Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2012/2013

Wydział Fizyki, Matematyki i Informatyki

Kierunek studiów: Informatyka

Profil: Ogólnoakademicki

Forma sudiów: niestacjonarne

Kod kierunku: I

Stopień studiów: II

Specjalności: Informatyka stosowana dla inżynierów

1 Informacje o przedmiocie

Nazwa przedmiotu	Technologie ochrony systemów informatycznych
Nazwa przedmiotu w języku angielskim	
Kod przedmiotu	WFMiI I oIIN D7 12/13
Kategoria przedmiotu	Przedmioty specjalnościowe
Liczba punktów ECTS	5.00
Semestry	3

2 Rodzaj zajęć, liczba godzin w planie studiów

Semestr	Wykład	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Seminarium	Projekt
3	18	0	9	0	0	0

3 Cele przedmiotu

Cel 1 Zapoznanie studentów z podstawowymi zagrożeniami systemów komputerowych.

Cel 2 Zapoznanie studentów z podstawowymi metodami zabezpieczenia systemu operacyjnego komputera i systemu komputerowego

4 Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1 zaliczenie przedmiotów: algebra, matematyka dyskretna

5 Efekty kształcenia

EK1 Wiedza Student wymienia i objaśnia podstawowe zagrożenia dla systemu komputerowego.

EK2 Umiejętności Student potrafi rozpoznać podstawowe zagrożenia dla systemu komputerowego.

EK3 Wiedza Student objaśnia podstawowe metody zabezpieczenia systemu komputerowego.

EK4 Umiejętności Student potrafi stosować wybrane metody zabezpieczenia danych w systemie operacyjnym i w sieci komputerowej

6 Treści programowe

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W1	Wstęp: potrzeba zabezpieczenia systemów komputerowych. Kryptografia i kryptoanaliza. Systemy kryptograficzne symetryczne i asymetryczne.	2
W2	Identyfikacja i uwierzytelnianie użytkownika: system haseł. Przechowywanie haseł, weryfikacja haseł. Ataki na system haseł. Słabe hasła. Weryfikacja haseł. Hasła jednorazowe. System Kerberos.	2
W3	Zabezpieczanie połączeń internetowych: pakiet Secure Shell-korzyści ze stosowania. Schemat nawiązywania połączenia. Pakiety WinSCP i PuTTy dla Windows. Nawiązywanie połączenia za pomocą klucza publicznego w systemie SSH.	2
W4	Zabezpieczanie połączeń internetowych: pakiet Secure Socket Layer. Korzystanie z pakietu. certyfikaty, elementy certyfikatu, instytucje certyfikujące.	2
W5	Wykrywanie włamań do systemów komputerowych. Analiza zachowań użytkowników. Analiza statystyczna i analiza na podstawie reguł.	2
W6	Szkodliwe programy: wirusy komputerowe, robaki, zombie, konie trojańskie i inne. Klasyfikacja, struktura, sposób działania wirusów i robaków.	2
W7	Ochrona przed wirusami i innymi złośliwymi programami: programy antywirusowe, klasyfikacja, metody działania. Systemy immunologiczne.	2
W8	Ściany ogniowe: zasady konstrukcji, funkcje, cele, rodzaje, konfiguracje. Kontrola dostępu do danych. Systemy zaufane.	2
W9	Zastosowania technik kryptograficznych: wybory elektroniczne, cyfrowe pieniądze.	2

Laboratorium		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
L1	Przypomnienie podstawowych pojęć z dziedziny algebry, wykorzystywanych w dalszym procesie kształcenia.	1
L2	Bezpieczeństwo systemu operacyjnego Linux	2
L3	Bezpieczeństwo systemu operacyjnego Windows	2
L4	Wprowadzenie do pakietu OpenSSL.	2
L5	Wykorzystanie pakietu OpenSSL do budowy bezpiecznych aplikacji.	2

7 Narzędzia dydaktyczne

N1 Ćwiczenia laboratoryjne

N2 Dyskusja

N3 Wykłady

N4 Konsultacje

8 Obciążenie pracą studenta

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z nauczycielem akademickim, w tym:	
Godziny wynikające z planu studiów	0
Konsultacje przedmiotowe	13
Egzaminy i zaliczenia w sesji	10
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	50
Opracowanie wyników	0
Przygotowanie raportu, projektu, prezentacji, dyskusji	50
Sumaryczna liczba godzin dla przedmiotu wynikająca z całego nakładu pracy studenta	**123**
Sumaryczna liczba punktów ECTS dla przedmiotu	5.00

9 Sposoby oceny

Ocena formująca

F1 Ćwiczenie praktyczne

F2 Odpowiedź ustna

F3 Sprawozdanie z ćwiczenia laboratoryjnego

Ocena podsumowująca

P1 Średnia ważona ocen formujących

P2 Test

Warunki zaliczenia przedmiotu

W1 Zaliczenie ćwiczeń mogą uzyskać studenci, którzy regularnie uczęszczali na ćwiczenia

W2 Do egzaminu mogą przystąpić studenci, którzy wcześniej uzyskali zaliczenie ćwiczeń laboratoryjnych.

