В работе излагается принцип построения генераторов псевдослучайных чисел, основанных на свойстве сложения псевдослучайных последовательностей со сдвигом по фазе. В результате были получены данные, характеризующие выигрыш в энергопотреблении в сравнении с классическими структурами.

Данный метод позволяет синтезировать менее энергоемкие генераторы без существенного увеличения аппаратных затрат, увеличивается только количество сумматоров по модулю два.

СТОЙКОСТЬ ЭЛЕКТРОННОГО ОБОРУДОВАНИЯ К ВОЗДЕЙСТВИЮ ЭЛЕКТРОМАГНИТНЫХ ИМПУЛЬСОВ

Л.М. ЛЫНЬКОВ, Г.И. ВЛАСОВА

Воздействие электромагнитного импульса, генерируемого при ядерных испытаниях, может привести к необратимому повреждению широкого спектра электрического и электронного оборудования, в особенности компьютеров и радио или радарных приемников, другого телекоммуникационного оборудования, а также вводимая в мире практика использования электронных бомб в экстремальных (военных) ситуациях для подавления информационных инфраструктур.

Основой технологической базы обычных (неядерных) электромагнитных бомб являются генераторы со сжатием потока с помощью взрывчатки, которые представляют собой устройство в компактной упаковке и производят электрическую энергию порядка десятков МДЖ.

Поражающее действие заключается в поглощении энергии через антенные комплексы ("парадный вход"), генерации больших переходных токов ("задний вход") на электрических кабелях или проводниках. Микроволновое оружие, функционирующее в сантиметровом и миллиметровом диапазонах, имеет дополнительный механизм проникновения энергии в оборудование через вентиляционные отверстия, щели между панелями и недостаточно экранированными интерфейсами.

Нацеливание электромагнитных бомб осуществляется методами обычной и технической разведки. Поскольку излучения от компьютерных мониторов, периферии, процессоров, источников питания различны по частоте и модуляции требуется соответствующая система пеленгации таких источников.

Основные методы обороны против электромагнитных бомб состоит в необходимости помещения оборудования в специальные электропроводящие клетки. Весьма существенным следует учитывать "мерцающие" неисправности, возникающие в полупроводниковых приборах, которые сложно диагностируются и ремонтируются.

Коммуникационные сети должны применять топологию с достаточной избыточностью и механизмами ликвидации сбоев, что не позволит пользователю электромагнитного вооружения вывести из строя данную сеть одной атакой.

Ограничения по применению электромагнитных систем вооружений:

- повышенная устойчивость лампового оборудования;
- трудности оценки повреждаемости субъектов из-за возможного затухания электромагнитного сигнала в атмосфере;
- возможность повреждения собственных электронных средств.

Представляется проблемным утверждение разработчиков электромагнитного оружия о "гуманном" воздействии на живые организмы, ведь может повреждаться сетчатка глаз человека, нарушаться излучения электромагнитных полей мозгом.

Для эффективной защиты человеческого организма от возможного контактирования с локальным импульсным электромагнитным воздействием необходима разработка специальных укрывных материалов, применяемых как средства индивидуальной защиты, так и средства для строительства, поглощающие электромагнитные поля.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКИХ СИСТЕМ ПОЧТОВОЙ СВЯЗИ

С.В. ЖДАНОВИЧ, Т.Г. КОВАЛЕНКО

Основными направлениями деятельности по вопросам информационной безопасности информационно-технологических систем почтовой связи являются:

проведение научно-исследовательских работ и разработка нормативных и правовых документов в области информационной безопасности в сфере почтовых технологий;

подготовка технико-экономических обоснований по выбору, созданию, внедрению и развитию средств и систем информационной безопасности на предприятия почтовой связи;

разработка стандартов, технических требований в области безопасности для почтовой связи с учетом международных рекомендаций и стандартов;

разработка методов по совершенствованию деятельности предприятий почтовой связи в области информационной безопасности;

разработка программных продуктов по организации и осуществлению информационной безопасности для информационно-технологической сети почтовой связи и автоматизированных систем обработки информации;

проектирование и внедрение систем информационной безопасности на предприятиях почтовой связи;

организация технической учебы, повышения квалификации сотрудников предприятий почтовой связи в области информационной безопасности.

