

ПОРІВНЯННЯ СУЧАСНИХ АЛГОРИТМІВ ШИФРУВАННЯ

Пчелінцев І.С.

Науковий керівник: **Григоренко О.Г.**

Інститут телекомунікаційних систем, КПІ ім. Ігоря Сікорського, Україна

E-mail: illia.pchelintsev@gmail.com

В роботі розглянуто алгоритми шифрування, що використовуються для забезпечення захисту даних в сучасних інфокомунікаційних мережах. Зроблено порівняльна оцінка таких алгоритмів шифрування, як Blowfish, DES, 3DES, CAST, AES, RSA, El-Gamal.

COMPARISON OF MODERN ENCRYPTING ALGORITHMS

Pchelintsev I.S.

Scientific adviser: **Grygorenko O.G.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: illia.pchelintsev@gmail.com

Encryption algorithms used to provide data protection in modern infocommunication networks are considered. A comparative assessment is made of such encryption algorithms as Blowfish, DES, 3DES, CAST, AES, RSA, El-Gamal.