State Final Examinations	Academic Year: 2018/2019
Master's Degree Studies Program:	Engineering Informatics
Study Branch:	Security Technologies, Systems and Management
Study Focus:	Technical, Management

Information Systems Protection

Compulsory Optional Subject

1. Systems Requirements - Integrated alarm systems, integrated alarm systems characteristics, application, configuration types, alarm and non-alarm applications.
2. Alarm and Non-alarm Applications and Integration Software - Functions, general schema, basic binding schematics, software product classification and description, classification and rights of SW user integration.
3. Systems Integration - Importance, system integration principles, possibilities, forms of system integration, the role of system integrators.
4. Integrated Non-production Automation Systems - Non-production automation areas, the meaning and principles of integration, the characteristics of system approach to integration.
5. Information Security Management Systems – The analysis and management of information security risks, Laws, standards and regulations related to the security of information systems and cyber security.
6. Hash Functions - MD and SHA function properties, the use of hash functions in industry and public administration, the possibilities of using hash algorithms in SMART technologies.
7. Identity and Access Management (IAM) - Access control, directory systems, provisioning, IAM solutions architecture, advanced identity management technologies, managing identities and approaches on the Internet, the future of digital identities.
8. Wireless Net Security - MAC address filtering, SSID hiding, WEP, WPA and WPA2 encryption.
9. Security Concept AAA, (Authentication, Authorisation, Accounting) - Principles and applications, protocols (TACACS, RADIUS) - principles, use, comparison, advantages, and disadvantages.
10. IS Intrusion Prevention Technology - Firewalls, IDS, IPS, operation principles, network integration, comparisons – advantages/disadvantages.
11. The VPN Concept - Principle, purpose, using tunnelling for VPN transmission, GRE, IPSec, SSL, protocols, usage principles, comparisons – advantages/ disadvantages, cloud computing.
12. 3D Information Security Models - Threats, information security requirements, information security risk management, security policy, evaluation criteria, methods and standards.
13. Encryption and Coding - Relationship and difference, basic terms: open text and encrypted text alphabet, key space computation relationships, symmetric/asymmetric and hybrid cryptography – principles - advantages and disadvantages, steganography - principles, divisions and examples.
14. Classical Cryptography: Substitution and Transposition Systems - Differences between them and their complete distribution, examples and principles of selected most important cryptographic systems.
15. Modern Cryptography: Symmetric Stream and Block Ciphers – The Vernam Cipher and other examples of modern cryptographic systems, differences, asymmetric cryptography – one-way cryptographic functions, Diffie-Hellman Protocol, RSA.

16. Cryptographic Systems Attacks - Distribution and description of the most basic cryptographic systems attacks, cryptanalysis - description and methods of simple substitution systems analysis, Vigener's substitution systems and modern ciphers.
17. Legitimate and Illegitimate Communication Interception Reasons for Computer Networks - The interception principle, the description of individual sniffer parts and their location in the network possibilities, the principle and evaluation of interception defence in computer network possibilities.
18. Virus Body-masking in Host File Methods - Virus decryptors, virus detection definition and detection methods, the DarkAvenger mutation engine.
19. Forensic Data Analysis – The preliminary safe secured -handling phase, data analyses on disks - (specify the most common), describe the most frequently-used network traffic data analysis methods (most frequently searched information + specific data that can be found in network traffic), what are the limiting network communication analysis conditions?
20. Penetration Test Implementation Tests - Characteristics of penetration test individual phases, the standards to be tested, the most frequently tested IT infrastructure structures, penetration test comparisons with real infrastructure attacks.