**Universitatea Naţională de Ştiinţă şi Tehnologie Politehnica Bucureşti**
**Facultatea de Electronică, Telecomunicaţii şi**
**Tehnologia Informaţiei**

# COURSE DESCRIPTION

## 1. Program identification information

| | |
|---|---|
| 1.1 Higher education institution | **National University of Science and Technology Politehnica Bucharest** |
| 1.2 Faculty | **Electronics, Telecommunications and Information Technology** |
| 1.3 Department | **Telecommunications** |
| 1.4 Domain of studies | Electronic Engineering, Telecommunications and Information Technology |
| 1.5 Cycle of studies | Masters |
| 1.6 Programme of studies | Advanced Wireless Communications |

## 2. Date despre disciplină

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2.1 Course name (ro)<br>(en) | | | | Managementul incidentelor de securitate şi audit<br>The Management and Audit of Security Incidents | | | |
| 2.2 Course Lecturer | | | | Conf. Dr. Constantin Viorel Marian | | | |
| 2.3 Instructor for practical activities | | | | Conf. Dr. Constantin Viorel Marian | | | |
| 2.4 Year of studies | 1 | 2.5 Semester | I | 2.6. Evaluation type | V | 2.7 Course regime | Ob |
| 2.8 Course type | | S | 2.9 Course code | 6 | | 2.10 Tipul de notare | Nota |

## 3. Total estimated time (hours per semester for academic activities)

| | | | | | |
|---|---|---|---|---|---|
| 3.1 Number of hours per week | 2 | Out of which: 3.2 course | 1.00 | 3.3 seminary/laboratory | 1 |
| 3.4 Total hours in the curricula | 28.00 | Out of which: 3.5 course | 14 | 3.6 seminary/laboratory | 14 |
| Distribution of time: | | | | | hours |
| Study according to the manual, course support, bibliography and hand notes<br>Supplemental documentation (library, electronic access resources, in the field, etc)<br>Preparation for practical activities, homework, essays, portfolios, etc. | | | | | 20 |
| Tutoring | | | | | 0 |
| Examinations | | | | | 2 |
| Other activities (if any): | | | | | 0 |

| | |
|---|---|
| 3.7 Total hours of individual study | 22.00 |
| 3.8 Total hours per semester | 50 |
| 3.9 Number of ECTS credit points | 2 |

## 4. Prerequisites (if applicable) (where applicable)

| | |
|---|---|
| 4.1 Curriculum | Have skills obtained as a result of completing the computer course(s).<br><br>• It is mandatory that students have knowledge to use the Linux operating system.<br>• Each student must have knowledge of Unix operating systems / environments (Free BSD, OpenBSD) and basic knowledge of configuring the Windows operating system).<br>• Each student must have basic knowledge of computer networking.<br>• In addition, each student must have a basic knowledge of programming.<br><br>Completion and/or promotion of the following programs is beneficial:<br><br>• Linux Operating Systems<br>• Databases<br>• Web Applications |
| 4.2 Results of learning | Accumulate the following knowledge:<br><br>• Each student must have the ability to use a personal computer and server.<br>• Students must know how to use networked computers.<br>• Use knowledge of computer configuration and computer networks.<br>• Use knowledge of Unix/Linux/Windows operating system configuration. |

**5. Necessary conditions for the optimal development of teaching activities** (where applicable)

| | |
|---|---|
| 5.1 Course | Projector<br>Course Notes<br>Recommended reading |
| 5.2 Seminary/ Laboratory/Project | Computers with minimum 2 Linux virtual machines, firewall;<br>Attendance and mandatory activities at laboratories (according to the regulations of the university studies in the UPB). |

**6. General objective** *(Reffering to the teachers' intentions for students and to what the students will be thought during the course. It offers an idea on the position of course in the scientific domain, as well as the role it has for the study programme. The course topics, the justification of including the course in the currcula of the study programme, etc. will be described in a general manner)*

The objective of this course is to provide an initial overview of procedural and IT security within a company, as well as to raise students' awareness of IT security. By the end of the course, students will understand some of the basic concepts of business management in general and procedural operational management applied to IT security concepts.

The course also aims to discuss the basic principles and main technologies used in securing personal computers, personal computer security management, and security services for protecting personal computers: definitions, techniques, and mechanisms used.

The applications aim to apply the concepts presented in the course, recognize the particularities of the context of application of IT security procedures and technologies, and select the optimal solution. The course aims to design, configure, operate, and audit the main technologies related to personal computer security and operating system security.

It also aims to provide knowledge and understanding of current types of cyber attacks, technical measures to prevent or remove them, the necessary procedures to be applied, and finally, the auditing of a complex system.

