДУДКА, канд. техн. наук, А.И. ЦОПА, канд. техн. наук

АНАЛИЗ СТРУКТУРНОЙ СКРЫТНОСТИ МНОГОУРОВНЕВЫХ ЛИНЕЙНЫХ СИГНАЛОВ ЦИФРОВЫХ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ НА ОСНОВЕ ШИРОКОПОЛОСНЫХ *xDSL* ТЕХНОЛОГИЙ

Введение

Потенциальная структурная скрытность сигналов является одним из важнейших требований информационной безопасности ведомственных систем связи (ВСС). При этом задачи по обеспечению скрытности ВСС ставятся, как правило, на сигнальном уровне, что предполагает выбор соответствующих характеристик и параметров сигнала, которые являются переносчиками информации [1].

В проводном сегменте ВСС для передачи мультимедийной информации широко применяются цифровые системы передачи информации (ЦСПИ) с широкополосными *xDSL* технологиями (*Digital Subscriber Line*), которые используют многоуровневые линейные сигналы [2 – 5]. Отметим также, что при построении сетей доступа используют в основном ЦСПИ зарубежного производства, со своими уровнем безопасности и алгоритмами взаимодействия.

В ряде работ [6, 7] на основе известного метода определения потенциальной структурной скрытности, не требующего знания алгоритма обработки сигнала в приемнике-обнаружителе нарушителя, проведен анализ структурной скрытности широкополосных сигналов, используемых в беспроводном сегменте ВСС. Однако анализ структурной скрытности сигналов, применяемых в проводных системах связи, пока отсутствует, что не позволяет провести комплексную оценку защищенности интегрированных ВСС от перехвата информации.

Цель работы – устранить существующий пробел и провести оценку потенциальной структурной скрытности широкополосных линейных сигналов, используемых в различных видах *xDSL* технологий, а также определить пути ее увеличения.

Основная часть

Потенциальная структурная скрытность определяется числом двоичных измерений (диз), которые необходимо осуществить для раскрытия структуры линейного сигнала. Общее выражение для потенциальной структурной скрытности имеет вид [8]:

$$S_P = \log_2 A \ \text{[диз]}, \tag{1}$$

где A – ансамбль (арсенал) реализаций, определяемый количеством всех возможных значений каких-либо параметров сигнала.

Такими параметрами могут быть несущая частота, амплитуда, вид модуляции, структура линейного кода, параметры формы и временные характеристики сигнала, а также другие специфические параметры, зависящие от физического уровня конкретной технологии передачи сигналов. В общем случае скрытность зависит от способа построения конкретного вида сигнала, используемого для переноса информации.

Так как в современных проводных ЦСПИ применяются составные сложные сигналы, то структурная скрытность S_Σ в этом случае будет суммой структурной скрытности отдельных элементов сигнала

$$S_\Sigma = S_1 + S_2 + .. + S_i = \log_2 A_1 + \log_2 A_2 + ... + \log_2 A_i \ \text{[диз]}, \tag{2}$$

где A_1, A_2, ... A_i – количество (арсенал, ансамбль) всех возможных значений каждого из i-параметров составного сигнала.

Рассмотрим сначала задачу поиска и перехвата линейного сигнала проводной ЦСПИ на основе *xDSL* технологий с неизвестной несущей частотой в диапазоне частот от f_1 до f_2. Теоретически для абсолютно точного решения этой задачи потребуется измерительная процедура бесконечной продолжительности.

Однако на практике время и точность любых измерений ограничена как возможностями аппаратуры нарушителя, так и практической целесообразностью. В рассматриваемом случае минимальное значение допустимой ошибки поиска сигнала по частоте может быть обусловлена, например, собственной нестабильностью частоты сигнала *xDSL* передатчика, влиянием ошибки измерения несущей частоты в приемнике-обнаружителе на качество приема перехватываемого сигнала и т.п.

Как известно [9], при описании статистических свойств какой-либо непрерывной случайной величины x обычно используется функция плотности вероятностей $w(x)$. Если устройство разведки частотного диапазона нарушителя не располагает какими-либо сведениями о рабочей частоте перехватываемого сигнала, то целесообразно использовать функцию равномерной плотности вероятностей $w(f)$ рабочей частоты f.

