О ПРИМЕНЕНИИ МОДЕЛИ ПАРАЛЛЕЛЬНОГО ВЫЧИСЛЕНИЯ ПРИ ШИФРОВАНИИ ИНФОРМАЦИИ

Ширинова А.О.
Азербайджанский государственный университет нефти и промышленности,
г. Баку

С развитием информационных технологий все больше растет потребность в средствах криптографической защиты информации. Одним из основных видов криптографического преобразования информации является шифрование [1, 2].

В настоящее время в современных информационных системах применяются технологии, которые требуют передачи больших объемов данных. Очевидно, что шифрование таких объемов информации классическими методами требует значительных временных затрат.

В связи с этим в данной работе с целью ускорения вычислительного процесса шифрования и дешифрования предлагается использовать модель параллельных вычислений. С этой целью выбирается модель параллельных вычислений, ориентированную на многопроцессорные вычислительные системі с общей памятью SMP [3, 4]. Разработана компьютерная программа в среде программирования Microsoft Visual C++ с использованием технологии параллельного программирования Open MP. Данная программа опробована для шифрования достаточно большого объема информации на азербайджанском языке путем применения подстановочных методов симметричного шифрования. При этом число возможных ключей равно числу возможных перестановок из 32 букв азербайджанского языка, то есть, 32!. Очевидно, что такой моноалфавитный шифр является стойким к взлому методом перебора возможных ключей. Однако проведенные численные эксперименть показал, что шифрование таким образом поддается криптоанализу, который начинается с подсчета каждого символа шифртекста и определения частоты его встречаемости. В связи с этим для обеспечения криптостойкости подстановочных методов шифрования, они были скомбинированы шифром, предложенным Гронсфельдом [1, 2].

Анализ результатов численных экспериментов свидетельствует, что использование модели параллельных вычислений в предложенном алгоритме криптографических преобразований позволяет значительно снизить временные затраты.

Литература:

1. *Мао Венбо.* Современная криптография: теория и практика. – М.: Вильямс, 2005. – 768 с. **2.** *Шнайер Брюс.* Прикладная криптография. М.: Триумф, 2002. – 816 с. **3.** Ceze L.H. Shared-Memory Multiprocessors // Encyclopedia of Parallel Computing. Boston, MA: Springer US, 2011. – P. 1810–1812. **4.** *Федотов И.Е.* Модели параллельного программирования. – М.: Солон-Пр., 2017. – 392 с.