Course title: INFORMATION SYSTEMS SECURITY

Lecturers	Asst.Prof. Tonimir Kišasondi, Ph.D.
Language of instruction:	Croatian and English
Schedule:	60 teaching hours - 4 hours per week (2 hours lectures + 2 hours laboratory exercises)
Study level	Master
Study programme	Information / Business Systems
Semester	Winter
ECTS	5
Goal	Introducing the students to problematics of information system security, especially in conditions of dependency of business systems upon business content communication with support of information technology. European legal regulative and means of fulfillment of that regulative as a pre-condition for certification. Introduction to methods of design and development of security. Role of individual measures for reduction of risk levels in individual segments of information system. Development of skills of construction of particular security measures. The goal of exercises is to introduce the students to technical means for realization of particular forms of protection and security of information systems. After passing the colloquium of exercises, the students should be able to build and manage protection of segment of information system supported by computer through aspects of protection which may be implemented on that level.
Content	1. Meaning of information system protection (4 hours) Notion of security and protection of information system efficiency; reasons for protection of information system; dependency of organizational development of business system upon efficient protection of information system. Historical development of system of protection and security with indicators of possible directions of development. (2 hours) Meaning of information content; economical, cultural or political motives of threat; types and forms of threats throughout history; threats to hardware and structural elements of information system; threats to software foundations; threats to communication system; threats to operators. Notion of computer

	crime, origins, development and form of computer crime, carriers of illegitimate activities based upon information technology. (2 hours) 2. Approach to information system projecting (8 hours) Planning and projecting security and protection in course of information system development. Review of standards used in projecting security of information resources; means of realization of information system security according to place of threats and according to place and method of protection. (2 hours) Steps in development of security system of business information system; defining the policy of information system security; choice of strategies for development of security systems of information system; choice of responsible parties for building security systems; choice of approach to mode of realization of security system. Evaluation of significance of business system data content; external factors of business content significance, internal factors of business data content significance; evaluation of forms and intensities of threats to data content regarding the evaluated content. (4 hours) Risk analysis; evaluation of risk of a particular content; quantitative measures of evaluation; fields of application of this method and qualitative measures of evaluation. Choice of protection measure. Security measures. Risk management, analysis of risk types, priority setting, plan of information system security. Plan of recovery from disaster. Valorization of efficiency of security methods. (2 hours) 3. Organizational, program, technical and physical security meaures (12 hours) Modes of realization of organizational, program, technical and physical security measures. Means of technical security. Boundaries of organizational, program, technical and physical security measures. (2 hours) Protection measures of information systems; material carrier as a protection measure; program protection measures; protection on the level of operation system; protection on the level of applicative program support; safety copy with change of material carrier as protection measure; protection by cryptographic protection measures; symmetric crypto systems; asymmetric crypto systems; function of digital signature; modes of realization of digital

	signature; infrastructure of digital signature; fields of application of digital signature. (3 hours) Anti-virus protection; history of virus origins; notion of virus and types of malicious software; routes of virus infection; consequences of virus attack; types of virus according to method of hiding; types of virus according to method of operation; methods of prevention in anti-virus protection; methods for virus detection; possibilities of program solutions for virus identification; "cure" and recovery of infected system. (3 hours) Technical measures of protection; measures of protection on the level of computer system; measures for increasing redundancy of equipment, depending upon risk of content disappearance and continuity of system functionality; protection measures made by setting alternate power systems; impeding access into protected area; supervision of area during trespassing; safety locks; chip cards; biometric inspection; fingerprint; geometry of hand; geometry of head; constitution of eye iris; voice checking; combined measures of inspection; conditions of application of a particular measure; physical protection measures; structural protection measures; placement of sensitive informatic equipment in space; placement of equipment within the building; measures of fire protection; preventive measures, identification measures and measures of fire extinguishing. (2 hours) Organizational protection measures; choice of norm; application of norm; elaboration of required organizational and implemental acts as organizational measure; system of certification of measures applied according to particular norm. Protection measures in legal domain, relation of the state toward security system through passing of particular acts, normative acts related to security within business system. Validity check of applied protection measures. (2 hours) 4. Data security during processing and storage: (4 hours) Realization of security on the level of operational system; licences and copyrights; comparison of Windows protection systems and concepts of protection on Unix platform; protection system with use of password; policies of password assignment and change. Assignment of user interface, deletion and temporal revoking of user interface, rules of exclusion. Conditions and modes of security firewall setting . (2 hours)