Предположим, что значения частоты сигнала легитимного модема $f_{ЛК}$ находятся в диапазоне D_f от частоты f_1 до частоты f_2 ($D_f = f_2 - f_1$) и имеют равномерную плотность вероятностей вида

$$w(f) = \frac{1}{D_f}. \qquad (3$$

Если шаг дискретизации по частоте Δf в приемнике-обнаружителе выбран так, что $N = D_f / \Delta f$ является целым числом (N – число одинаковых интервалов дискретизации), а среднеквадратическое отклонение (СКО) частоты σ_f для равномерной плотности вероятностей $\sigma_f = D_f / \sqrt{12}$ [9], то вероятность попадания P_n значения частоты $f_{ЛК}$ в заданный интервал поиска согласно [8]

$$P_n = \frac{1}{N} = \frac{\Delta f}{D_f} = \frac{\Delta f}{\sigma_f \cdot \sqrt{12}}. \qquad (4$$

В этом случае потенциальную скрытность сигнала S_f (1), которая определяется числом возможных значений параметра частоты легитимного модема $f_{ЛК}$ в диапазоне частот разведки сигнала, можно найти из выражения

$$S_f = -\sum_{n=1}^{N} P_n \cdot \log_2 P_n = \log_2(N) = \log_2\left(\frac{D_f}{\Delta f}\right) = \log_2\left(\frac{\sqrt{12}\cdot\sigma_f}{\Delta f}\right) = \log_2\left(\frac{\sigma_f}{\Delta f}\right) + 1{,}792. \qquad (5$$

График зависимости потенциальной скрытности S_f от отношения шага дискретизации Δf к СКО приведен на рис. 1.

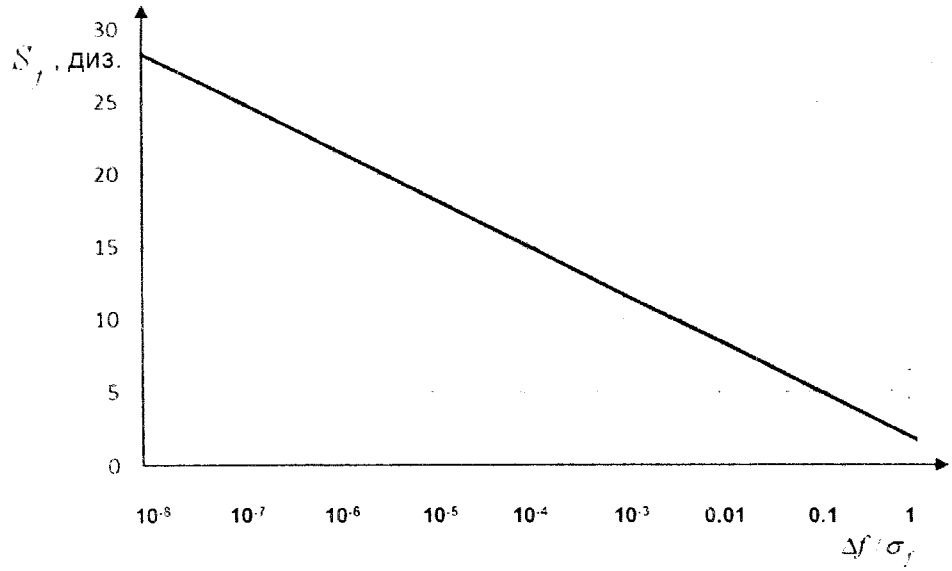

Рис. 1. График зависимости потенциальной скрытности S_f от отношения $\Delta f / \sigma_f$

Из рис. 1 видно, что увеличение стабильности частоты тактового генератора легитимного модема $f_{ЛК}$ (например, менее 10^{-6} *ppm*), приводящее к необходимости уменьшения шага дискретизации Δf в приемнике-обнаружителе нарушителя существенно повышает потенциальную структурную скрытность линейного сигнала *xDSL* модема.