W3 Egzamin ma formę testu lub odpowiedzi ustnej

W4 Ocena końcowa jest średnią z ocen P1-P2.

Kryteria oceny

Efekt kształcenia 1	
Na ocenę 2.0	Student nie zna ogólnych zasad działania szkodliwych programów komputerowych (wirusy i inne) lub zasad wyboru i kontroli haseł.
Na ocenę 3.0	Student zna ogólne zasady działania szkodliwych programów komputerowych (wirusy i inne), zasady wyboru i kontroli haseł.
Na ocenę 3.5	Student zna różne zasady działania szkodliwych programów komputerowych (wirusy i inne), zasady wyboru i kontroli haseł.
Na ocenę 4.0	Student zna i rozumie różne zasady działania szkodliwych programów komputerowych (wirusy i inne), zasady wyboru i kontroli haseł.
Na ocenę 4.5	Student zna i prawidłowo rozumie różne zasady działania szkodliwych programów komputerowych (wirusy i inne), zasady wyboru i kontroli haseł. Potrafi uzupełniać wiadomości uzyskane podczas zajęć informacjami z innych źródeł.
Na ocenę 5.0	Student zna i w pełni prawidłowo rozumie różne zasady działania szkodliwych programów komputerowych (wirusy i inne), zasady wyboru i kontroli haseł. Potrafi uzupełniać wiadomości uzyskane podczas zajęć informacjami z innych źródeł. Potrafi wyciągać logiczne wnioski z posiadanych w tym zakresie informacji.
Efekt kształcenia 2	
Na ocenę 2.0	Student nie potrafi wymienić i opisać podstawowych zagrożeń dla systemu komputerowego i sieci komputerowej.

Na ocenę 3.0	Student potrafi wymienić i opisać podstawowe zagrożenia dla systemu komputerowego i sieci komputerowej.
Na ocenę 3.5	Student potrafi wymienić i opisać różne zagrożenia dla systemu komputerowego i sieci komputerowej.
Na ocenę 4.0	Student potrafi wymienić i prawidłowo opisać różne zagrożenia dla systemu komputerowego i sieci komputerowej.
Na ocenę 4.5	Student potrafi wymienić i prawidłowo opisać różne zagrożenia dla systemu komputerowego i sieci komputerowej. Potrafi uzupełniać wiadomości uzyskane podczas zajęć informacjami z innych źródeł.
Na ocenę 5.0	Student potrafi wymienić i prawidłowo opisać różne zagrożenia dla systemu komputerowego i sieci komputerowej. Potrafi uzupełniać wiadomości uzyskane podczas zajęć informacjami z innych źródeł. Potrafi wskazać zagrożenia dla systemu komputerowego i sieci komputerowej w konkretnych sytuacjach.
Efekt kształcenia 3	
Na ocenę 2.0	Student nie zna podstawowych metod identyfikacji i uwierzytelniania użytkownika, zabezpieczenia połączeń internetowych, sposobów ochrony przed wirusami, metod wykrywania intruzów, zasad działania ścian ogniowych.
Na ocenę 3.0	Student zna podstawowe metody identyfikacji i uwierzytelniania użytkownika, zabezpieczenia połączeń internetowych, sposoby ochrony przed wirusami, metody wykrywania intruzów, zasady działania ścian ogniowych.
Na ocenę 3.5	Student zna różne metody identyfikacji i uwierzytelniania użytkownika, zabezpieczenia połączeń internetowych, sposoby ochrony przed wirusami, metody wykrywania intruzów, zasady działania ścian ogniowych.
Na ocenę 4.0	Student zna i rozumie różne metody identyfikacji i uwierzytelniania użytkownika, zabezpieczenia połączeń internetowych, sposoby ochrony przed wirusami, metody wykrywania intruzów, zasady działania ścian ogniowych.
Na ocenę 4.5	Student zna i prawidłowo rozumie różne metody identyfikacji i uwierzytelniania użytkownika, zabezpieczenia połączeń internetowych, sposoby ochrony przed wirusami, metody wykrywania intruzów, zasady działania ścian ogniowych. Potrafi uzupełniać wiadomości uzyskane podczas zajęć informacjami z innych źródeł.
Na ocenę 5.0	Student zna i i w pełni prawidłowo rozumie różne metody identyfikacji i uwierzytelniania użytkownika, zabezpieczenia połączeń internetowych, sposoby ochrony przed wirusami, metody wykrywania intruzów, zasady działania ścian ogniowych. Potrafi uzupełniać wiadomości uzyskane podczas zajęć informacjami z innych źródeł. Potrafi wyciągać logiczne wnioski z posiadanych w tym zakresie informacji.
Efekt kształcenia 4	
Na ocenę 2.0	Student nie potrafi wykonac poprawnie dwóch z nastepujacych zadan: zastosowac wybrana metode zapewnienia bezpieczenstwa danych w wybranym systemie operacyjnym, zaszyfrowac plik danych szyfrem blokowym DES, wykorzystac podstawowe komendy pakietu OpenSSL w trybie z linii komend w celu budowy centrum certyfikujacego.

