УДК 621.391

МЕТОД ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ КАСКАДНЫХ КОДОВЫХ КОНСТРУКЦИЙ

Кузнецов А. А., ктн, снс, Харьковский университет Воздушных Сил им. Ивана Кожедуба,
Грабчак В. И., Военный институт ракетных войск и артиллерии СумГУ

Перспективным направлением в развитии комплексных механизмов обеспечения информационной скрытности и достоверности передачи данных являются теоретико-кодовые схемы – секретные системы теоретической стойкости, сложность взлома которых сводится к решению теоретико-сложностной задачи декодирования случайного кода. Их практическое использование позволяет реализовать в одном устройстве методы канального кодирования и специального преобразования данных. В тоже время, как показывает проведенный анализ, для реализации известных методов необходимы огромные объемы ключевых данных (0,5 – 1,5 Мбит). Кроме того, неприемлемо высоки временная и емкостная сложности алгоритмов формирования и декодирования кодограмм.

Для устранения указанных недостатков предлагается использовать каскадные кодовые конструкции. Среди каскадных кодов наиболее общим классом являются обобщенные каскадные коды, применение которых, позволяет без значительного ухудшения кодовых параметров снизить сложность их практической реализации. Кроме того, как показано в докладе, применение обобщенных каскадных кодов для построения теоретико-кодовых схем позволяет обеспечить эффективную защиту информации со сравни-

тельно небольшими объемами ключевых данных. Проведенные исследования способов маскирования обобщенного каскадного кода показали, что наиболее приемлемым по соотношению «число переборов оптимального статистического опробования/объем ключа» является маскирование кодов второй ступени и использование обобщенных каскадных кодов высокого порядка. С учетом полученных результатов разработаны каскадные схемы защиты информации, позволяющие обеспечить требуемые показатели информационной стойкости и достоверности передачи данных. Проведенные исследования стойкости разработанных схем к криптоаналитическим атакам противника показали, что наилучшей стратегией противника является применение атаки с подобранным открытым текстом и с подобранной кодограммой. Однако удачная реализация любой из рассмотренных атак не позволит противнику однозначно получить правило быстрого декодирования кода для восстановления информационного содержания передаваемых сообщений. Анализ полученных экспериментальных результатов статистической безопасности показывает, что разработанные схемы позволяют эффективно выполнять криптографическое преобразование данных – по своим показателям статистический портрет предлагаемой схемы не уступает лучшим известным криптоалгоритмам, принятым в качестве национальных стандартов ведущих государств мира.

Таким образом, в результате проведенных исследований показано, что применение разработанных каскадных теоретико-кодовых схем позволяет эффективно обеспечить передачу сообщений в пункты приема с заданной точностью и сохранять в тайне от противника смысловое содержание передаваемых сообщений и, таким образом, обеспечить требуемые показатели достоверности и информационной скрытности передачи данных в АСУВ.