Для увеличения скорости передачи информации в канале связи несущая частота $f_{ЛК}$ модема обычно модулируется; к примеру, может использоваться многопозиционная квадратурная амплитудная модуляция *QAM-M* (*Quadrature Amplitude Modulation*), уровень *M* которой задает количество различных значений вектора модулированного сигнала, т.е. $M = 2^n$ – размерность ансамбля сигналов, где $n = 2,3,...15$ [2]. Тогда для сигнала *QAM-M* количество вариантов соответствия каждой точке сигнального ансамбля символа, который состоит из n бит, составляет $M!$ без учета ограничений кода Грея. Соответственно, структурная скрытность сигнального созвездия в виде прямоугольной решетки с *M* точками

$$S_{QAM} = \log_2(M!) \ \text{[диз]}. \tag{6}$$

В современных проводных ЦСПИ широко используется система сигналов с многими поднесущими частотами, в основе которой лежит использование быстрого преобразования Фурье при синтезе сигнала на передаче и демодуляции его на приеме. Этот вид модуляции стандартизирован *ANSI* в качестве метода линейного кодирования для систем передачи данных и называется дискретной мультитоновой модуляцией *DMT* (*Discrete Multi-tone Modulation*).

Метод модуляции *DMT* основывается на принципе разделения диапазона частот, в котором осуществляется передача данных (от 35 *кГц* до 30 *МГц*), на N поддиапазонов шириной в 4,3125 *кГц* (8,6250 *кГц*). В зависимости от качества проводного канала связи каждая из N поднесущих частот использует *QAM* модуляцию со своим уровнем модуляции M_i, т.е. каждая поднесущая f_i несет n_i бит информации. Учитывая то, что база сигнала *DMT* приблизительно равна количеству поднесущих $B_C \approx N$, то потенциальная скрытность сигнала

$$S_{DMT} = \log_2(N) \ \text{[диз]}. \tag{7}$$

На рис. 2 приведены графики зависимости потенциальной скрытности сигналов *DMT* $S_{DMT\ QAM} = \log_2(N) + \log_2(M!)$ от количества поднесущих частот N и различных значений размерности M ансамбля сигналов *QAM*.

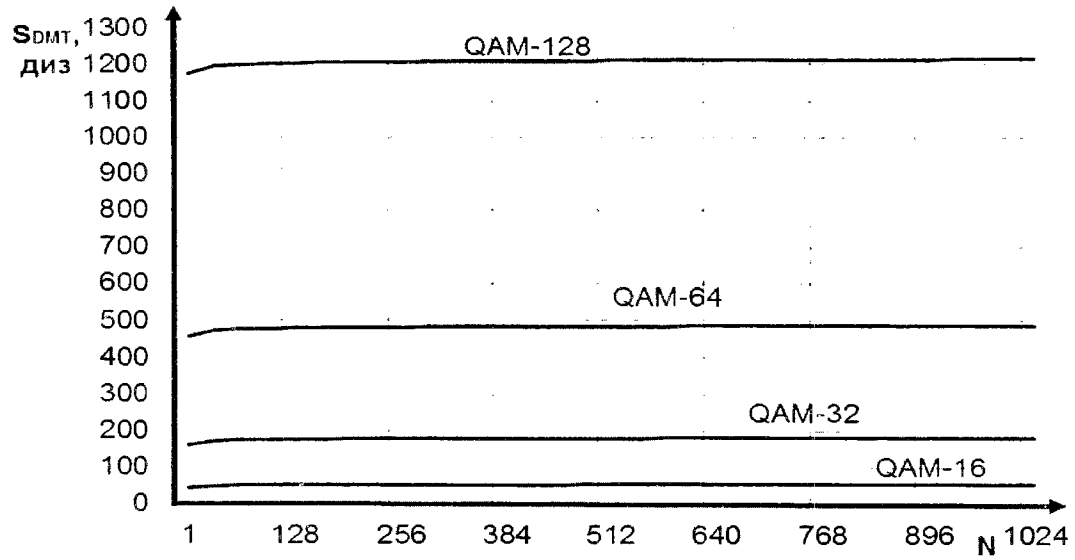

Рис. 2. Графики зависимости потенциальной скрытности $S_{DMT\ QAM}$ от числа поднесущих частот N и уровня M модуляции *QAM*

Как видно из графиков, скрытность сигналов *DMT* повышается с увеличением числа поднесущих частот f_i, кроме того на величину S_{DMT} существенно влияет размерность *QAM*.

