**Secure software development**

Contact person: Dr. Lívia Szedmina (slivia@vts.su.ac.rs)

Course objective:

The aim of the course is to teach students the life cycle of secure software development, covering the following main phases of the software life cycle: requirements, design, testing, development, and implementation. The main goal of the course presupposes the realization of several sub-goals: - introduction to the use of development techniques; -acquaintance with methods for exploiting software errors; -knowledge of ways to eliminate certain errors; -knowledge of basic concepts and techniques of cryptography.

Course outcome:

Students who take and successfully pass the exam will be able to: - understand the issues related to security aspects of software development; - identification of possible sources of software security threats - avoidance of typical programming errors in software development - application of methods and techniques for detection, prevention and neutralization of security breaches - development of reliable and secure applications using modern technological protection tools.

Theoretical classes:

Basic terms. Categories of possible attacks. The most common mistakes of developers. Principles of problem prevention. Application development path. Static and dynamic code analysis. Code analysis tools. Basic levels of cyber-attack. Cryptography techniques. Symmetric cryptography. Asymmetric cryptography. Applied cryptography. Cryptographic algorithms. Security protocols. Access control and network barriers. Intrusion detection and prevention systems. Data protection tools. Classic examples of software implementation problems. Typical security errors in the use of scripting languages. Exploiting bugs in programming languages. Attacks targeting system design and protocol design errors.

Practical teaching:

Tasks and problems in practical teaching follow the content of theoretical teaching. Exercise through examples and tasks. Encryption block. Symmetric cryptography (DES, DES-CBC, IDEA, RC5, RC6, AES algorithms, Blowfish). Asymmetric and hybrid cryptosystems. Digital signature (MD5, SHA-1). Entity authentication; key exchange algorithms; key management. Security services in the TCP / IP model. Implementation of security and safety techniques in web application development. Security aspects of application development in C / C ++ language.