10.04.01 Information Security "Theoretical and practical cryptography"

In the modern world, work in the field of information security requires versatile training, which is unattainable without mastering fundamental theoretical and practical disciplines. This feature is reflected in the name of the program. At first students are given the necessary knowledge base including mathematical disciplines, programming methods and the basics of information security. Without them it is impossible to develop and analyze modern information security systems including cryptographic ones. Original courses use the developments of domestic and foreign scientists in recent years and are taught on synthesis and analysis including methods for identifying vulnerabilities and protecting against cyberattacks.

Unique disciplines:

- Fundamentals of cryptanalysis
- Modern models of cyberattacks
- Additional sections of low-level programming
- Algebraic Foundations of Cryptography
- Applied Information Security
- Elliptic curves in cryptography
- Practical application of cryptographic protocols
- Cryptography standards
- Methods for constructing destructive influences
- Modern cryptosystems
- Targeted attacks on computer systems
- Secure Information Systems
- Methods of discrete mathematics in cryptography
- Multiparadigm programming
- Introduction to Dynamic Software Analysis Techniques

Professional opportunities:

- FSTEC of Russia
- CryptoPro
- Kaspersky
- Informzaschita
- Infotecs