ITMO

MOBILE SYSTEMS SECURITY

Course Workload		Assessment form (examination/ graded test/ ungraded test)
ECTS	Hours	
3	108	Exam test

The course targets on basics of the modern mobile device platforms, analysis and testing of mobile applications, cryptographic protection methods in mobile devices and wireless communication systems, software and hardware protection of data storage systems in mobile devices. The course main aims are: introducing and reviewing cryptographic methods for protecting mobile devices and wireless protocols. learning the main categories of threats for mobile devices, threat models for modern mobile operating systems; studying access control models for mobile operating systems; choosing software and hardware tools for mobile device analysis; developing design solutions for the use of software and hardware (including cryptographic) means of protecting mobile devices.

Course structure:

1. MOBILE DEVICE PLATFORMS

    1.1. The main types of mobile device vulnerabilities. Architectural differences and similarities between Android and Apple iOS platforms. Overview of mobile platform features: iBeacon, AirDrop, App Verification, Google Wear. Android and iOS access control models. Application isolation.

2. ANALYSIS AND TESTING OF MOBILE APPLICATIONS

    2.1. Jailbreak mobile devices. Identification, authentication of users of mobile devices.

3. CRYPTOGRAPHIC PROTECTION METHODS IN MOBILE DEVICES AND WIRELESS COMMUNICATION SYSTEMS

    3.1. Basic mechanisms and software and hardware protection in mobile devices.

4. SOFTWARE AND HARDWARE PROTECTION OF DATA STORAGE SYSTEMS IN MOBILE DEVICES.

    4.1. Means for monitoring network activity of wireless communication systems. Reverse engineering of mobile applications. Software and hardware for security analysis of mobile applications. Techniques for obfuscation of the source code of mobile applications.