Government of Russian Federation

Federal State Autonomous Educational Institution of High Professional Education

“National Research University Higher School of Economics”

Syllabus for the course “Theoretical computer science”

for postgraduate program in 09.06.01 Computer Science and Computer Engineering / 05.13.01 “Systems Analysis, Control Theory, and Information Processing”, 05.13.11 “Mathematical Theory and Software for Computing Machinery, Systems, and Networks”, 05.13.17 “Theoretical Foundations of Computer Science”, 05.13.18 “Mathematical Modeling, Numerical Methods, and Software Systems”

Authors:
Bruno Bauwens, assistant professor, brbauwens@gmail.com

Moscow – 2018

1. Scope of Use

This program establishes the minimal requirements to postgraduate students' knowledge and skills for 09.06.01 Computer Science and Computer Engineering / 05.13.01 "Systems Analysis, Control Theory, and Information Processing", 05.13.11 "Mathematical Theory and Software for Computing Machinery, Systems, and Networks", 05.13.17 "Theoretical Foundations of Computer Science", "05.13.18 Mathematical Modeling, Numerical Methods, and Software Systems" and determines the content of the course and educational techniques used in teaching the course.

The present syllabus is aimed at faculty teaching the course and postgraduate students studying 09.06.01 Computer Science and Computer Engineering / 05.13.01 "Systems Analysis, Control Theory, and Information Processing", 05.13.11 "Mathematical Theory and Software for Computing Machinery, Systems, and Networks", 05.13.17 "Theoretical Foundations of Computer Science", 05.13.18 "Mathematical Modeling, Numerical Methods, and Software Systems".

This syllabus meets the standards required by:

- Educational standards of National Research University Higher School of Economics;
- Postgraduate educational program for 09.06.01 Computer Science and Computer Engineering.
- University curriculum of the postgraduate program for 09.06.01 Computer Science and Computer Engineering / 05.13.01 "Systems Analysis, Control Theory, and Information Processing", 05.13.11 "Mathematical Theory and Software for Computing Machinery, Systems, and Networks", 05.13.17 "Theoretical Foundations of Computer Science", 05.13.18 Mathematical Modeling, Numerical Methods, and Software Systems", approved in 2014.

2. Learning Objectives

The learning objective of the course "Theoretical Computer Science" is to provide PhD students with theoretical background for their research in computer science. Also, they need to train writing and presentation skills in English

- Automata and languages
- Computability theory
- Computational complexity
- Cryptography

3. Main Competencies Developed after Completing the Study of This Discipline

Skills for research are developed, the students will learn to:
- solve mathematically challenging problems
- carefully write and present theoretical results
- read, write and present theoretical papers

After completing the study of the discipline the PhD student should have developed the following competencies:

Competence	Code	Descriptors (indicators of achievement of the result)	Educative forms and methods aimed at generation and development of the competence
The ability to carry out research in the field of professional activity using current research methods and information and communication technologies.	ОПК-1	Students obtain necessary knowledge to understand and formulate the theoretical difficulty of problems they are solving. Moreover, both for exercise lessons, the project and during the exam the students will be stimulated to search and share online information.	The student is allowed to use any information he find on the web for his project and during the exam.
The ability to carry out theoretical analysis and design of programming languages and systems, to use methods for analysing program semantics.	ОПК-2	Expressive power of several theoretical computing devices (Automata, Turing machines) and even a few programming languages will be investigated (topics 1, 2, and 3).	Examples covered during the lectures and exercises sessions.
The ability to develop and use methods for improving the efficiency and reliability of data and knowledge processing and transmission in computing machinery, systems, and networks.	ОПК-3	A separate part (topic 4) is devoted to the mathematical foundations of cryptography.	Lectures and exercise sessions
The ability to do research in transformation of information into data and knowledge, models of data and knowledge representation, methods for knowledge processing, machine learning and knowledge discovery methods, principles of building and operating software for automation of these processes.	ОПК-4	A separate part (topic 5) is devoted to learning theory. In this part we study the process of extracting models from data.	Lectures and exercise sessions

4. Place of the Discipline in the Postgraduate Program Structure

This is an elective course for 05.13.01 “Systems Analysis, Control Theory, and Information Processing”, 05.13.11 “Mathematical Theory and Software for Computing Machinery, Systems, and Networks”, 05.13.17 “Theoretical Foundations of Computer Science”, 05.13.18 “Mathematical Modeling, Numerical Methods, and Software Systems”.