**7. Competences** *(Proven capacity to use knowledge, aptitudes and personal, social and/or methodological abilities in work or study situations and for personal and proffesional growth. They refflect the empolyers requirements.)*

| | |
|---|---|
| **Specific Competences** | • The ability to specify, plan, track and execute a technical project in the field of telecommunications, especially in mobile communications and wireless access networks;<br>• Giving a comprehensive image on the detection and recovery techniques of data transmitted over wireless channels (reception diversity, modulation / demodulation techniques, equalization, detection, etc.);<br>• The ability to design and implement on the field a mobile access system, in a variety of wireless communication technologies;<br>• Design, implementation and management of small and large radio networks, in order to ensure safe access and guaranteed performance;<br>• The ability to analyze and determine the system-level specification of physical layer equipment and their higher level modules;<br>• The ability to specify services and applications for mobile communications, to develop such small and medium-scale applications and to implement them in a mobile communication system;<br>• Solving of the professional tasks with precise identification of objectives to be achieved, potential risk factors, available resources, financial aspects, working conditions, time schedule and execution terms;<br>• Responsibly working in a multidisciplinary team with abilities to assume roles specific to different hierarchical levels;<br>• Capacity to identify the need for continuous education and efficient use of information sources, communication resources and training assistance (Internet portals, specialized software, databases, online courses) both in Romanian and a foreign language. |
| **Transversal (General) Competences** | • Ability to team work;<br>• Ability to effectively communicate in written, oral and poster format;<br>• Skills of computer use, information technology and specific equipment;<br>• Capacity to take responsibilities;<br>• Capacity to document, research and develop specialized studies;<br>• Capacity to continue education and develop professional competences. |

**8. Learning outcomes** *(Synthetic descriptions for what a student will be capable of doing or showing at the completion of a course. The learning outcomes reflect the student's acomplishments and to a lesser extent the teachers' intentions. The learning outcomes inform the students of what is expected from them with respect to performance and to obtain the desired grades and ECTS points. They are defined in concise terms, using verbs similar to the examples below and indicate what will be required for evaluation. The learning outcomes will be formulated so that the correlation with the competences defined in section 7 is highlighted.)*

| | |
|---|---|
| **Knowledge** | *The result of knowledge aquisition through learning. The knowledge represents the totality of facts, priciples, theories and practices for a given work or study field. They can be theoretical and/or factual.*<br><br>• Ability to analyze security risks and determine specifications for secure electronic and communication equipment and systems;<br>• Identification of vulnerabilities and security risks at the level of telecommunications protocols and networks (including virtualization and cloud) and use of security protocols;<br>• Conceiving, designing, and implementing security plans at the critical organization/infrastructure level;<br>• The ability to design and implement cryptographic applications, systems, and protocols using FPGA devices, on-chip systems, software, etc.<br>• Ability to design and implement secure hardware (computers, mobile terminals) and software (databases, software applications) systems<br>• Ability to assess and audit the security of industrial control systems and critical infrastructures, to apply security and auditing standards;<br>• Ability to understand and propose advanced security solutions based on machine learning, artificial intelligence, and big data<br>• Ability to analyze and propose solutions for securing and exploiting multimedia content<br>• Performing professional tasks with the accurate identification of objectives to be achieved, potential risk factors, available resources, economic and financial aspects, conditions for their completion, work stages, working time, and related deadlines;<br>• Responsible execution of tasks in a multidisciplinary team, assuming roles at different hierarchical levels. |
| **Skills** | *The capacity to apply the knowledge and use the know-how for completing tasks and solving problems. The skills are described as being cognitive (requiring the use of logical, intuitive and creative thinking) or practical (implying manual dexterity and the use of methods, materials, tools and intrumentation).*<br><br>• Ability to work in a team;<br>• Communication skills;<br>• Computer, information technology, and specific equipment skills;<br>• Ability to take responsibility;<br>• Ability to document, research, and develop specialized studies;<br>• Ability to engage in continuous training and personal and professional development throughout one's career. |
| **Responsability and autonomy** | *The student's capacity to autonomously and responsably apply their knowledge and skills.*<br><br>• Ability to work in a team<br>• Communication skills |

**9. Teaching techniques** *(Student centric techniques will be considered. The means for students to participate in defining their own study path, the identification of eventual fallbacks and the remedial measures that will be adopted in those cases will be described.)*

- Lecture

- Explanation
- Problematic
- Demonstration
- Conversation
- Case Studies

Courses are taught in an interactive way, encouraging the active participation of students with multimedia tools and techniques (video projector).

