Security of IT Systems - course description

General information

Course name	Security of IT Systems
Course ID	11.3-WK-IiEP-BSI-L-S14_pNadGenNI2CA
Faculty	Faculty of Mathematics, Computer Science and Econometrics
Field of study	Informatics and Econometrics
Education profile	academic
Level of studies	First-cycle studies leading to Bachelor's degree
Beginning semester	winter term 2022/2023

Course information

Semester	6
ECTS credits to win	5
Available in specialities	Information Systems
Course type	optional
Teaching language	polish
Author of syllabus	• dr inż. Janusz Jabłoński

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
Laboratory	30	2	-	-	Credit with grade
Lecture	30	2	-	-	Exam

Aim of the course

Zapoznanie studenta z wybranymi modelami technikami i metodami Inżynierii Oprogramowania w realizacji systemów rozproszonych.

Prerequisites

Podstawy projektowania systemów informatycznych oraz protokołów i sieci komputerowych.

Scope

Wykład

1. Prawne i normalizacyjne uwarunkowania ochrony danych. (2 godz.).
2. Ustawa o ochronie danych niejawnych oraz ochronie danych osobowych (2 godz.)
3. Zagrożenia systemów informatycznych: poufność, integralność dostępność. (4 godz.)
4. Modele i klasy bezpieczeństwa dla systemów informatycznych. (2 godz.)
5. Kryptografia i krypto-analiza. (6 godz.)
6. Prawo telekomunikacyjne i ustawa o podpisie cyfrowym. (2 godz.)
7. Modele uwierzytelniania i strategie kontroli dostępu. (2 godz.)
8. Wirusy, trojany, rotkity ... – metody obrony. (2 godz.)
9. Środowiska o podwyższonym bezpieczeństwie i usługi narzędziowe. (2 godz.)
10. Ataki lokalne i sieciowe - systemy wykrywania ataków oraz ochrony. (2 godz.)
11. Definiowanie polityki bezpieczeństwa. (2 godz.)
12. Podpis elektroniczny i infrastruktury klucza publicznego. (2 godz.)

Laboratorium

1. System operacyjny - funkcje w zakresie ochrony danych. (2 godz.)
2. Konfigurowanie kont użytkowników systemu operacyjnego. (2 godz.)
3. Zaawansowane usługi systemu operacyjnego. (2 godz.)
4. Narzędzia kryptograficzne w zabezpieczaniu danych i kont użytkowników . (2 godz.).
5. ACL i VPN - konfigurowanie narzędzi "pracy zdalna" i kontroli zasobów. (4 godz.).
6. Poprawa efektywności szyfrowania i metody krypto-analizy - przykłady (4 godz.)
7. "Przepełnienie bufora" skutki i przeciwdziałanie. (2 godz.)
8. Ochrona przed "SQL Injection", "podszywaniu" i wyłudzanie danych. (2 godz.)
9. Przeciwdziałanie "skanowaniu portów" oraz kontrola aktywności w sieci. (2 godz.)
10. Instalacja i konfiguracja programów Antywirusowych. (2 godz.).
11. Definiowanie polityki bezpieczeństwa. (2 godz.)
12. Instalowanie i użytkowanie certyfikatów - przykłady wykorzystania (2 godz.)
13. Pasywne i aktywne systemów zabezpieczeń sieciowych. (2 godz.)

Teaching methods

Wykład z wykorzystaniem technik prezentacyjnych, ćwiczenia laboratoryjne, prezentacje opracowań studentów, pogadanka.

Learning outcomes and methods of theirs verification

Outcome description	Outcome symbols	Methods of verification	The class form
Student rozumie znaczenie uczciwości intelektualnej w działaniach własnych i innych osób oraz zdaje sobie sprawę z konieczności przestrzegania prawa w zakresie ochrony danych.	• K_K04 • K_K07	• an evaluation test • an ongoing monitoring during classes • carrying out laboratory reports	• Laboratory
Student zna podstawowe uwarunkowania prawne ochrony oraz zagrożenia bezpieczeństwa danych w systemach informatycznych	• K_W02	• an exam - oral, descriptive, test and other	• Lecture
Student potrafi przygotować bezpieczny profil dla użytkownika systemu komputerowego oraz potrafi zabezpieczyć stanowisko komputerowe odpowiednim programem	• K_U33	• a draft • activity during the classes • an evaluation test • carrying out laboratory reports	• Laboratory
Student ma ogólną wiedzę z zakresu metod, technik i narzędzi wykorzystywanych w przeciwdziałaniu zagrożeniom bezpieczeństwa informatycznego i ochrony danych.	• K_W14	• an exam - oral, descriptive, test and other	• Lecture
Student umie dobrać narzędzia dla pracy zdalnej i skonfigurować bezpieczny kanał VPN.	• K_U21	• activity during the classes • carrying out laboratory reports	• Laboratory

Assignment conditions

Ostateczna ocena z przedmiotu uwzględnia ocenę z laboratorium (50%) i ocenę z egzaminu (50%), przy założeniu, że student osiągnął wszystkie zakładane efekty kształcenia w stopniu dostatecznym. Warunkiem zaliczenia przedmiotu jest uzyskanie oceny pozytywnej z wykładu i laboratorium.

Recommended reading

1. J. Pieprzyk, T. Hardjono, J. Seberry, Teoria bezpieczeństwa systemów komputerowych, Helion, Gliwice 2005.
2. Lukatsky, Wykrywanie włamań i aktywna ochrona danych, Helion, Gliwice 2004.
3. Białas, Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, WNT, Warszawa 2006.

Further reading

1. E. Cole, R.L. Krutz, J. Conley, Bezpieczeństwo sieci, Helion, Gliwice 2005.
2. R. Anderson, Inżynieria zabezpieczeń, WNT Warszawa 2005
3. M. Sokół, R. Sokół, Internet. Jak surfować bezpiecznie, Helion Łódz 2005
4. D.E. Denning, Wojna informacyjna i bezpieczeństwo informacji, WNT Warszawa 2002

Notes

Modified by dr Alina Szelecka (last modification: 19-05-2022 21:47)