	Security on the application level; creation of user interface; assignment of system resources according to problem domain of a workplace. Data storage on carriers with analogue inscription. Means of storage with digital inscription; system of security storage; normal storage; incremental storage; differential storage; daily storage; storage strategies. Multimedia systems of storage. (2 hours) 5. Other aspects of information system security (2 hours) Security standards. Legal protection of softwares; copyright; ownership of software product; licence rights. International aspect of information system protection. Efficiency analysis of the applied protection methods of information center content and users; evaluation of functionality of information protection. Ergonomical aspect of information system security. (2 hours)
Exercises	Exercises: 1. Safety settings in Windows XP operational system (2 hours) User accounts – types, creating, rights. Modes of system access (used security protocols). User groups. User account management. Local Security Settings – policy of user accounts, local politics, limitation of software access, IP security policy. 2. Security settings in NTFS file system (2 hours) Features and structure of NTFS file system. ACL. NTFS access rights to resources. Supervision and analysis of access control. Encrypted file system. 3. Security settings in Linux 1 operating system (2 hours) Linux users and groups – storing of user information; change of users and passwords. Means of system registration (used security protocols). Supervision of users – quote, setting limitations through PAM, bash limitation. Use of Webmin tool for configuration of users, groups and related properties. 4. Security settings in Linux 2 operating system (2 hours) Critical systemic configuration files. Following system notes – general security of notes, system notes. Cryptographic file system – Linux CryptoAPI. 5. Cryptography – PGP/GPG (2 hours) Asymmetrical cryptography. Implementation of asymmetric cryptography through PGP/GPG tools. Installation and configuration of PGP and GPG

	(GnuPG) tools (Windows/Linux). Generating the pair private/public key. Exchange of public keys through key-servers and key-server search. 6. Cryptography – PGP/GPG (2 hours) Use of PGP/GPG tools – encryption of files and e-mails, digital signature; file and e-mail decryption; digital signature validity check. 7. Anti-virus protection and firewall (2 hours) Norton Antivirus – installation, setting customization, media scanning, restoration of base with virus definitions, reports, carantine. Purpose of firewall, device for traffic filtering. Personal firewall – Integrated Windows Firewall (ICF), Kerio Personal Firewall, Sygate Personal Firewall – installation, configuration, filtering rule definition 8. Security data storage (1 hour) Types of security storage – copying (with or without compression), common backup, differential and incremental backup. Security storage of system computer settings. Application through Windows Backup Utility. In the course of exercises, the students use standard program tools, which are commercially used for support to electronic business operations, and apply them to practical examples. The students learn to create XML documents and their definitions, to transform XML documents and to transfer them into various specifications. Furthermore, the students use standard commercial tools for support to managing the chain of supply, learn about its parameters, setup principles and usage mode.
Preconditions	-
Realization and examination	Classes: Lectures, seminars and exercises Exam: Compulsory testing of practical work on computer as a pre-condition for theoretical part of exam, which is realized in written and oral examination. Written part of examination consists of seminar evaluation and several written tests during lectures, or written tests after lectures. Oral part of examination is evaluation of authenticity of previous results and possibility for grade improvement achieved through written exams. The exams are partially conducted through LMS.
Related courses	1. IT-Security, TUG (Techniche Universitat Graz)

	2. Telematik IV - IT Security, Albert-Ludwigs Univ., Freiburg 3. Computer and Network Security, University of Florida
Literature	Basic: 1. BS ISO/IEC 17799:2000 - BS 7799-1:2000 norma - Information Technology - Code of Practice for Information Security Management, BSI, UK, 2001. 2. Peltier R.T., Information Security Risk Analysis, Auerbach, CRC press, 2000. 3. Tudor J.K., Information Security Architecture, CRC Press LLC, USA, 2001. Exercises: 1. Bott E., Siechert C., Microsoft Windows XP Inside Out, Microsoft Press, 2001 2. Linux dokumentacija, URL: http://dokumentacija.linux.hr/ Additional: 1. Ashbourn J., Biometrics - Advanced Identity Verification, Springer-Verlag, UK, 2000. 2. Humphreys E.J, Moses R.H., Plate A.E., Guide to Risk Estimation and Risk Management, BSI, UK, 1998. 3. Scheiner B., Applied Cryptography, John Wiley & Sons Inc., USA, 1996Thorenson J.D., Blankenship J.H., Information Secrets, Valuable Information Ltd, USA, 1996. Exercises: 1. Various textbooks and on-line documentation for program tools used in exercises course.