- Conversation
- Demonstration
- Individual experiment
- Experiment in small group
- Exercises
- Case Studies
- Presentations reports
- Evaluation / assessment

Project / laboratory applications are based on individual experimentation of the methods and techniques presented in the course. Students are required to study the bibliography and to complete a project.

**10. Contents**

| **COURSE** | | |
|---|---|---|
| **Chapter** | **Content** | **No. hours** |

| | | |
|---|---|---|
| 1 | 1. The organizational context for security incidents.<br>Management of the organization / enterprise in relation to information security.<br>IT security auditing procedure:<br>• interviews with the company's technical department;<br>• observing the way employees work;<br>• hardware / software configuration analysis of the equipment;<br>• the concept and design of an IT & C security policy;<br>• implementing the most appropriate network security solutions;<br>• protected access systems, locally or remotely;<br>• firewall and VPN solutions;<br>• intrusion detection (IDS) and vulnerability assessment;<br>• Content security (antivirus solutions, web filtering and email);<br>• authentication solutions;<br>• encryption solutions and digital signatures;<br>• security management solutions;<br>• Developing a comprehensive IT infrastructure and security report.<br>2. Risk assessment / risk management planning<br>3. Resources needed for implementation<br>4. Implementation and control of functional processes<br>5. Evaluating the effectiveness and performance of implementing information security measures<br>6. Continuous monitoring and improvement<br>7. Standardization of ITIL (IT Infrastructure Library) and IT Service Management<br>• Service strategy<br>• design<br>• transition<br>• Operation<br>• Continuous improvement | 14 |
| | **Total:** | 14 |

**Bibliography:**

1. C. V. Marian, "Support for course and lab" , "Suport de curs si laborator", Moodle UPB, https://curs.upb.ro/
2. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems (replacing Sistemul de management al securităţii informaţiei ISO/IEC 27001:2013)
3. MIHAI Ioan-Cosmin, "Securitatea sistemului informatic", ISBN 978-973-627-369-8, Editura Dunărea de Jos (2007)
4. L Brotherston, A Berlin. "Defensive Security Handbook: Best Practices for Securing Infrastructure", O'Reilly Media Ed, 2017.
5. S Bosworth, M E Kabay, E Whyne. "Computer Security Handbook, 6th Edition (vol 1, vol 2)", Wiley Ed, 2014.
6. C. V. Marian, „Operating systems and web applications fundamentals”, Editura Politehnica Press, Bucureşti, 2021, ISBN 978-606-515-989-1
7. C. V. Marian, „Apprendre l'administration des systèmes d'exploitation par des exemples (Linux)”, Editura Politehnica Press, Bucureşti, 2022, ISBN 978-606-9608-19-7
8. C. V. Marian, „Applications pour les administrateurs de systèmes et les serveurs Linux”, Editura Politehnica Press, Bucureşti, 2023, ISBN 978-606-9608-67-8
9. M. T. Goodrich, R. Tamassia. "Introduction to Computer Security". Person Ed., International Edition. 2010.
10. Wm. A. Conklin, G. G. White, C. Cothren, D. Williams, R. L. Davis. "Principles of Computer Security. Security+ and Beyond". Mc Graw Hill Higher Education Ed. 2004.
11. W. Stallings. "Computer Security: Principles and Practice". Prentice Hall Ed. 2011.
12. W. Stallings. "Cryptography and Network Security: Principles and Practice". Pearson Ed., International Edition. 2010.
13. G. Avoine, P. Junod, P. Oechslin. "Computer System Security". EPFL Press. 2007.

**LABORATORY**

| Crt. no. | Content | No. hours |
|---|---|---|
| 1 | 1. Formulate organizations' safety objectives and requirements;<br>Ensuring that security risks are managed cost-effectively;<br>2. Ensuring compliance with legislation and regulations;<br>Implement and manage existing information security management processes;<br>3. Defining new information security management processes;<br>Identify and clarify existing information security management processes;<br>4. Its use by management of organizations to determine the status of information security management activities;<br>5. Use by internal and external auditors of organizations to determine compliance with policies, directives, and standards adopted by the organization;<br>Providing relevant information about information security policies, directives, standards and procedures to trading partners and other organizations with which the organization interacts for operational or commercial reasons;<br>6. Implementing the strategy by activating information security;<br>Provide relevant information about the organization's information security.<br>7. Final Colloquium | 14 |
| | **Total:** | 14 |

