

III Висновки

Використання для захисту інформації волоконно-оптичної системи передачі з спектральним розділенням каналів, по частині яких передається маскуючий сигнал, та постійним рефлектометричним моніторингом лінійного тракту дозволить значно підвищити рівень захисту інформації на волоконно-оптичних мережах зв'язку.

Література: 1. Каток В. Б., “Манько А. А. Защита информации в оптических линейных трактах методом спектрального разделения” Ювілейна науково-технічна конференція “Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні” Україна, Київ, 9-11 червня 1998р.

УДК 621.391.052

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ МЕТОДА ЗАЩИТЫ ИНФОРМАЦИИ В ОПТИЧЕСКИХ ТРАКТАХ

Виктор Каток, Юлий Лев

Научно-инженерный центр линейно-кабельных сооружений при Государственном комитете связи и информатизации Украины, г. Киев

Анотація: Наведена блок-схема імітаційної моделі цифрового обладнання передачі та прийому інформації, в якому символи 1 і 0 кодуються М-последовністю. Показано, що довжина кодових М-последовностей, яка перевищує 15 символів, це обладнання забезпечує велику завадостійкість і скритність передачі інформації.

Summary: The simulation model bloc-diagram of the digital information transmitting and receiving equipment where symbols 1 and 0 are coordinated with M-sequences is brought. It is shown that the equipment provides with high interference the stability and hide of date transmission if the length of M-sequences code exceed 15 symbols.

Цифрови тракти передачі, безпека інформації, кодування символів, М-последовність.

I Введение

В данном докладе приведены результаты имитационного моделирования системы передачи, в которой используется метод защиты информации, предложенный в [1,2]. В передатчике этой системы символам 1 и 0 входного цифрового потока со скоростью передачи R_i ставятся в соответствие кодовые М-последовательности [3], причем М-последовательность кодирующая символ 1 инверсна М-последовательности, которая кодирует символ 0. Скорость передачи цифрового потока на выходе передатчика $R_n = m_i R_i$, где m_i – длина кодового блока.

Сигнал на выходе передатчика имеет циклическую структуру; заголовок цикла (цикловой синхросигнал) также представляет собой М-последовательность, длина которой $m_{дс} > m_i$.

В приемнике осуществляется тактовая и цикловая синхронизация и декодирование – вычисление коэффициента взаимной корреляции K между принятыми кодовыми блоками и эталонной М-последовательностью, соответствующей символу 1. При $K > 0$ принимается решение, что передавался символ 1, при $K < 0$ – что передавался символ 0.

II Имитационная модель

На рисунке 1 представлена блок-схема алгоритма имитационного моделирования. На схеме изображены основные компоненты программного обеспечения, которые последовательно осуществляют преобразования данных, соответствующие всем узлам тракта “передатчик – линия - приемник”. Результаты работы каждого компонента заносятся в соответствующие файлы; файл, сформированный на каждом шаге моделирования, является входом следующего компонента программы.

Результаты выполнения программы моделирования заносятся в протокол – текстовый файл, содержащий

сведения о работе всех компонентов модели и анализ результатов моделирования при заданных исходных данных.

Модуль программы ГПСП (генератор псевдослучайной последовательности) моделирует последовательность битов, поступающую на вход передатчика.

Модуль ИВС (имитатор входного стыка) в начале и в конце каждого периода ПСП вводит специальные блоки заданной длины. Это необходимо для того, чтобы при декодировании проанализировать скорость и точность вхождения приемника в цикловой синхронизм.

Модуль Код (имитатор кодера) формирует кодовые М-последовательности, соответствующие символам 1 и 0, цикловой синхросигнал и полные циклы передачи, т.е. моделирует линейный сигнал.

Модуль ИЛ (имитатор линии) состоит из двух частей. Сначала моделируются детерминированные искажения символов линейного сигнала, затем с искаженным сигналом суммируются случайные числа, моделирующие флуктуационную помеху (белый шум) с заданным среднеквадратичным значением.

В модуле Рег (имитатор регенератора) выделяется тактовый синхросигнал и осуществляется восстановление формы импульсов.

Модуль Дек (имитатор декодера) имитирует процессы цикловой и блочной синхронизации и декодирования.

Модуль анализа результатов моделирования осуществляет обработку файлов всех шагов моделирования и выдает таблицу статистики ошибок.

