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: stacjonarne

Kod kierunku: I

Stopień studiów: II

Specjalności: Informatyka stosowana dla licencjatów

1 Informacje o przedmiocie

Nazwa przedmiotu	Technologie ochrony systemów informatycznych
Nazwa przedmiotu w języku angielskim	
Kod przedmiotu	WFMiI I oIIS 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	30	0	30	0	0	0

3 Cele przedmiotu

Cel 1 Zapoznanie studentów z podstawowymi pojęciami i metodami kryptograficznego zabezpieczania informacji.

Cel 2 Zapoznanie studentów z podstawowymi algorytmami kryptograficznymi

Cel 3 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 objaśnia podstawowe pojęcia z zakresu kryptografii

EK2 Umiejętności Student potrafi zrealizować podstawowe algorytmy kryptograficzne

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. Podział systemów kryptograficznych. Systemy stosowane w przeszłości.	2
W2	Symetryczne systemy kryptograficzne: ogólne zasady, współczesne realizacje: DES, AES, inne systemy. Wzrastające wymagania wobec systemów symetrycznych.	2
W3	Asymetryczne systemy kryptograficzne: ogólne zasady, system RSA.	2
W4	Systemy oparte na logarytmie dyskretnym: Masseya-Omury, El Gamala, wymiany klucza Diffiego-Hellmana.	2
W5	Funkcje skrótu: ogólne zasady budowy funkcji skrótu, kolizje, odporność na kolizje. Ataki na funkcje skrótu, paradoks urodzinowy, wnioski. realizacje funkcji skrótu.	2
W6	Podpis elektroniczny: określenie, cechy, ramy prawne. Schemat podpisu elektronicznego w systemie z kluczem publicznym: RSA, DSA.	2
W7	Schemat podpisu z algorytmem symetrycznym. podpisy z załącznikiem i podpisy z odtwarzaniem wiadomości. Podpisy niezaprzeczalne. Podpisy ślepe.	2
W8	Identyfikacja użytkownika: system haseł. Przechowywanie haseł, weryfikacja haseł. Ataki na system haseł. Słabe hasła. Weryfikacja haseł. Hasła jednorazowe. System Kerberos.	2
W9	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
W10	Zabezpieczanie połączeń internetowych: pakiet Secure Socket Layer. Korzystanie z pakietu. certyfikaty, elementy certyfikatu, instytucje certyfikujące.	2

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W11	Wykrywanie włamań do systemów komputerowych. Analiza zachowań użytkowników. Analiza statystyczna i analiza na podstawie reguł.	2
W12	Szkodliwe programy: wirusy komputerowe, robaki, zombie, konie trojańskie i inne. Klasyfikacja, struktura, sposób działania wirusów i robaków.	2
W13	Ochrona przed wirusami i innymi złośliwymi programami: programy antywirusowe, klasyfikacja, metody działania. Systemy immunologiczne.	2
W14	Ataki typu Denial of Service. Struktura ataku, sieci ataku, metody przeciwdziałania.	2
W15	Ściany ogniowe: zasady konstrukcji, funkcje, cele, rodzaje, konfiguracje. Kontrola dostępu do danych. Systemy zaufane.	2

Laboratorium		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
L1	Przypomnienie podstawowych pojęć z dziedziny algebry, wykorzystywanych w dalszym procesie kształcenia.	2
L2	Bezpieczeństwo systemu operacyjnego Linux.	4
L3	Bezpieczeństwo systemu operacyjnego Windows	4
L4	Realizacja, w dowolnym (obiektowym) języku programowania algorytmu podpisu cyfrowego RSA.	2
L5	Realizacja, w dowolnym (obiektowym) języku programowania protokołu Diffiego-Hellmana.	2
L6	Realizacja, w dowolnym (obiektowym) języku programowania szyfru blokowego DES	4
L7	Wprowadzenie do pakietu OpenSSL.	2
L8	Budowa centrum certyfikującego z wykorzystaniem pakietu OpenSSL w trybie z linii komend.	4
L9	Wykorzystanie pakietu OpenSSL do budowy bezpiecznych aplikacji.	6

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	10
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	70
Opracowanie wyników	0
Przygotowanie raportu, projektu, prezentacji, dyskusji	0
Sumaryczna liczba godzin dla przedmiotu wynikająca z całego nakładu pracy studenta	**90**
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 1. Zaliczenie ćwiczeń mogą uzyskać studenci, którzy regularnie uczęszczali na ćwiczenia

W2 2. Ocena końcowa jest średnią z ocen P1-P2.

