INFORMATION THEORY AND CRYPTOGRAPHY

Lecturer: Idrisova Valeriya Aleksandrovna

Semester: 1 **Duration**: 6 weeks

Workload (h): 180 **Presence** (h): 74 **Self-Study** (h): 106

Contents: The course contains topics about basic notions and concepts in the information theory, data compression, coding theory and cryptography.

Background and relations to other courses: algebra, discrete mathematics and combinatorics, number theory, probability theory.

Main topics and learning objectives:

Themes	**Learning objectives**
Introduction to the information theory, signal theory, sampling, notion of entropy.	*To know and understand* the notion of information and approaches to measuring the amount of information.
Transmission through the noisy channel. Error-correcting codes. LDCP-codes.	*To know and understand* widespread methods of error-correction. *To apply* these methods in practice.
Data compression theory.	*To know and understand* basic techniques of data compression and classic algorithms such as Huffman coding, arithmetic coding, LZ77, LZ78 etc. *To apply* these methods in practice.
Modern methods of cryptography and cryptanalysis. Perfect secrecy. Block ciphers and stream ciphers. Boolean functions. Public-key cryptography. Cryptanalysis of symmetric and public-key systems.	*To know and understand* classic and modern ciphers and cryptosystems such as DES, AES, GOST, A5/1, Grain, RSA, ElGamal etc. *To know* basic methods of cryptanalysis meet-in-the-middle attack, birthday paradox attack, linear, differential and algebraic techniques of statistical cryptanalysis. *To apply and implement* these methods in practice.

Assessment:

Formative: in interaction with lecturer and tutor during learning period.

Summative:

Number and Type; Connection to Course	**Duration**	**Part of final mark in %**
Final interview	2 hours	50%
Course Assignments		50%

Learning outcomes:

Academic: to be able to develop software that includes algorithms and notions mentioned above.

Prerequisites for Credit Points: The credit points will be granted when the course has been successfully completed, i.e. all parts of the examination are passed.