КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ДАННЫХ НА ОСНОВЕ АЛГОРИТМОВ СЖАТИЯ

С.С. Куликов, С.А. Иванов, К.Н. Куховец

Алгоритм сжатия данных, предложенный Д. Хаффманом, требует построения двоичного дерева, с помощью которого возможно восстановление сжатых данных в исходное состояние.

Хранение структуры двоичного дерева отдельно от сжатых данных позволяет использовать алгоритм сжатия Хаффмана для криптографической защиты информации. Таким же образом можно использовать и другие алгоритмы сжатия, требующие наличия определённой структуры данных для сжатия и восстановления информации.

Преимущество предлагаемого подхода заключается в том, что операция сжатия данных совмещается с операцией шифрования, что позволяет не только защитить данные, но и уменьшить размер криптотекста. Использование для дешифрования файла, хранящего структуру двоичного дерева, позволяет исключить случаи использования некриптостойких паролей, которые могут быть легко подобраны или узнаны методами социальной инженерии.

Модификация предлагаемого подхода, основанная на дополнительном шифровании (с использованием введённого пользователем пароля) файла, хранящего структуру двоичного дерева, позволяет повысить защищённость данных: злоумышленнику недостаточно перехватить криптотекст и файл с двоичным деревом, ему также необходимо для успешной дешифровки перехватить или подобрать введённый пользователем пароль.

Предлагаемый подход имеет практическое применение при передаче данных по слабозащищённым каналам передачи данных. Так криптотекст может быть передан по высокоскоростному незащищённому каналу передачи данных, файл с двоичным деревом — по низкоскоростному защищённому каналу передачи данных, а введённый пользователем пароль — по третьему, физически отличному от предыдущих двух, каналов передачи данных (например, в виде короткого сообщения по мобильной телефонной связи).