Kryteria oceny

Efekt kształcenia 1	
Na ocenę 2.0	Student nie zna ogólnych zasad systemów kryptograficznych symetrycznych i niesymetrycznych lub nie ma podstawowych wiadomości na temat funkcji skrótu i podpisu elektronicznego lub nie potrafi podać po 1 przykładzie dla każdego wymienionego zagadnienia.
Na ocenę 3.0	Student zna ogólne zasady systemów kryptograficznych symetrycznych i niesymetrycznych, ma podstawowe wiadomości na temat funkcji skrótu i podpisu elektronicznego. Potrafi podać po 1 przykładzie dla każdego wymienionego zagadnienia.
Na ocenę 3.5	Student zna ogólne zasady poszczególnych systemów kryptograficznych symetrycznych i niesymetrycznych, ma wystarczające wiadomości na temat funkcji skrótu i podpisu elektronicznego. Potrafi podać przykłady dla każdego wymienionego zagadnienia.
Na ocenę 4.0	Student zna algorytmy różnych systemów kryptograficznych symetrycznych i niesymetrycznych, zna algorytmy funkcji skrótu i podpisu elektronicznego. Potrafi podać różne przykłady dla każdego ze znanych systemów kryptograficznych.
Na ocenę 4.5	Student zna algorytmy różnych systemów kryptograficznych symetrycznych i niesymetrycznych, zna algorytmy funkcji skrótu i podpisu elektronicznego. Potrafi podać różne przykłady dla każdego ze znanych systemów kryptograficznych. Rozumie matematyczne podstawy tych systemów.
Na ocenę 5.0	Student zna szczegółowo algorytmy różnych systemów kryptograficznych symetrycznych i niesymetrycznych, zna szczegółowo algorytmy funkcji skrótu i podpisu elektronicznego. Potrafi podać przykłady dla każdego znanego systemu kryptograficznego. Rozumie matematyczne podstawy tych systemów.
Efekt kształcenia 2	
Na ocenę 2.0	Student nie potrafi wykonac poprawnie trzech z następujących zadań: zrealizować programowo wybrany algorytm podpisu cyfrowego, wybrany protokół uzgadniania kluczy, wybrany szyfry blokowy, wybrany algorytm szyfrowania z kluczem publicznym, wybrany współczesny algorytm szyfrowania z kluczem tajnym, wybrany algorytm funkcji skrótu.
Na ocenę 3.0	Student potrafi wykonać poprawnie trzy z następujących zadań: zrealizować programowo: wybrany algorytm podpisu cyfrowego, wybrany protokół uzgadniania kluczy, wybrany szyfr blokowy, wybrany algorytm szyfrowania z kluczem publicznym, wybrany współczesny algorytm szyfrowania z kluczem tajnym, wybrany algorytm funkcji skrótu.
Na ocenę 3.5	Student potrafi wykonać poprawnie cztery z następujących zadań: zrealizować programowo: wybrany algorytm podpisu cyfrowego, wybrany protokół uzgadniania kluczy, wybrany szyfr blokowy, wybrany algorytm szyfrowania z kluczem publicznym, wybrany współczesny algorytm szyfrowania z kluczem tajnym, wybrany algorytm funkcji skrótu.

Na ocenę 4.0	Student potrafi wykonać poprawnie pięć z następujących zadań: zrealizować programowo: wybrany algorytm podpisu cyfrowego, wybrany protokół uzgadniania kluczy, wybrany szyfr blokowy, wybrany algorytm szyfrowania z kluczem publicznym, wybrany współczesny algorytm szyfrowania z kluczem tajnym, wybrany algorytm funkcji skrótu.
Na ocenę 4.5	Student potrafi wykonać poprawnie wszystkie z następujących zadań: zrealizować programowo: wybrany algorytm podpisu cyfrowego, wybrany protokół uzgadniania kluczy, wybrany szyfr blokowy, wybrany algorytm szyfrowania z kluczem publicznym, wybrany współczesny algorytm szyfrowania z kluczem tajnym, wybrany algorytm funkcji skrótu.
Na ocenę 5.0	Student potrafi wykonać poprawnie wszystkie z następujących zadań: zrealizować programowo: wybrany algorytm podpisu cyfrowego, wybrany protokół uzgadniania kluczy, wybrany szyfr blokowy, wybrany algorytm szyfrowania z kluczem publicznym, wybrany współczesny algorytm szyfrowania z kluczem tajnym, wybrany algorytm funkcji skrótu. Potrafi logicznie uzasadnić wybór zastosowanych metod.
Efekt kształcenia 3	
Na ocenę 2.0	Student nie zna podstawowych zasad identyfikacji użytkownika, zabezpieczenia połączeń internetowych, działania wirusów komputerowych i sposobów ochrony przed nimi, zasady działania ścian ogniowych.
Na ocenę 3.0	Student zna podstawowe zasady identyfikacji użytkownika, zabezpieczenia połączeń internetowych, działanie wirusów komputerowych i sposoby ochrony przed nimi, zasadę działania ścian ogniowych.
Na ocenę 3.5	Student zna różne zasady identyfikacji użytkownika, zabezpieczenia połączeń internetowych, działanie wirusów komputerowych i sposoby ochrony przed nimi, zasadę działania ścian ogniowych.
Na ocenę 4.0	Student zna i rozumie różne zasady identyfikacji użytkownika, zabezpieczenia połączeń internetowych, działanie wirusów komputerowych i sposoby ochrony przed nimi, zasadę działania ścian ogniowych.
Na ocenę 4.5	Student zna i rozumie różne zasady identyfikacji użytkownika, zabezpieczenia połączeń internetowych, działanie wirusów komputerowych i sposoby ochrony przed nimi, zasadę działania ścian ogniowych. Potrafi wyciągać logiczne wnioski z posiadanych w tym zakresie informacji.
Na ocenę 5.0	Student zna i i w pełni rozumie różne zasady identyfikacji użytkownika, zabezpieczenia połączeń internetowych, działanie wirusów komputerowych i sposoby ochrony przed nimi, zasadę działania ścian ogniowych. Potrafi wyciągać logiczne wnioski z posiadanych w tym zakresie informacji. Potrafi uzupełniać wiadomości uzyskane podczas zajęć informacjami pozyskanymi z zewnątrz.
Efekt kształcenia 4	

