4.1. Name: **Symmetric cryptography** (system analysis)

4.2. Abstract of educational discipline: educational discipline acquaints with classic ciphers, theory of Shennon, cryptographic properties of boole functions, modern block ciphering and stream ciphering systems of enciphering by principles of their construction and methods of application.

4.3. Type: discipline of the free choice of the student (in blocks).

4.4. Term of study: 7th semester.

4.5. Amount of credits: 2 credits.

4.6. Name of lecturer: full professor Savchuk Mykhajlo Mykola.

4.7. Aim of educational discipline: to give knowledge in an area of theoretical cryptography and bases of cryptoanalysis of symmetric cryptosystem. Discipline acquaints works of the symmetric cryptographic systems with basic principles, by the mathematical models of information generators, by the concepts of theoretical and practical secrecy, perfect secrecy cryptosystems. The concrete types of algorithms of the symmetric enciphering and cryptographic transformations are examined in accordance with their classification on classic ciphers, mechanical and electromechanics encipherings machines, modern block ciphering and stream ciphering systems of enciphering.

4.8. Previous requirements: provided by courses: discrete mathematics, algebra and geometry, theory of probability and mathematical statistics, information and code, programming theory and algorithmic languages, random processes.

4.9. Teaching methods: employments are conducted in form lectures.

5.0. Evaluation methods: estimated after the module-rating system. The results of educational activity of students are estimated on a 100-ball scale and end with a test.

5.1. Teaching language: Ukrainian.