

УДК 681.3.06

**Безопасность режимов блочного шифрования** / С.А. Головашич // Радиотехника: Всеукр. межвед. науч.-техн. сб. 2001. Вып. 119. С. 00 — 00.

В статье дан анализ основных режимов применения блочных симметричных шифров. Проанализированы достоинства и недостатки каждого из режимов, предложены способы устранения обнаруженных недостатков. Приведены две схемы режимов поточного шифрования удовлетворяющие, предложенным требованиям.

Ил. 2. Библиогр. 8 назв.

УДК 681.3.06

**Безпека режимів блокового шифрування** / С.О. Головашич // Радіотехніка: Всеукр. міжвід. наук.-техн. зб. 2001. Вип. 119. С. 00 — 00.

У статті дано аналіз основних режимів застосування блокових симетричних шифрів. Проаналізовано переваги та недоліки кожного з режимів, запропоновані засоби усунення виявлених недоліків. Наведено дві схеми режимів потокового шифрування, які задовольняють запропонованим вимогам.

Іл. 2. Бібліогр. 8 назв.

UDC 681.3.06

**Block ciphers modes of operations security** / S.A. Golovashich // Radiotekhnika. All-Urk. Sci. Interdep. Mag. 2001. N 119. P. 00 — 00.

The symmetric block ciphers standard modes of operations analysis is carried out. The advantages and disadvantages of each mode is analyzed, the improvement methods are suggested. The schemes of two new modes for stream encryption are proposed. These schemes completely satisfy suggested requirements.

2 fig. Ref.: 8 items.