Na ocenę 2.0	Student nie potrafi wykonac poprawnie trzech z nastepujacych zadan: zastosowac wybrana metode zapewnienia bezpieczenstwa danych w wybranym systemie operacyjnym, zaimplementowac algorytm podpisu cyfrowego RSA, przeprowadzic procedure uzgadniania kluczy Diffiego-Hellmana, zaszyfrowac plik danych szyfrem blokowym DES, wykorzystac podstawowe komendy pakietu OpenSSL trybie z linii komend w celu budowy centrum certyfikujacego
Na ocenę 3.0	Student potrafi wykonać poprawnie trzy z następujących zadań: zastosować wybraną metody zapewnienia bezpieczeństwa danych w wybranym systemie operacyjnym, zaimplementować algorytm podpisu cyfrowego RSA, przeprowadzić procedurę uzgadniania kluczy Diffiego-Hellmana, zaszyfrować plik danych szyfrem blokowym DES, wykorzystać podstawowe komendy pakietu OpenSSL trybie z linii komend w celu budowy centrum certyfikującego
Na ocenę 3.5	Student potrafi wykonac poprawnie cztery z nastepujacych zadan: zastosowac wybrana metody zapewnienia bezpieczenstwa danych w systemie operacyjnym, zaimplementowac algorytm podpisu cyfrowego RSA, przeprowadzic procedure uzgadniania kluczy Diffiego-Hellmana, zaszyfrowac plik danych szyfrem blokowym DES, wykorzystac podstawowe komendy pakietu OpenSSL trybie z linii komend w celu budowy centrum certyfikujacego
Na ocenę 4.0	Student potrafi wykonac poprawnie wszystkie z nastepujacych zadan: zastosowac wybrana metody zapewnienia bezpieczenstwa danych w systemie operacyjnym, zaimplementowac algorytm podpisu cyfrowego RSA, przeprowadzic procedure uzgadniania kluczy Diffiego-Hellmana , 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 poprawnie wszystkie z nastepujacych zadan: zastosowac wybrana metody zapewnienia bezpieczenstwa danych w systemie operacyjnym, zaimplementowac algorytmu podpisu cyfrowego RSA, przeprowadzic procedure uzgadniania kluczy Diffiego-Hellmana , 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 poprawnie wszystkie z nastepujacych zadan: zastosowac wybrane metody zapewnienia bezpieczenstwa danych w systemie operacyjnym Linux i Windows, zaimplementowac algorytmu podpisu cyfrowego RSA, przeprowadzic procedure uzgadniania kluczy Diffiego-Hellmana , 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

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 W3 W4 W5 W6 W7 L1 L4 L5 L6	N2 N3 N4	F1 F2 F3 P1 P2
EK2	I2_U03,I2_U10	Cel 2	W1 W2 W3 W4 W5 W6 W7 L1 L4 L5 L6	N1 N2 N4	F1 F2 F3 P1 P2
EK3	I2_W03,I2_W08	Cel 3	W8 W9 W10 W11 W12 W13 W14 W15 L2 L7 L8 L9	N2 N3 N4	F1 F2 F3 P1 P2
EK4	I2_U03,I2_U10	Cel 3	W8 W9 W10 W11 W12 W13 W14 W15 L2 L3 L7 L8 L9	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)

.....

.....