

mgr inż. Łukasz Dziel
Wojskowa Akademia Techniczna
Wydział Cybernetyki
Instytut Matematyki i Kryptologii

Analiza możliwości implementacji algorytmu NLSv2 w strukturach programowalnych

Podstawowe informacje o NLSv2 — elementy budowy i zasady działania.

Podstawowe informacje o strukturach programowalnych, które były brane pod uwagę podczas analizy.

Dobór kryteriów projektowych — możliwe sposoby realizacji algorytmu w strukturze.

Propozycja realizacji algorytmu w strukturze dla zadanych kryteriów projektowych — opis zasady działania i elementy budowy.

Wyniki porównawcze efektywności zrealizowanej implementacji sprzętowej w porównaniu do implementacji programowych i realizacji sprzętowych innych szyfrów strumieniowych.