**Bibliography:**

1. C. V. Marian, "Support for course and lab" , "Suport de curs si laborator", Moodle UPB, https://curs.upb.ro/
2. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems (replacing Sistemul de management al securităţii informaţiei ISO/IEC 27001:2013)
3. L Brotherston, A Berlin. "Defensive Security Handbook: Best Practices for Securing Infrastructure", O'Reilly Media Ed, 2017.
4. W. Stallings. "Computer Security: Principles and Practice". Prentice Hall Ed. 2011.
5. Paul Cobbaut. Linux Security http://linux-training.be/index.php?nav=security
6. C. V. Marian, Operating systems and web applications fundamentals, Editura Politehnica Press, Bucureşti, 2021, ISBN 978-606-515-989-1
7. C. V. Marian, Apprendre l'administration des systèmes d'exploitation par des exemples (Linux), Editura Politehnica Press, Bucureşti, 2022, ISBN 978-606-9608-19-7
8. C. V. Marian, Applications pour les administrateurs de systèmes et les serveurs Linux, Editura Politehnica Press, Bucureşti, 2023, ISBN 978-606-9608-67-8

**11. Evaluation**

| Activity type | 11.1 Evaluation criteria | 11.2 Evaluation methods | 11.3 Percentage of final grade |
|---|---|---|---|
| 11.4 Course | • Knowledge of fundamental theoretical notions regarding the technical and procedural security of computers;<br>• Knowing how to apply procedures to specific problems;<br>• Differential analysis of theoretical audit techniques and methods;<br>• Ability to analyze specialized literature through individual study and extract key information on removing security vulnerabilities. | Exam written in the exam session corresponding to the semester; the subjects cover the whole matter, making a synthesis between the theoretical comparative study of the subject and the applications. | 20% |
| 11.5 Seminary/laboratory/project | • Configuration of the equipment according to the course notions and the techniques presented at the laboratory. | Final project / laboratory project colloquium. Both the understanding of the theoretical aspects and the ability to implement and test a practical problem are evaluated. | 80% |
| 11.6 Passing conditions | | | |

| |
|---|
| Knowledge, understanding and correct use of procedures and fundamental concepts in the field of personal computer security<br>Understanding the main types of computer attacks and the ability to design and process a functional security system<br>Fulfillment of the project / laboratory activities (participating in the planned works). |

**12. Corroborate the content of the course with the expectations of representatives of employers and representative professional associations in the field of the program, as well as with the current state of knowledge in the scientific field approached and practices in higher education institutions in the European Higher Education Area (EHEA)**

The subject meets national and international requirements in the domain of electronics and IT&C and its economic financial impact, being correlated with similar subjects in and outside Romania.

In the present development context the domain electronics offers a wide range of activity, potential employers belonging to the industry, to education and research and development with NGOs and national, international and multinational enterprises from the field of electronics and IT&C.

The students aquire competencies that meet the present requirements and allow them a rapid insertion on the labour market after graduation, as well as the chance to continue to study various master and doctoral programms, this program being well integrated in the policies and strategies of the University POLITEHNICA Bucharest regarding its content and its structure, as well as the skills and the international perspective offered to the students.

Course and project / laboratory applications provide students with the knowledge base needed to understand the main security issues related to personal computers and specific approaches. Concretely, the discipline provides both the knowledge needed to design and validate security policies that are appropriate for the protection of personal computers and the ability to apply techniques for analyzing and detecting computer attacks and eliminating or mitigating the effect of these attacks on personal computing systems.

The program of the discipline responds concretely to the current development and evolution requirements of the European economy and ICT services. In the context of the current technological progress of electronic computing systems and devices, the areas of activity concerned are virtually limitless, ranging from the use of large-scale computing to the use of state-of-the-art portable terminals. The program refers to both the technical measures that are required for the protection of information technology and those concerning the behavior of the employees in their relationship with the computer equipment.

The discipline provides the graduates with the appropriate skills with the current qualification requirements and a modern, high quality and competitive scientific and technical training that will allow them to be hired after graduation, being perfectly integrated into the politics of POLITEHNICA University in Bucharest, both in terms of content and structure, as well as from the point of view of the aptitudes and international openness offered to the students. Possible employers target both the academic environment (didactic and research profile) as well as the industrial R & D environment as organizations / firms of any size, from small ones created by students / master students to multinationals using personal computers (connected or not on the network) and are interested in managing their security.

**Universitatea Naţională de Ştiinţă şi Tehnologie Politehnica Bucureşti**

**Facultatea de Electronică, Telecomunicaţii şi**

**Tehnologia Informaţiei**

| | | |
|---|---|---|
| Date | Course lecturer | Instructor(s) for practical activities |
| | Conf. Dr. Constantin Viorel Marian | Conf. Dr. Constantin Viorel Marian |
| Date of department approval | Head of department | |
| Date of approval in the Faculty Council | Dean | |