Algebraic-probabilistic methods of investigation of cryptographic algorithms and protocols resistans and effectiveness.

State registration: **0108U001549.**
Head prof Savchuk M.M.

Results

The purpose of work consists in development and improvement probabilistic for algebra methods of research of cryptographic transformations, analysis of symmetric and asymmetric algorithms of enciphering, methods of avtentifikacii, cryptographic protocols, taking into account the last achievements of kriptologii and application of results for the estimation of firmness and efficiency of modern kriptosistem and cryptographic protocols, improvement of methods of cryptographic priv.

The effective algorithms of decision of the linear systems of equalizations are developed above the complete fields with distortions; algorithms of rozv"yazannya of cilochislovikh equalizations of the special kind. Innovative methods and programs of attacks of algebra are improved and developed on potokovi codes. Got estimations of descriptions of boole functions, vazhkooborotnikh functions. The methods of kriptoanalizu are developed, that optimum the methods of algebra and facilities of surplus use cross-correlation dependences.