

| STUDY MODULE DESCRIPTION FORM | | |
|---|---|---|
| Name of the module/subject Information security in Internet | | Code 1010335431010334336 |
| Field of study Information Engineering | Profile of study (general academic, practical) (brak) | Year /Semester 2 / 3 |
| Elective path/specialty Security of Information Technology (IT) | Subject offered in: polish | Course (compulsory, elective) obligatory |
| Cycle of study: Second-cycle studies | Form of study (full-time, part-time) part-time | |
| No. of hours Lecture: 16 Classes: - Laboratory: 12 Project/seminars: - | | No. of credits 5 |
| Status of the course in the study program (Basic, major, other) (brak) | | (university-wide, from another field) (brak) |
| Education areas and fields of science and art technical sciences | | ECTS distribution (number and %) 100 5% |
| Responsible for subject / lecturer: dr hab. inż. Janusz Stokłosa, prof. nadzw. email: janusz.stoklosa@put.poznan.pl tel. +48 61 665 37 57 Wydział Elektryczny ul. Piotrowo 3A 60-965 Poznań | | |
| Prerequisites in terms of knowledge, skills and social competencies: | | |
| 1 | Knowledge | Eng. ver. - Ma pogłębioną wiedzę w zakresie bezpieczeństwa danych. Ma pogłębioną wiedzę w zakresie kryptografii i wstępna w zakresie kryptoanalizy. |
| 2 | Skills | Eng. ver. - Potrafi stosować zaawansowane narzędzia i technologie informatyczne. |
| 3 | Social competencies | Eng. ver. - Rozumie potrzebę przekazywania społeczeństwu informacji dotyczących osiągnięć informatyki i innych aspektów działalności inżyniera-informatyka; podejmuje starania, aby przekazać informacje w sposób zrozumiały, przedstawiając różne punkty widzenia. |
| Assumptions and objectives of the course: Presentation of cryptographic protocols on the Internet. | | |
| Study outcomes and reference to the educational results for a field of study | | |
| Knowledge: | | |
| 1. Eng. ver. - Ma wiedzę o aktualnych trendach dotyczących zastosowań informatyki oraz kluczowych problemów z tym związanych. - [K_W06] | | |
| 2. Eng. ver. - Ma wiedzę o trendach rozwojowych i najistotniejszych nowych osiągnięciach w zakresie informatyki - [K_W14] | | |
| Skills: | | |
| 1. Eng. ver. - Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji i krytycznej oceny, a także wyciągać wnioski oraz formułować i wyczerpująco uzasadniać opinie. - [K_U01] | | |
| 2. Eng. ver. - Potrafi zaproponować i uzasadnić ulepszenia istniejących rozwiązań informatycznych. - [K_U12] | | |
| Social competencies: | | |
| 1. Eng. ver. - Potrafi myśleć i działać w sposób kreatywny i przedsiębiorczy. - [K_K01] | | |
| Assessment methods of study outcomes | | |
| Written or/and oral examination based on lecture. Laboratory: written test. | | |
| Course description | | |

| | | |
|--|------------------------------------|--------------------|
| <p>Standardization, TLS, IPsec (ESP, AH, ISAKMP, IKE), PKIX (Profiles, LDAP i OSCP, certification policy), PKCS (Cryptographic libraries, PKCS #11 - Cryptoki), Time stamping, cryptographic algorithms in access networks (GSM, UMTS, IEEE 802.11i).</p> <p>Laboratory: SSL, TLS, S-HTTP protocols; Digital certificate; Public cryptographic system ? based on RSA, Communication security ? Secure Shell; Cryptographic algorithms in radio access networks</p> | | |
| <p>Basic bibliography:</p> <ol style="list-style-type: none"> 1. Bezpieczeństwo danych w systemach informatycznych, Stokłosa J., Bilski T., Pankowski T., Wydawnictwo Naukowe PWN, Warszawa-Poznań, 2001 2. Network and Internetwork Security, W. Stallings, Prentice Hall, 1994 3. RFC., http://www.ietf.org/rfc.html | | |
| <p>Additional bibliography:</p> <ol style="list-style-type: none"> 1. Digital Signature Schemes., B. Pfitzmann, Springer, Berlin, 1996 2. Protection and Security on the Information Superhighway, F. B. Cohen, J. Wiley, New York, 1995. 3. Selected papers from Lecture Notes in Computer Science, Springer. | | |
| <p>Result of average student's workload</p> | | |
| <p>Activity</p> | <p>Time (working hours)</p> | |
| 1. Lecture | 30 | |
| 2. Laboratory | 15 | |
| 3. Preparation to the laboratory | 15 | |
| 4. Realization of laboratory reports | 10 | |
| 5. Preparation to tests | 10 | |
| 6. Preparation to the examination | 35 | |
| 7. Participation in the consultations and examination | 10 | |
| <p>Student's workload</p> | | |
| <p>Source of workload</p> | <p>hours</p> | <p>ECTS</p> |
| Total workload | 125 | 5 |
| Contact hours | 50 | 2 |
| Practical activities | 25 | 1 |