

УДК 681.3.06

**Метод конструювання циклових функцій БСШ / С.А. Головашич // АСУ та прилади автоматики. 2001. № 00, С. 000–000.**

У статті пропонується метод конструювання циклового нелінійного перетворення (f-функції) ітеративних алгоритмів блокового симетричного шифрування побудованих, на базі фіксованих нелінійних перетворень (S-блоків). Запропонований метод забезпечує, незалежно від використовуваного циклового ключа, фіксовані показники “розсіювання” та “розмноження” активізації окремих S-блоків. Наводиться декілька простих у реалізації схем бітової перестановки та лінійного комбінування.

Табл. 0. Ил. 3, Бібліогр.: 4 назв.

UDC 681.3.06

**One method of design round function for block ciphers / S.A. Golovashich // Management Information System and Devices. All-Ukr. Sci. Interdep. Mag. 2001. № 00, P. 000–000.**

Tab. 0. Fig. 3, Ref.: 4 items.

A design method of round functions of iterated block ciphers is proposed. The round function is non-linear transformations based on S-boxes. The suggested method provides permanent diffusion and propagation indexes independent of the used round key. Several simple and easy to implement schemes of bit permutation and linear transformation are proposed.