Арсенал сигналов *DMT* можно существенно повысить, если использовать случайную перестановку передаваемых символов между поднесущими частотами f_i, согласованную между передатчиком и приемником. В этом случае арсенал $A_{DMT} = N!$ и потенциальная структурная скрытность увеличивается $S_{DMT} = \log_2(N!)$.

Возможна также реализация более сложного алгоритма взаимодействия между передатчиком и приемником ЦСПИ при реализации псевдослучайной перестройки частоты (ППЧ поднесущих по согласованному закону. Это позволит значительно увеличить потенциальную скрытность сигналов *DMT* $S_{ППЧ} = 0{,}697 \cdot N \cdot \log_2 N$ [8].

Используя приведенные выше выражения для потенциальной скрытности отдельных параметров линейных сигналов, проведем общую оценку скрытности основных *xDSL* технологий, которые применяются при построении проводных ЦСПИ для ВСС.

Симметричная технология *SHDSL* использует сигналы многоуровневую амплитудно-импульсную модуляцию *PAM-M* (*Pulse Amplitude Modulation*) с уровнем модуляции $M = 4,8,16,32,64,128$ и формированием формы линейного сигнала с помощью фильтра приподнятого косинуса *RC* (*Raise Cosines*) (арсенал состояний коэффициента сглаживания фильтра $A_{RS} = 128$). Тогда потенциальная скрытность будет определяться арсеналом состояний всех составляющих сигнала

$$S_{SHDSL} = S_f + S_{QAM} + S_{RS} = \log_2\left(\frac{\sqrt{12}\cdot\sigma_f}{\Delta f}\right) + \log_2(M!) + \log_2(A_{RS}). \qquad (8$$

Ассиметричная технология *ADSL* использует многочастотные *DMT* сигналы с модуляцией *QAM*. Количество поднесущих частот $N = 256 \setminus 512$, а уровень *QAM* модуляции M

может меняться в широких пределах $(QAM-4, QAM-8, QAM-16, ..., QAM-32768)$. Уровень модуляции для каждой поднесущей частоты устанавливается отдельно и зависит от неравномерности частотной характеристики кабельной линии связи, а также от уровня шума в системе связи.

Потенциальная скрытность будет определяться арсеналом состояний всех составляющих сигнала

$$S_{ADSL} = S_f + S_{DMT} + S_{QAM} = \log_2\left(\frac{\sqrt{12}\cdot\sigma_f}{\Delta f}\right) + \log_2(N) + \log_2(M!). \quad (9)$$

Высокоскоростная технология *VDSL* использует многочастотные *DMT* сигналы с модуляцией *QAM*. Количество поднесущих частот $N = 1024 \setminus 2048$, а уровень *QAM* модуляции M может меняться в широких пределах в зависимости от отношения сигнал/шум в проводном канале связи. Кроме того, в этой технологии для уменьшения перекрестных искажений в многопроводных линиях связи реализован принцип дискретного изменения уровня мощности P_C линейного сигнала в пределах от -17 до +17 *дБм* с шагом 1 *дБм* (арсенал $A_P = 34$). Потенциальная скрытность для технологии *VDSL* будет определяться арсеналом состояний всех составляющих линейного сигнала

$$S_{VDSL} = S_f + S_{DMT} + S_{QAM} + S_P = \log_2\left(\frac{\sqrt{12}\cdot\sigma_f}{\Delta f}\right) + \log_2(N) + \log_2(M!) + \log_2(A_P). \quad (10)$$

Используя выражения (8) – (10), можно провести сравнительный анализ структурной скрытности линейных сигналов различных *xDSL* технологий.