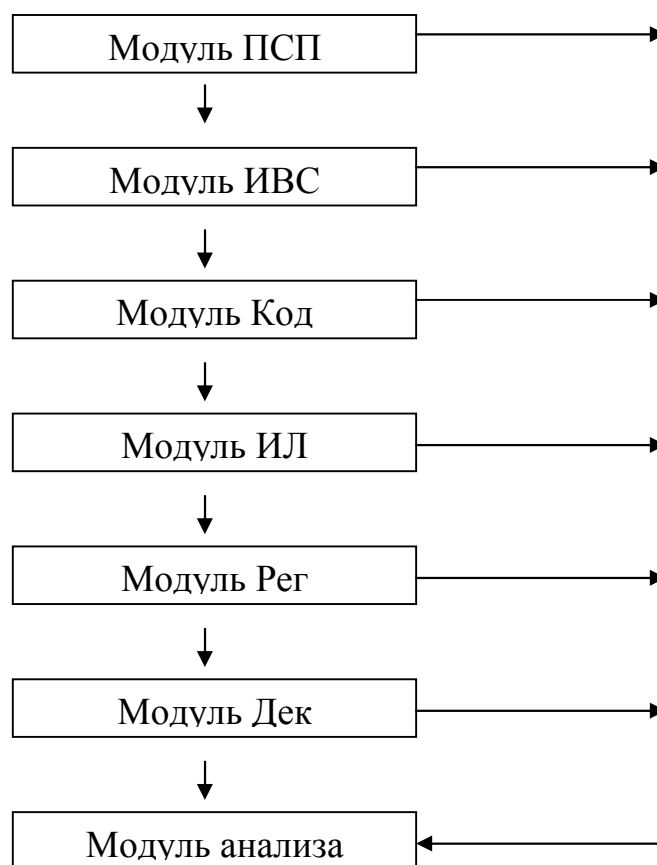
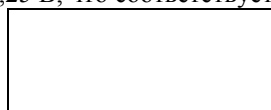


Рисунок 1 - Блок-схема алгоритма имитационного моделирования

III Результаты моделирования

Моделирование осуществлялось при скоростях передачи входных цифровых потоков $R_1 = 2\,048$ кбит/с и $R_2 = 8\,448$ кбит/с и скорости передачи в линии $R_{\text{л}} = 139\,264$ кбит/с.

При моделировании на вход передатчика подаются стандартные псевдослучайные последовательности длиной $(2^m - 1)$ битов. Дисперсионные искажения волоконного световода имитируются заменой всех переходов 0-1 и 1-0 на гладкую функцию $\sin^2 \omega t$; значение ω выбрано так, чтобы длительность фронта импульса на выходе была равна тактовому интервалу линейного сигнала. Для имитации помехи в модели использован гауссов процесс с независимыми значениями и нулевым средним. Передача символа 0 имитируется напряжением $U(0)=0$ В, передача символа 1 - $U(1)=1$ В. Имитировались шумы со среднеквадратическим значением $\sigma = 0,25$ В; 0,5 В; 0,75 В; 1,00 В; 1,25 В, что соответствует защищенности на входе регенератора



12 дБ; 6 дБ; 2,5 дБ; 0,0 дБ; и минус 1,9 дБ

(1)

Результаты имитационного моделирования приведены в таблице 1.

Результаты имитационного моделирования

Таблица 1

R_i , кбит/с	A_z , дБ	$N_{\text{рег}}$	$N_{\text{ош.рег}}$	$K_{\text{ош.рег}}$	$N_{\text{дек}}$	$N_{\text{ош.дек}}$	$K_{\text{ош.дек}}$
2048	12,0	34816000	735853	0,021	512000	0	0,00000
	6,0		5498297	0,158		0	0,00000
	2,5		8785050	0,252		6	0,00001
	0,0		10740453	0,308		390	0,00076
	-1,9		11995805	0,345		2936	0,00573
8448	12,0	8704000	184118	0,021	528000	0	0,00000
	6,0		1374262	0,158		487	0,00092
	2,5		2195356	0,252		9525	0,01804
	0,0		2684349	0,308		30497	0,05776
	-1,9		2998235	0,344		54907	0,10399

где:

$N_{\text{рег}}$ - число символов (битов) на выходе регенератора;

$N_{\text{ош.рег}}$ - число символов, регенерированных ошибочно вследствие искажений и аддитивной помехи;

$K_{\text{ош.рег}} = \frac{N_{\text{ош.рег}}}{N_{\text{рег}}}$ — коэффициент ошибок на выходе регенератора;

$N_{\text{дек}}$ - число символов (битов) на выходе декодера;

$N_{\text{ош.дек}}$ - число символов (битов) декодированных ошибочно;

$K_{\text{ош.дек}} = \frac{N_{\text{ош.дек}}}{N_{\text{дек}}}$ — коэффициент ошибок на выходе декодера.

IV Заключение

Имитационное моделирование показало, что предложенный в [1,2] метод обеспечивает высокую помехоустойчивость, защищенность от несанкционированного доступа и имитостойкость при передаче цифровых потоков первого и второго уровней передачи цифровой информации (2048 кбит/с и 8448 кбит/с) по четверичному цифровому тракту (139264 кбит/с).

Аналогичные результаты будут иметь место для любых других скоростей передачи информации при условии, что символы входного цифрового потока кодируются достаточно длинными M -последовательностями.

Литература: 1. Каток В.Б., Конофольский В.А., Лев О.Ю., Лев Ю.О., Охрименко В.М. Винахід "Комплект обладнання передачі і прийому інформації". Рішення Держпатенту України про видачу патенту від 08.10.1998 р. 2. В.Б. Каток, Ю.А. Лев. Метод обеспечения высокой помехоустойчивости, скрытности и имитостойкости передачи информации в цифровых оптических трактах. Перша науково-технічна конференція "Правове нормативне та метрологічне забезпечення системи захисту інформації в Україні", Киев, июнь 1998 г. 3. М.Б.