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;