ЗАЩИТА ИНФОРМАЦИИ КОДОВЫМИ КРИПТОСИСТЕМАМИ НА ОСНОВЕ ТЕОРИИ НОРМ СИНДРОМОВ И СВОЙСТВ ЦИКЛОТОМИЧЕСКОЙ ПЕРЕСТАНОВКИ ЧИСЕЛ

В.К. Конопелько, О.Г. Смолякова

Современные методы защиты информации включают в себя применение кодовых криптосистем с отрытым ключом, использующих порождающую матрицу кода в качестве отрытого ключа. Устойчивость ко взлому таких кодовых криптосистем определяется сложностью синдромного декодирования, то есть так называемой проблемой селектора. С увеличением длины кода и его расстояния сложность декодирования такой криптосистемы возрастает экспоненциально и уменьшить ее для санкционированного пользователя можно применяя при генерации пары "открытый-закрытый ключ" нормы синдромов векторов ошибок кода и их размещение при использовании циклотомической перестановки.

В докладе предлагается вариант кодовой криптосистемы, использующей в качестве открытого ключа специальным образом сконструированную порождающую матрицу кода, а в качестве закрытого — знание норменного циклокласса к которому могут принадлежать нормы синдромов разрешенных векторов ошибок. При кодировании с помощью порождающей матрицы кодовые слова имеют "искусственный дефект", то есть внесенные предумышленно ошибки. Норма синдрома такого кодового слова указывает на норменный циклотомический класс, с помощью которого происходит восстановление информации.

Полученные результаты позволяют конструировать кодовые криптосистемы, в основе которых лежат коды большой длины, увеличивая этим проблему селектора; знание закрытого ключа — норменного циклокласса — позволяет избежать этой проблемы санкционированному пользователю.