The following knowledge and competences are needed to study the discipline:

- Basic English language, both oral and written.
- Basics of linear algebra, discrete mathematics and probability theory.

5. Schedule

№	Topic	Total hours	Contact hours			Self-study
			Lectures	Seminars	Practice lessons	
1.	Automata and languages	16	2		2	12
2.	Computability theory	64	8		8	48
3.	Computational complexity	64	8		8	48
4.	Quantum computation	16	2		2	12
5.	Topics of interest to the students	30	4		4	22
	Total	190	24		24	142

6. Requirements and Grading

Project	1	A project which involves reading a choosen paper, carefully write out technical details, and present the result in the classroom.
Exam	2	Intermediate exam and a final exam.

7. Assessment

The assessment consists of a project with a paper writing assignment and oral presentation.

Final assessment is the final exam. Students have to demonstrate knowledge of the material covered during the entire course and the ability to apply the materials.

8. The grade formula

Final course mark *is obtained from the following formula*: Final mark = 0.4 (Project) + 0.3 (Intermediate exam) + 0.3*(Final exam).

All grades having a fractional part greater than 0.5 are rounded up.

Table of Grade Accordance

Ten-point Grading Scale	**Five-point Grading Scale**	
1 - very bad	Unsatisfactory - 2	**FAIL**

2 – bad 3 – no pass		
4 – pass 5 – highly pass	Satisfactory – 3	**PASS**
6 – good 7 – very good	Good – 4	
8 – almost excellent 9 – excellent 10 – perfect	Excellent – 5	

9. Course description.

Topic 1. Automata and regular languages

Discrete finite automata: deterministic, non-deterministic, equivalence and pumping lemma.
Regular expressions and equivalence with finite automata.

We follow Sipser's book chapter 1.

Topic 2. Computability theory

- Turing machines: expressive power, equivalence with register machines, tag-systems.
- Halting problem, undecidability of tilings and a few other problems.
- Proof systems: decidability of arithmetic with addition, undecidability of number theory, and Godel incompleteness.
- Kolmogorov complexity: definitions, Shannon-Fano code, additivity

Notes will be given.

Topic 3. Computational complexity

- Classes P and NP, dynamic programming, the Levin-Cook theorem, NP-completeness of Hamiltonian path, vertex cover, etc.
- Classes L, PSPACE, NPSPACE, EXPSPACE, Savitch theorem, completeness of: formula game, generalized geography, testing equivalence of regular expressions.
- Oracle computation and oracles A and B for which P^A = NP^A and P^B != NP^B.
- The class RP, BPP and prime testing.

We follow Sipser's book chapters 7-10.

Topic 4. Quantum computation

Introduction and Shor's algorithm for factorization (We follow the last chapter of Papadimitriou's book).

Topic 5. Topics suggested by the students

For example, cryptography, blockchain, combinatorial optimization,

10. Educational technologies

The following educational technologies are used in the study process:

- notes provided by the lecturer
- weekly consultation time
- student can hand in exercises to be corrected by the lecturer.

11. Final exam questions

The final exam will consist of a selection of problems. Students are allowed to bring use textbooks, notes and they will have a laptop available with pdf-files of some books. They may not access the internet or communicate in any other way. Each question will require to solve mathematical problems using materials presented during the lectures and some of the project presentations.

12. Reading and Materials

Literature:

1. M. Sipser. *Introduction to the Theory of Computation*. Cengage Learning, 2012.
2. S. Arora and B. Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, 2009.
3. J. Katz, & Y. Lindell. *Introduction to modern cryptography*. CRC Press, 2014.
4. S. Dasgupta, C. H. Papadimitriou, and U. V. Vazirani. *Algorithms.* Mc Graw Hill, 2006.

13. Equipment.

Blackboard. Computer room for the exam.