ABSTRACT

Bachelor paper consists of five sections, contains 64 pages, 13 figures, 6 tables, 3 appendices, 18 sources.

The purpose of the Bachelor project is the development of the system based on a threshold cryptosystem for user data protection.

In the Bachelor project considered were such algorithms as RSA public key encryption, Shamir's secret sharing, AES + CBC-MAC (CCB) symmetric encryption, Schnorr signature.

In the information provisioning section defined were input and output data for the spectra of tasks considered.

The expedience of the chosen cryptographic algorithms and methods is corroborated in the mathematical provisioning section.

In the software section the major development tools used for project tasks are described, technical requirements are specified, software architecture is defined and elaborated.

In the technology section the user manual is provided; test reports are also provided for each project task.

CRYPTOSYSTEM, RSA, AES-CBC, GROUP KEY, VERIFICATION KEY, SHAMIR'S SECRET SHARING, SCHNORR SIGNATURE, PEER-TO-PEER NETWORK.