

ТЕКСТОВЫЙ ПРОЦЕССОР С ФУНКЦИЕЙ ПЕРЕДАЧИ ЗАЩИЩЕННОГО СООБЩЕНИЯ

*канд. экон. наук, доцент М.И. Главчев, магистр Е.В. Ткаченко,
Национальный технический университет "Харьковский
политехнический институт", г. Харьков.*

Текстовый процессор – компьютерная программа, приложение, текстовый редактор с расширенными возможностями.

Шифрование применяется для хранения важной информации в ненадёжных источниках и передачи её по незащищенным каналам связи. Главным образом, шифрование служит задачей соблюдения конфиденциальности передаваемой информации. Важной особенностью любого алгоритма шифрования является использование ключа, который утверждает выбор конкретного преобразования из совокупности возможных для данного алгоритма.

Шифром называется пара алгоритмов, реализующих каждое из указанных преобразований. Эти алгоритмы применяются над данными с использованием ключа. Ключи для шифрования и для расшифровывания могут отличаться, а могут быть одинаковыми. При шифровании очень важно правильно содержать и распространять ключи между собеседниками, так как это является наиболее уязвимым местом любой криптосистемы. Процесс, содержанием которого является составление и распределение ключей между пользователями, играет важнейшую роль в криптографии как основа для обеспечения конфиденциальности обмена информацией.

Для того чтобы прочесть зашифрованную информацию, принимающей стороне необходимы ключ и дешифратор (устройство реализующее алгоритм расшифровывания). Идея шифрования состоит в том, что злоумышленник, перехватив зашифрованные данные и не имея к ним ключа, не может ни прочесть, ни изменить передаваемую информацию. Кроме того, в современных криптосистемах (с открытым ключом) для шифрования, расшифровывания данных могут использоваться разные ключи.