ГУБКА С.А. к.т.н., доц.,
ГУБКА А.С., к.т.н., доц.,
НОСОВА Н.Ю., асп.
Национальный аэрокосмический университет
им. Н.Е. Жуковского «ХАИ»,
г. Харьков

РАЗРАБОТКА МЕТОДА РАЗДЕЛЕНИЯ КЛЮЧЕЙ ШИФРОВАНИЯ

Предложен метод шифрования, позволяющий повысить криптостойкость передаваемых по открытым каналам связи конфиденциальных данных.

Актуальность. В современном мире наблюдается стремительное внедрение компьютерных систем (КС) во все сферы человеческой деятельности. В связи с этим остро встает задача защиты информации, передаваемой в рамках КС и открытых каналов связи. Наиболее эффективным средством защиты информации, по мнению большинства специалистов, является криптографические методы защиты информации с закрытым ключом.

Цель исследования. Повышение защищенности конфиденциальной информации (в том числе персональных данных) пользователей.

Основная часть. Современные алгоритмы шифрования с закрытым ключом предполагают использование общего ключа шифрования в разных элементах криптографического алгоритма. Однако использование одного и того же ключа в разных частях алгоритма может снизить криптографическую стойкость самого алгоритма.

На основании вышеизложенного предложен метод, который позволяет разделить псевдослучайным образом исходный ключ шифрования на несколько подключей.

Выводы. Таким образом, данный метод можно использовать для защиты любых конфиденциальных данных, в том числе и в различных социальных сетях. Предложенный метод разделения ключей реализован в модернизированном симметричном алгоритме шифрования по ДСТУ ГОСТ 28147:2009. Сам модернизированный симметричный алгоритм реализован в виде программной системы, написанной на платформе Microsoft.NET, с использованием технологий ADO.NET, ASP.NET и Framework 4.5. Благодаря этому она обладает улучшенной производительностью по сравнению с другими используемыми технологиями. Кроме того, в системе существует возможность подключения дополнительных аппаратных средств, которые существенно ускоряют операции шифрования/расшифровывания.

Библиографический список

1. Панасенко С.П. Алгоритм шифрования ГОСТ 28147-89 [Электронный ресурс] / С.П. Панасенко. – Режим доступа: http://www.inssl.com/standart-of-cipher.html**.**