

Kody korekcyjne w kryptografii

dr Iwona Krzyżanowska i dr Aleksandra Nowel

W okresie dynamicznego rozwoju techniki komputerowej i systemów teleinformatycznych duże znaczenie mają metody ochrony informacji. Zagadnienia te są rozpatrywane w teorii kodowania i kryptografii.

Teoria kodów korekcyjnych opiera się na algebrze ciał skończonych. Kody korekcyjne umożliwiają zwiększenie niezawodności informatycznego systemu cyfrowego, lecz ich zastosowanie powoduje wzrost objętości danych, co wiąże się z koniecznością zwiększenia przepustowości kanałów transmisyjnych i wielkości pamięci.

Seminarium ma na celu przedstawienie podstaw matematycznych teorii kodowania i kryptografii i ich zastosowania w zagadnieniach ochrony informacji przed błędami i nielegalnym dostępem w nowoczesnych systemach komputerowych i teleinformatycznych.

Literatura

1. Mochnacki, W. *Kody korekcyjne i kryptografia* Oficyna Wydawnicza Politechniki Wrocławskiej, 2000
2. Moon T.K. *Error Correction Coding. Mathematical Methods and Algorithms*, Wiley-Interscience 2005
3. Biernat, J. *Kodowanie i szyfrowanie* Akademicka Oficyna Wydawnicza EXIT, Warszawa 2017