О. С. Варламов

ИСТОРИЯ РАЗВИТИЯ ВОЗДУШНЫХ ПАРАМЕТРИЧЕСКИХ АНТЕНН И ВОЗМОЖНОСТЬ ИХ ПРИМЕНЕНИЯ В ЗАДАЧАХ ЗАЩИТЫ ИНФОРМАЦИИ

Проблема создания высоконаправленного звукового поля возникла достаточно давно, одним из первых создать направленный источник звука пытался в конце XIX в. физик-экспериментатор Роберт Вуд, однако его мегафон имел гигантские размеры, большой вес, низкие эксплуатационные характеристики и большую стоимость изготовления.

Компромисс был найден за счет использования параметрической антенны. В 1960-х годах ученые заметили, что из-за нелинейных эффектов в воде появляются более низкие, чем излучаемые, частоты. Это привело к разработке новой математической базы параметрических акустических антенных решеток.

В 1975 г. профессор Техасского университета Дэвид Блэксток и его студентка Мери Беннетт опубликовали статью о том, что им удалось получить слышимые частоты из ультразвука в воздухе. Следующие десятилетия инженеры Мацушита, Денон и Рикох пытались извлечь из этого эффекта практическую пользу. При распространении ультразвука в воздухе звук превращался в слышимый, но коэффициент гармонических искажений доходил до 50 %, в 1997 г. Джозеф Помпеи сконструировал первый практически применимый узконаправленный источник звука.

Использование параметрических антенн возможно в комплексах, где необходимо создать направленное звуковое поле большой интенсивности, например в подавителях диктофонов.

А. А. Варфоломеев, А. М. Коренева, А. А. Краснопевцев, Ю. М. Туманов, В. М. Фомичев

О РЕАЛИЗАЦИИ МЕТОДА ПОЛНОГО ОПРОБОВАНИЯ КЛЮЧЕЙ КРИПТОСИСТЕМ В УСЛОВИЯХ РАЗЛИЧНЫХ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ РАСПРЕДЕЛЕННЫХ ВЫЧИСЛЕНИЙ

В рамках Федеральной целевой программы «Научные и научно-педагогические кадры инновационной России» на 2009—2013 годы коллективом кафедры № 42 НИЯУ МИФИ выполняется НИР по изучению эффективности использования систем распределенных вычислений (РВ) для решения задач анализа криптографических систем [1, 2]. На завершившихся этапах НИР исследовалась эффективность реализации метода полного опробования ключей криптографических систем при известных открытом и шифрованном текстах в условиях различных математических моделей РВ [3—5].

Вычислительный потенциал современных вычислительных средств, интегрированных в вычислительные сети, резко и неуклонно возрастает. В связи с этим высока актуальность выполненных исследований НИР, посвященных распределенным вычислениям для полного опробования ключевого множества криптосистем. Распределенные вычисления являются новым мощным средством криптографического анализа [6—8], возникшим в связи с возможностями, предоставляемыми пользователям больших вычислительных сетей.

В работе [9] приведена классификация систем РВ, их архитектура предусматривает наличие координатора, который распределяет вычислительные задания среди участников, выполняющих