чтения, модификации или удаления. Основное назначение МБ в системе - аутентификация (удостоверение подлинности) кристалла на всех этапах производства и эксплуатации ЭПК. Ключи с течением времени могут сменяться, в том числе дистанционно, или одновременно могут действовать несколько ключей.

Важным элементом, обеспечивающим безопасность системы, является бесполезность такого занятия, как получение информации о ключах посредством логического анализатора — информация при очередном сеансе связи повторяться не будет и логику смены данных проследить невозможно.

Система организована так, что защита транспортного пути кристалла может производиться на ключах, которые не используются в системе. Таким образом изготовитель кристаллов не имеет возможности получить информацию о рабочих ключах. Смена транспортных ключей производится на каждой партии, и поэтому вероятная утечка ключевой информации не приведет к взлому системы.

Хищение МБ из таксофона или вместе с таксофоном также не позволяет взломать систему в целом из-за недоступности ключевой информации. Для защиты от имитации ЭПК, кроме традиционных методов в системе предусмотрена модификация индивидуального кода карты после каждого сеанса связи.

Для повышения стойкости системы к взлому в ней используются МБ с различными ключами на этапах изготовления и эксплуатации ЭПК. При изготовлении кристалла изготовителю передается МБ с транспортными ключами А1-А16. Изготовитель использует эти ключи для записи в кристалл зашифрованного транспортного кода и для создания транспортной карты, содержащей опять таки зашифрованный транспортный ключ. При этом для каждой партии кристаллов используются один из ключей А, а по истечении определенного времени может быть произведена полная замена ключей. Прочитать исходные ключи А в открытом виде и получить информацию о рабочих ключах Б изготовитель кристаллов не может.

После изготовления ЭПК транспортная карта и МБ с ключами Аi используются для входа в режим персонализации карты. Войти в этот режим можно только в случае, если зашифрованные транспортные ключи в кристалле и транспортной карте будут успешно расшифрованы и опознаны МБ с ключами А. Непосредственно для персонализации используется МБ с рабочими ключами Бi, которые также должны содержать МБ, установленные в таксофонах. По окончании персонализации транспортный ключ из карты удаляется, но в закрытую для чтения область памяти записывается индивидуальный ключ карты (ИКК) длиной 256 бит, зашифрованный на рабочем ключе Бi. Изготовителю таксофонов передается МБ с рабочими ключами Б1-Б16, также недоступными для чтения, модификации и удаления. При этом ему неизвестны транспортные ключи.

В настоящее время в системе используется лишь малая часть возможностей, предоставляемых МБ. Поэтому в случае внедрения система имеет дальнейшие перспективы развития, например в части шифрации информационного обмена между таксофоном и АТС, защиты от несанкционированного подключения к линиям связи и т.д.

Система в целом может использоваться и для других применений, где требуется использование предварительно оплаченного кредита. В настоящее время все компоненты системы освоены в серийном производстве в НИРУП "ЦНИИТУ" Научно-производственного объединения "Центрсистем" и прошли эксплуатационные испытания на телефонной сети Республики Беларусь. Результаты позволяют говорить о высокой степени защищенности и хорошем качестве ЭПК.

Литература

1. J. Glave. Pirate Cash in on Weak Chips // Wired News. 1998. N 218 (May).
2. Deutsche Telecom hit by Eurochip reload fraud //User Guide 99. P. 57.

СИНТЕЗ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

А.А. ШАМШУР

В настоящее время генераторы случайных чисел получили широкое распространение благодаря применению в различного рода устройствах для защиты информации от несанкционированного доступа, в средствах встроенного самотестирования и т.д. Рост мобильности устройств выдвигает новые требования ко всем узлам, в том числе и к генератору случайных чисел. Основным требованием в мобильном устройстве является энергопотребление, поэтому на сегодняшний день актуальна проблема построения генератора случайных чисел с наименьшим энергопотреблением.

Известно несколько подходов к решению проблемы энергопотребления: изменение схемы устройства, исключение лишних узлов и т.д.; уменьшение частоты работы, что приводит, однако, к уменьшению производительности; изменение структуры блока.

В данной работе рассматривается внесение структурных изменений в широко распространенную схему генератора псевдослучайных последовательностей на основе сдвигового регистра с линейной обратной связью, известного в англоязычной литераторе как Linear Feedback Shift Register (LFSR). Весь регистр делится на две части, работающие на разных частотах, причем на самой большой частоте — частоте появления наборов на выходе схемы, работает только оконечная часть схемы, вся остальная часть работает на меньших частотах, за счет чего и достигается уменьшение энергопотребления.

Для генерирования выходной псевдослучайной последовательности высокой частоты используется несколько сдвигов одной и той же псевдослучайной последовательности меньшей частоты. После сложения двух последовательностей при помощи сумматора по модулю два, получается так же псевдослучайная последовательность, но уже большей частоты.

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;