Security Engineering - course description

General information

Course name	Security Engineering
Course ID	11.9-WI-INFD-IB
Faculty	Faculty of Computer Science, Electrical Engineering and Automatics
Field of study	Computer Science
Education profile	academic
Level of studies	Second-cycle studies leading to MSc degree
Beginning semester	winter term 2019/2020

Course information

Semester	1
ECTS credits to win	5
Course type	obligatory
Teaching language	polish
Author of syllabus	• dr hab. inż. Bartłomiej Sulikowski, prof. UZ

Classes forms

The class form	Hours per semester (full-time)	Hours per week (full-time)	Hours per semester (part-time)	Hours per week (part-time)	Form of assignment
Lecture	30	2	18	1,2	Exam
Laboratory	30	2	18	1,2	Credit with grade

Aim of the course

- zapoznanie studenta z aktami prawnymi w Polsce regulującymi zasady ochrony informacji niejawnej oraz regulacjami z nich wynikającymi

- zapoznanie studenta z algorytmami i protokołami kryptograficznymi

- ukształtowanie umiejętności w zakresie stosowania procedur ochrony informacji

- zapoznanie studenta i ukształtowanie umiejętności definiowania i stosowania polityki bezpieczeństwa w przedsiębiorstwie

Prerequisites

Sieci Komputerowe

Scope

Bezpieczeństwo informacji. Wprowadzenie. Definicje. Infrastruktura. Modele bezpieczeństwa.

Stan prawny. Ustawa o ochronie informacji niejawnej i akty pokrewne. Ustawa o cyberbezpieczeństwie. Kancelarie tajne. Klauzule tajności. Dostęp do systemu. Kontrola dostępu do systemu. Zarządzanie dostępem użytkowników. Zakres odpowiedzialności użytkowników. Szacowanie i zarządzanie ryzykiem.

Bezpieczeństwo systemów i sieci teleinformatycznych. Typy ataków. Firewalle (IDS i IPS). Metody ochrony fizycznej. Systemy alarmowe. Ochrona przed podsłuchem elektromagnetycznym – norma TEMPEST. Polityka bezpieczeństwa. Rola i zadania Administratora Bezpieczeństwa Informacji.

Bezpieczeństwo przemysłowe.

Kryptografia. Algorytmy symetryczne (DES, 3DES, AES, Twofish, rodzina RCx, Serpent, Mars) i asymetryczne (RSA, DH, ElGamal, EC). Protokoły kryptograficzne. Kryptografia klucza publicznego. Jednokierunkowe funkcje skrótu. Podpis elektroniczny i jego weryfikacja. Certyfikacja urządzeń i użytkowników. Architektura PKI. Inne usługi wykorzystujące kryptografię. Kody korekcyjne i ich zastosowania.

Teaching methods

wykład: wykład konwencjonalny, dyskusja

laboratorium: ćwiczenia laboratoryjne

Learning outcomes and methods of theirs verification

Outcome description	Outcome symbols	Methods of verification	The class form
posiada wiedzę w zakresie problemów podpisu elektronicznego	• K_W05 • K_W14 • K_W15 • K_U15 • K_K01 • K_K02	• activity during the classes • an evaluation test • an observation and evaluation of activities during the classes	• Lecture • Laboratory

Outcome description	Outcome symbols	Methods of verification	The class form
zna strukturę pionu ochrony w jednostce organizacyjnej (przedsiębiorstwie), rozumie zadania pracowników pionu ochrony w stosunku do danych oraz innych pracowników tej jednostki	• K_W05 • K_W14 • K_W15 • K_U15 • K_K03 • K_K04	• an evaluation test	• Lecture
zna cechy charakterystyczne algorytmów i protokołów kryptograficznych oraz jednokierunkowych funkcji skrótu	• K_W05 • K_U15 • K_K02	• activity during the classes • an evaluation test • an observation and evaluation of activities during the classes	• Lecture • Laboratory
rozumie problemy związane ze bezpieczeństwem przemysłowym	• K_W14 • K_W15 • K_U15	• activity during the classes • an evaluation test • an observation and evaluation of activities during the classes	• Lecture • Laboratory
posiada wiedzę o stanie prawnym w zakresie ochrony informacji niejawnej w Polsce	• K_W05 • K_W14 • K_W15	• an evaluation test	• Lecture
potrafi dobrać parametry kryptosystemu realizującego założone funkcje w odniesieniu do ochrony danych	• K_W01 • K_W05 • K_W14 • K_W15 • K_U15	• activity during the classes • an evaluation test • an observation and evaluation of activities during the classes	• Lecture • Laboratory
zna zasady ochrony informacji niejawnej, w szczególności ochrony fizycznej i elektromagnetycznej	• K_W05 • K_W14 • K_W15 • K_U15	• an evaluation test	• Lecture

Assignment conditions

Wykład - warunkiem zaliczenia jest uzyskanie pozytywnych ocen z sprawdzianów wiedzy w formie pisemnej, przeprowadzonych co najmniej raz w semestrze

Laboratorium - warunkiem zaliczenia jest realizacja co najmniej 80% przewidzianych ćwiczeń laboratoryjnych i uzyskanie pozytywnych ocen ze sprawdzianów weryfikujących wiedzę i umiejętności zdobyte podczas ćwiczeń

Składowe oceny końcowej = wykład: 50% + laboratorium: 50%

Recommended reading

1. I. Stankowska, Ustawa o ochronie informacji niejawnych. Komentarz, wyd. LexisNexis, Warszawa 2011.
2. Ustawa z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych, Dz. U. z 2010 r., nr 182, poz. 1228.
3. Wytyczne w sprawie określenia zasad postępowania z materiałami zawierającymi informacje niejawne zał. do Decyzji Nr 362/MON z dnia 28 września 2011 r.
4. W. Stallings, Kryptografia i bezpieczeństwo sieci komputerowych, Tomy 1-2, Helion, 2017
5. Lukatsky A.: Wykrywanie włamań i aktywna ochrona danych, Helion, 2004.

Further reading

1. Russell R. i in. : Hakerzy atakują. Jak przejąć kontrolę nad siecią, Helion, 2004.
2. Potter B., Fleck B.: 802.11. Bezpieczeństwo, Wyd. O'Reilly, 2005.
3. Balinsky A. i in.: Bezpieczeństwo sieci bezprzewodowych, PWN, CISCO Press, 2007.
4. G. Weidman, Bezpieczny system w praktyce. Wyższa szkoła hackingu i testy penetracyjne, Helion, 2015
5. P. Kim, Podręcznik pentestera. Bezpieczeństwo systemów informatycznych, Helion, 2015
6. M. Goodman, Zbrodnie przyszłości. Jak cyberprzestępcy, korporacje i państwa mogą używać technologii przeciwko Tobie, Helion, 2016

Notes

Modified by dr hab. inż. Bartłomiej Sulikowski, prof. UZ (last modification: 06-05-2019 08:45)