В таблице приведены данные о потенциальной структурной скрытности *SHDSL*, *ADSL* и *VDSL* технологий при различных значениях отдельных параметров линейного сигнала [10].

Вид технологии	Тип сигнала	Количество поднесущих N	Уровень модуляции M	Скрытность S, диз
HDSL	*PAM-16*	1	16	65
SHDSL	*PAM-128*	1	128	747
ADSL	*DMT QAM-256*	256	256	1720
ADSL2	*DMT QAM-1024*	512	1024	8839
VDSL	*DMT QAM-2048*	1024	2048	19700
VDSL2	*DMT QAM-4096*	2048	4096	43479

Полученные данные свидетельствуют о высокой потенциальной структурной скрытности современных цифровых технологий передачи информации по кабельным каналам связи. Особенно это относится к *VDSL* технологиям, использующим для передачи информации большое количество поднесущих частот и высокие уровни модуляции *QAM*.

Для увеличения структурной скрытности ВСС необходимо не только, по возможности, расширять ансамбли применяемых сигналов, но и использовать оригинальные методы формирования линейного сигнала в ЦСПИ собственной разработки, что позволит применять *xDSL* технологии в проводных сегментах ВСС для доступа к специализированным базам данных и передачи служебной информации.

Заключение

1) На основе известной методики проведена оценка потенциальной структурной скрытности многоуровневых линейных сигналов проводных ЦСПИ и получены новые данные о структурной скрытности сигналов современных *xDSL* технологий.

2) Для увеличения структурной скрытности сигналов, которые используются в *xDSL* технологиях, необходимо, по возможности, расширять ансамбль используемых сигналов, в том числе и используя дополнительные возможности физического уровня этих технологий.

3) Для увеличения защищенности ВСС необходимо использовать отечественные ЦСПИ, в которых реализованы оригинальные алгоритмы повышения структурной скрытности сигнала.

Список литературы: 1. *Хорошко В. А., Чекатков А. А.* Методы и средства защиты информации. – К. : ЮНИОР, 2003. – 504 с. 2. *Балашов В. А., Лашко А.Г., Ляховецкий Л. М.* Технологии широкополосного доступа *xDSL*. – М. : Эко-Трендз, 2009. – 256 с. 3. *Цопа А. И.* Выбор линейных сигналов и анализ их спектральных характеристик в системах передачи информации с использованием *xDSL* технологий // Радиотехника. – 2006. – Вып. № 146. – С. 66-74. 4. *Шинкаренко И. В.* Экспериментальная оценка защищенности мультимедийных цифровых систем передачи информации на основе *SHDSL* технологий / И. В. Шинкаренко, А. И. Цопа // Известия Вузов. Радиоэлектроника. – Київ : НТУ «КПИ», 2011. – Т. 54. – Вип. 5. – С. 30-36. 5. *Дудка А. А.* Прогнозирование зон обнаружения для кабельных линий связи в сети абонентского доступа на основе *VDSL* технологий / А. А. Дудка, А. И. Цопа, В. М. Шокало // Сучасний захист інформації. – Київ : ДУІКТ, 2010. – Вип. 3. – С. 45-53. 6. *Захарченко Н. В.* Структурная скрытность таймерных сигналов в системах с кодовым разделением сигналов / Н. В. Захарченко, В. В. Корчинский, Б. К. Радзимовский // Восточно-европейский журнал передовых технологий. – 2011. – №2/9(50). – С. 7-9. 7. *Кувшинов О. В., Вознюк Р. В.* Оцінка структурної критності широкосмугових сигналів // Зб. наук. праць ВІТІ НТУ «КПІ». – 2011. – № 1. – С. 106-111. 8. *Каневский З. М.* Теория скрытности / З. М. Каневский, В. П. Литвиненко. – Воронеж : ВГУ, 1991. – 144 с. 9. *Вентцель А. Д.* Курс теории случайных процессов. – М. : Наука. Физматлит, 1996. – 400 с. 10. *Цопа А. И.* Оценка предельной производительности проводных каналов связи с различными *xDSL* технологиями // Радиотехника. – 2010. – Вып. № 160. – С. 234-246.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 13.08.2011