ITMO University

Information Security Risk Management

Course Workload		Assessment form (examination/ graded test/ ungraded test)
ECTS	Hours	
6	216	Exam

In the course of studying the discipline, the student: Learns information security risks, sources of information security risks, goals and objectives of information security risk management, conditions for the implementation of risks and measures to counter them. Learn to identify within the framework of the chosen solution issues (tasks) to be further developed and justify its choice. Learn how to upgrade the software and hardware of artificial intelligence technologies and systems to solve professional problems, taking into account the requirements of information security in various subject areas.

Course structure:

1. Conceptual foundations of IT-Security risk management

1.1. Concepts of IT-Security risk. Sources of IT-Security risks.
1.2. Goals and objectives of IT-Security risk management.
1.3. The place of the IT-Security risk management task in the Deming cycle.
1.4. Formal statement of the task of IT-Security risk management.
1.5. The life cycle of the information system and the tasks of the URIB at its stages.
1.6. IT-Security risk management as a complex task.
1.7. Factors influencing the determination of the value of assets and damages from the implementation of risks.
1.8. Modeling of risk management components of an integrated information security system using formal techniques.
1.9. Conditions for the implementation of risks and measures to counteract them.
1.10. Setting a task for the development in the discipline.
1.11. Coordination of tasks and approval of plans for the implementation.

2. IT-Security risk assessment methodologies

2.1. GOST requirements for documentation (GOST 7.32, 15.101, GOST ESKD, ESPD ...).
2.2. Guidance, regulatory and reference documents in the field of information security management (IT-Security risk assessment).

2.3. Mastering of information resources on the subject of the discipline in relation to the topic of WRC, methods and means of accounting for IT-Security risks in the process of designing means and systems of informatization in protected execution; independent information search in arrays of open documentation; work with guidance documents and standards; mastering professional terminology
2.4. The concept and classification of IT-Security risk assessment methodologies, their comparative characteristics.
2.5. Criteria for choosing an IT-Security risk assessment methodology.
2.6. Guidance documents in the field of IT-Security risk assessment.
2.7. IT-Security risk assessment procedure Current regulations and best practices in the field of IT-Security risk assessment.
2.8. Methods of expert evaluation of hard-to-formalize factors: problems, ways to resolve them, best practices.
2.9. Modeling of components of an integrated information security system using formal techniques (in relation to the topic of the WRC).

3. Introduction to the mathematical foundations of IT-security risk management

3.1. Formulation of the mathematical problem of optimal control.
3.2. Classification of optimal control problems.
3.3. Mathematical programming.
3.4. Graphical interpretation of a linear programming problem.
3.5. The use of standard mathematical models to solve the problem of risk management in information security.
3.6. Reduction of practical risk management tasks to standard mathematical programming tasks.
3.7. Selection and justification of the mathematical apparatus for the implementation of the stages of the complex task of information security risk management.
3.8. Presentation of the draft decision.

4. IT-Security risk management

4.1. Implementation of a comprehensive project to solve the problems of IT-Security risk management at the stages of the Information Systems life cycle.
4.2. Criteria for the selection of IT-Security risk management tools.
4.3. Investigation of the capabilities of IT-Security risk management tools.
4.4. Comparative analysis of IT-Security risk management tools.
4.5. The content of the Technical specification for the development of a component of an IT-Security risk management tool.
4.6. Development of technical specifications for the development of a component of an IT-Security risk management tool.
4.7. Use (component) of the IT-Security risk management tool.