ВЫБОР КОДА ДЛЯ СИСТЕМЫ СВЯЗИ, ОБЕСПЕЧИВАЮЩЕЙ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

А.И. МИТЮХИН

Одним из требований, предъявляемых к современным системам связи является способность противостоять подслушиванию и преднамеренным помехам. Во избежание обнаружения кодированного сигнала несущего сообщение, передача в такой системе ведется с минимальным излучением мощности. Кодирование реализуется посредством использования кодов большой мощности $M=q^k$, где q и k основание и размерность кода соответственно. При этом период сигнала $T=n/f_т$ должен быть соизмерим со временем между сменами кодов ($f_т$ – тактовая частота в системе, n – значность кода).

Обнаруживающая способность подслушивающей стороны ограничивается отношением Q энергии $E_в$ (приходящейся на один бит сообщения) перехваченного сигнала к спектральной плотности мощности шума N_o. Возникает задача выбора класса кодов, определения его мощности, других его параметров, обеспечивающих минимальную вероятность ошибки декодирования $P_{ош}$ в основном канале при заданном минимальном отношении $Q=E_в/N_o$.

Пусть {G} является [n, k]-кодом над полем из q элементов. В системе используется M кодовых слов кода G. Для удобства назовем совокупность M действительных векторов $X=(x_1...x_n)$ множеством сигналов

$G=\{x^1,x^2,...,x^S,...,x^M\}$, $S\in\{1,2,...,M\}$.

Оптимальная процедура декодирования M сигналов на основе стратегии максимального правдоподобия заключается в нахождении номера S одного из M корреляторов с максимальным по абсолютной величине выходным сигналом. Декодирование сводится к сравнению входного вектора $Y=(x+E)$ с каждым словом кода G, где $Y=(y_0y_1...y_i...y_{n-1})$; $X=(x_0x_1...x_i...x_{n-1})$, $X\in G$; $E=(e_0e_1...e_i...e_{n-1})$ – вектор ошибок; $y_i,x_i,e_i\in\{0,1\}$. При условии, что все кодовые слова равновероятны, вектор Y декодируется в ближайшее по расстоянию Хэмминга кодовое слово. Это равносильно определению номера i, для которого вычисляется значение

$|F_i| = G\cdot Y^T$, для $i\in\{1,2,...,M\}$,

где $F_i=(f_0f_1...f_i...f_{n-1})^T$; G – матрица кодовых слов кода.

Если взаимное влияние сигналов отсутствует, то на величину вероятности ошибки декодирования $P_{ош}$ кодового слова X^S влияет только отношение сигнал/шум Q. Для того, чтобы в системе не было взаимного влияния сигналов должно выполняться условие

$R_{X^jX^S}(\tau)=0$ при всех $j\neq S$; $j, S\in\{1,2,...,M\}$.

Здесь $R_{X^jX^S}(\tau)=n-2wt(x^j+Д^\tau x^S)$, (1)

для $0\le\tau\le n-1$ — взаимная корреляционная функция; Д — оператор циклического сдвига последовательности X на одну позицию влево.

С точки зрения получения минимальной величины $P_{ош}$ или помехоустойчивого декодирования (приема в условиях воздействия организованных помех), множество сигналов {G} необходимо характеризовать коэффициентами ВКФ (1). Таким образом, оценка $P_{ош}$ для выбранного кода будет зависеть не только исключительно от отношения ($E_в/N_o$), но и корреляционной матрицы кодированных сигналов.

Рассмотрим, как можно осуществить реальный выбор кода для скрытной передачи информации. Будем исходить из того, что обнаружение подслушивателем передачи состоит в некогерентном накоплении энергии сигналов за период кодированных сообщений. В системе предусмотрена частая смена кодовых слов кода, затрудняющая правильное декодирование подслушивающей стороне. Такая тактика применения кодов требует тщательного анализа ВКФ больших множеств слов.

Известно, что большой совокупностью множеств слов кода G обладает двоичный симплексный $[2^k, k]$-код. К его достоинствам можно также отнести простоту формирования и относительно несложное декодирование. Недостатком симплексных кодов и их производных (Голда, Касами, ЛРД и др.) является сравнительно малое множество слов с хорошими взаимно-корреляционными свойствами. В качестве примера приведем М-код длиной 31. Всего существует 6 различных проверочных полиномов h(x) над полем GF(2) длиной 31. Полиномы h(x) запишем в восьмеричном представлении, в виде коэффициентов многочленов и в виде многочленов (см. табл.).

Примитивные многочлены степени 5

$h_1(x)$	45	100101	x^5+x^2+1
$h_2(x)$	75	111101	$x^5+x^4+x^3+x^2+1$
$h_3(x)$	67	110111	$x^5+x^4+x^2+x+1$
$h_4(x)$	51	101001	x^5+x^3+1