Na ocenę 3.0	Student potrafi wykonać poprawnie dwa z następujących zadań: zastosować wybraną metody zapewnienia bezpieczeństwa danych w wybranym systemie operacyjnym, zaszyfrować plik danych szyfrem blokowym DES, wykorzystać podstawowe komendy pakietu OpenSSL w trybie z linii komend w celu budowy centrum certyfikującego.
Na ocenę 3.5	Student potrafi wykonac poprawnie wszystkich nastepujacych zadan: zastosowac wybrana metody zapewnienia bezpieczenstwa danych w systemie operacyjnym, zaszyfrowac plik danych szyfrem blokowym DES, wykorzystac podstawowe komendy pakietu OpenSSL w trybie z linii komend w celu budowy centrum certyfikujacego
Na ocenę 4.0	Student potrafi wykonac poprawnie wszystkie z nastepujacych zadan: zastosowac wybrana metodę zapewnienia bezpieczenstwa danych w systemie operacyjnym, zaszyfrowac plik danych szyfrem blokowym DES, wykorzystac podstawowe komendy pakietu OpenSSL trybie z linii komend w celu budowy centrum certyfikujacego
Na ocenę 4.5	Student potrafi wykonac w pełni prawidłowo wszystkie z nastepujacych zadan: zastosowac wybrana metodę zapewnienia bezpieczenstwa danych w systemie operacyjnym, zaszyfrowac plik danych szyfrem blokowym DES, wykorzystac zaawansowane komendy pakietu OpenSSL trybie z linii komend w celu budowy centrum certyfikujacego, potrafi zaimplementowac aplikacje, wykorzystujaca narzedzia OpenSSL
Na ocenę 5.0	Student potrafi wykonac w pełni prawidłowo wszystkie z nastepujacych zadan: zastosowac wybrane metody zapewnienia bezpieczenstwa danych w systemie operacyjnym Linux i Windows, zaszyfrowac plik danych szyfrem blokowym DES, wykorzystac zaawansowane komendy pakietu OpenSSL trybie z linii komend w celu budowy centrum certyfikujacego, potrafi zaimplementowac aplikacje, wykorzystujaca narzedzia OpenSSL z pełnym zrozumieniem wykorzystanych metod i algorytmów.

10 Macierz realizacji przedmiotu

Efekt kształcenia	Odniesienie danego efektu do szczegółowych efektów zdefiniowanych dla programu	Cele przedmiotu	Treści programowe	Narzędzia dydaktyczne	Sposoby oceny
EK1	I2_W03, I2_W08	Cel 1	W1 W2 W5 W6 L1 L2 L3	N2 N3 N4	F1 F2 F3 P1 P2
EK2	I2_W03, I2_W08, I2_U03, I2_U10	Cel 1	W1 W2 W5 W6 L1 L2 L3	N1 N2 N4	F1 F2 F3 P1 P2

Efekt kształcenia	Odniesienie danego efektu do szczegółowych efektów zdefiniowanych dla programu	Cele przedmiotu	Treści programowe	Narzędzia dydaktyczne	Sposoby oceny
EK3	I2_W03, I2_W08	Cel 2	W1 W3 W4 W7 W8 W9 L1 L4 L5	N2 N3 N4	F1 F2 F3 P1 P2
EK4	I2_U03, I2_U10	Cel 2	W1 W3 W4 W7 W8 W9 L1 L4 L5	N1 N3 N4	F1 F2 F3 P1 P2

11 Wykaz literatury

Literatura podstawowa

[1] M. Kutyłowski, W.B. Strothmann — *Kryptografia. Teoria i praktyka zabezpieczania systemów komputerowych*, Warszawa, 1999, ReadMe

[2] J. Pieprzyk, T. Hardjono, J. Seeberry — *Teoria bezpieczeństwa systemów komputerowych*, Gliwice, 2004, Helion

Literatura uzupełniająca

[1] M. Karpiński, I. P. Kurytnik — *Sieci komputerowe: bezpieczeństwo*, Bielsko - Biała, 2006, Wyd. ATH

[2] B. Schneier — *Kryptografia dla praktyków*, Warszawa, 2002, WNT

12 Informacje o nauczycielach akademickich

Osoba odpowiedzialna za kartę

dr hab. Andrzej Karafiat (kontakt: akaraf@pk.edu.pl)

Osoby prowadzące przedmiot

1 Dr hab Andrzej Karafiat (kontakt: akaraf@pk.edu.pl)

2 Dr Agnieszka Krok (kontakt: agakrok@poczta.fm)

13 Zatwierdzenie karty przedmiotu do realizacji

(miejscowość, data) (odpowiedzialny za przedmiot) (dziekan)

Przyjmuję do realizacji (data i podpisy osób prowadzących przedmiot)

. . . . . .

. . . . . .