

DESCRIPTION OF A STUDY COURSE – SYLLABUS

| | | | | | |
|---|---|-----------------|--|---------------------|---|
| Title of a course | Information Systems Security | | | | |
| Head of course | PhD Bernard Vukelić, College Professor | | | | |
| Study programme | Professional undergraduate study Information Science | | | | |
| Status of a course | Obligatory | | | | |
| Year of study | 2 | Semester | III | ECTS credits | 5 |
| Teaching plan (L + E + S+ Pr) | 2+2+0+0 | | | | |
| Goals of a course | | | | | |
| The aim of course is to acquire knowledge about aspects of information systems security and to develop awareness of the importance of information security in the enterprise. | | | | | |
| Conditions for enrolling course | | | | | |
| No conditions | | | | | |
| Learning outcomes on a level of a study programme which includes course | | | | | |
| Outcome 5: Apply website design and implementation methods. Outcome 6: Apply appropriate business information system protection techniques. Outcome 12: Apply engineering methods and principles in information science. Outcome 15: Independently present professional content in written and spoken form in Croatian and English. | | | | | |
| Expected learning outcomes on a level of a course | | | | | |
| <ol style="list-style-type: none"> 1. Describe the concepts of security, information systems security, information systems security management and privacy. 2. Describe the legal and institutional aspects and different norms and standards in the field of information systems security. 3. Assess the impact of the elements of integrity, confidentiality and accessibility on information in the information system 4. Determine the impact of information systems security management on a company's business operations and business continuity 5. Develop a company's security policy 6. Identify internal and external threats and vulnerabilities of a company's information system 7. Assess security risks in an information system 8. Plan technical solutions for information systems protection | | | | | |
| Content of a course | | | | | |
| Importance of information system for owner and user. Importance of information system security, concept of security, realisation of information system effectiveness, models of information system security. Approach to information system security project and organization: planning, standards, risk analysis, safety measures. Organizational, program, technical and physical safety measures by types and means. Data security during processing and storing. Other aspects of information system protection. | | | | | |
| Teaching modes | <input checked="" type="checkbox"/> lectures <input type="checkbox"/> auditory exercises <input checked="" type="checkbox"/> seminars and workshops <input type="checkbox"/> distance learning <input type="checkbox"/> field classes | | <input checked="" type="checkbox"/> individual assignments <input type="checkbox"/> multimedia and network <input type="checkbox"/> laboratory <input type="checkbox"/> supervisor's work <input type="checkbox"/> other _____ | | |
| Comments | | | | | |
| Students' obligations | | | | | |
| Submit homework or solved assignment. | | | | | |
| Grading, evaluation and monitoring of students' work continuously during lectures and exams | | | | | |

Grading is based upon evaluation of course's learning outcomes' adoption. Grading is performed continuously during lectures and/or during exam, in compliance with the provisions of Regulation on the assessment of students.

Continuous check-up:

| Outcomes | Written test | Assignment | Home assignment | Threshold | Max |
|--------------------|--------------|------------|-----------------|-----------|-------|
| Outcome 1 | 5% | | | 2,5% | 5% |
| Outcome 2 | 5% | | | 2,5% | 5% |
| Outcome 3 | 10% | | | 5% | 10% |
| Outcome 4 | 10% | | | 5% | 10% |
| Outcome 5 | | | 10% | 5% | 10% |
| Outcome 6 | | | 10% | 5% | 10% |
| Outcome 7 | 10% | 20% | | 15% | 30% |
| Outcome 8 | | 20% | | 10% | 20% |
| Percentage of ECTS | 2 | 2 | 1 | - | - |
| Total | 40% | 40% | 20% | 50 % | 100 % |

A student has passed the exam if he has acquired a percentage of credits for each learning outcome higher or equal to defined threshold.

Exam term:

| Outcomes | Theoretical part / Written exam | Practical part / Oral exam / Assignment | Max |
|--------------------|---------------------------------|---|-------|
| Outcome 1 | 10% | | 10% |
| Outcome 2 | 10% | | 10% |
| Outcome 3 | 10% | | 10% |
| Outcome 4 | 10% | | 10% |
| Outcome 5 | 10% | | 10% |
| Outcome 6 | 10% | | 10% |
| Outcome 7 | | 20% | 20% |
| Outcome 8 | | 20% | 20% |
| Percentage of ECTS | 3 | 2 | - |
| Total | 60% | 40% | 100 % |

A student has passed the exam if he has acquired a percentage of credits for each learning outcome higher or equal to defined threshold.

Grading:

A student has passed the exam if he has acquired at least 50% of anticipated credits of a specific learning outcome.

If a student has passed learning outcomes of all courses, the accomplished credits (percentages) of all passed learning outcomes are being added, while the final grade is defined upon following table:

| Range of credits (percentages) | Numerical grade | ECTS grade |
|--------------------------------|------------------|------------|
| 90,00 – 100,00 | Excellent (5) | A |
| 75,00 – 89,99 | Very good (4) | B |
| 60,00 – 74,99 | Good (3) | C |
| 50,00 – 59,99 | Sufficient (2) | D |
| 0,00 – 49,99 | Insufficient (1) | F |

- | |
|---|
| 1. Klasić, K.; Zaštita informacijskih sustava, Biblioteka inženjera sigurnosti, Zagreb, Visoka škola za sigurnost na radu – IPROZ, 2002., Bača M.: Uvod u računalnu sigurnost, NN, Zagreb, 2004., ISO/IEC 27001 standard, Hrvatski zavod za norme |
|---|

| |
|------------------------------|
| Additional literature |
|------------------------------|

- | |
|---|
| 1. CERT Hrvatska – www.cert.hr – Dokumenti po nastavnoj temi |
|---|

