4.1. Name: **Asymmetric cryptography and public-key cryptosystems** (system analysis).

4.2. Abstract of educational discipline: educational discipline acquaints with theoretical bases cryptographies with public-key, asymmetric systems of enciphering, systems of digital signature, authentication, by various cryptographic protocols, their application in the protective information systems of in various spheres, where information technologies are used and also with new perspective directions of development of methods of cryptographic protection.

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

4.4. Term of study: 8th 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 to the students of knowledge in an area of public-key cryptography. Discipline indoctrinates with the theory complication of functions and algorithms, with one-way functions and their application for the construction of asymmetric cryptosystems, with various cryptographic protocols, in particular with protocols of authentication, digital signature and others like that. In a course the examples of application of cryptographic protocols are examined in electronic commerce. Considerable attention is spared to cryptosystems on elliptic curves.

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

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.