ИССЛЕДОВАНИЕ СТОЙКОСТИ К ВЗЛОМУ ПРОТИВНИКОМ КАСКАДНЫХ ТЕОРЕТИКО-КОДОВЫХ СХЕМ

к.т.н., с.н.с. Кузнецов[1] А.А., ст. преп. Грабчак[2] В.И., адъюнкт Евсеев[1] С.П.

([1]Харьковский университет Воздушных Сил)

([2]Военный институт РВ и А Сумского ГУ)

Важными требованиями к перспективной АСУВ являются достоверность и информационная скрытность обрабатываемых и передаваемых данных. Эти показатели характеризуют способность системы обеспечивать точное воспроизведение передаваемых сообщений в пунктах приема и противостоять раскрытию противником содержания передаваемой информации. Обеспечить требуемые показатели достоверности и информационной скрытности возможно путем применения комплексных механизмов помехоустойчивого кодирования и специального преобразования данных. В качестве эффективного метода построения таких механизмов авторами рассматриваются теоретико-кодовые схемы – секретные системы теоретической стойкости, построение которых основано на использовании алгебраических блоковых кодов.

По определению, теоретико-кодовая схема – это секретная система, построенная с использованием трудноразрешимой задачи декодирования случайного кода. Формально она задается совокупностью следующих множеств: множество открытых текстов; множество криптограмм; множество прямых отображений; множество обратных отображений; множество ключей, параметризирующих прямые отображения; множество ключей, параметризирующих обратные отображения таких, что сложность выполнения обратного отображения без знания ключа сопряжено с решением теоретико-сложностной задачи декоди-

рования случайного кода (кода общего положения). Другими словами, алгебраический код с быстрым алгоритмом декодирования маскируется под случайный код. Не зная правила маскировки, противник вынужден использовать сложный алгоритм декодирования случайного кода. Напротив, уполномоченный пользователь, знающий правило маскировки, может воспользоваться быстрым алгоритмом декодирования алгебраического кода. Под каскадной теоретико-кодовой схемой понимается секретная система, построенная по обобщенному каскадному коду.

По определению алгебраически заданный обобщенный каскадный код порядка m однозначно определяется n_2 квадратными двоичными матрицами H_0^j, $j=\overline{1,n_2}$ порядка n_1 (задающих (n_1,k_i,d_{1i}) коды первой ступени) и $m+1$ групповыми над $GF(2^{a_i})$, $i=\overline{1,m+1}$ кодами второй ступени с параметрами (n_2,b_i,d_{2i}). Формирование каскадной кодовой схемы осуществляется путем маскирования кодового слова обобщенного каскадного кода под случайный код. Существуют следующие варианты маскирования:

1. Маскирование кодов первой ступени.
2. Маскирование кодов второй ступени.
3. Одновременное маскирование кодов первой и второй ступени.

Авторами исследуется стойкость каскадных теоретико-кодовых схем к взлому противником методом оптимального статистического опробования.

Проведенные исследования показали, что наиболее эффективным, с точки зрения соотношения длины ключа и числа переборов оптимального статистического опробования противником, является маскирование кодов второй ступени в обобщенном каскадном коде высокого порядка.