Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2016/2017

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	Information technology security systems
Kod przedmiotu	WFMiI I oIIN D7 16/17
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 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, aplikacji internetowej, oraz systemów typu Chmurowego

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, ochrony informacji, zabezpieczania aplikacji oraz systemów typu Chmurowego

EK2 Umiejętności Student potrafi zrealizować podstawowe algorytmy kryptograficzne służące ww celom

EK3 Kompetencje społeczne Student potrafi współdziałać w grupie laboratoryjnej w celu wspólnej identyfikacji podstawowych zagrożeń bezpieczeństwa informacji, aplikacji oraz systemów typu Chmurowego

EK4 Umiejętności Student potrafi wskazać i przeanalizować międzynarodowe normy, standardy oraz regulacje dotyczące bezpieczeństwa i ochrony danych oraz systemów IT

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. Międzynarodowe standardy oraz normy dotyczące bezpieczeństwa systemów komputerowych.	1
W2	Symetryczne systemy kryptograficzne: ogólne zasady, współczesne realizacje: DES, AES, inne systemy. Wymagania wobec systemów symetrycznych.	2
W3	Asymetryczne systemy kryptograficzne: ogólne zasady, system RSA.	2
W4	Funkcje skrótu: ogólne zasady budowy funkcji skrótu, kolizje, odporność na kolizje. Ataki na funkcje skrótu, paradoks urodzinowy, wnioski. realizacje funkcji skrótu.	2
W5	Podpis elektroniczny: określenie, cechy, ramy prawne. Schemat podpisu elektronicznego w systemie z kluczem publicznym: RSA, DSA.	3
W6	Zagrożenia bezpieczeństwa oraz zabezpieczania aplikacji webowych	4
W7	Zagrożenia bezpieczeństwa oraz metody zabezpieczania systemów typu Chmurowego	4

Laboratorium		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
L1	Realizacja, w dowolnym (obiektowym) języku programowania algorytmu szyfru doskonałego.	1

Laboratorium		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
L2	Realizacja, w dowolnym (obiektowym) języku programowania algorytmu podpisu cyfrowego RSA.	2
L3	Porównanie wybranych bibliotek kryptograficznych na przykładzie implementacji szyfru symetrycznego, asymetrycznego, funkcji skrótu oraz podpisu cyfrowego.	2
L4	Analiza bezpieczeństwa wybranej aplikacji webowej w kontekście listy zagrożeń OWASP TOP TEN.	2
L5	Analiza bezpieczeństwa systemu chmurowego w kontekście międzynarodowych standardów na przykładzie 2 wybranych systemów.	2

7 Narzędzia dydaktyczne

N1 Wykład

N2 Dyskusja

N3 Ćwiczenia laboratoryjne

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	30
Konsultacje przedmiotowe	10
Egzaminy i zaliczenia w sesji	2
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	20
Opracowanie wyników	10
Przygotowanie raportu, projektu, prezentacji, dyskusji	10
Sumaryczna liczba godzin dla przedmiotu wynikająca z całego nakładu pracy studenta	**82**
Sumaryczna liczba punktów ECTS dla przedmiotu	5.00

9 Sposoby oceny

Ocena formująca

F1 Ćwiczenie praktyczne

F2 Odpowiedz ustna

Ocena podsumowująca

P1 Średnia ważona ocen formujących

P2 Test

Warunki zaliczenia przedmiotu

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

W2 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 podstawowe algorytmy wybranych systemów kryptograficznych symetrycznych i niesymetrycznych. Potrafi podać przykłady dla wybranych systemów kryptograficznych. Student zna metody ochrony informacji, lub zabezpieczania aplikacji lub systemów typu Chmurowego.
Na ocenę 3.5	Student zna podstawowe algorytmy wybranych systemów kryptograficznych symetrycznych i niesymetrycznych, podpisu cyfrowego. Potrafi podać przykłady dla wybranych systemów kryptograficznych. Student zna metody ochrony informacji, lub zabezpieczania aplikacji lub systemów typu Chmurowego.
Na ocenę 4.0	Student zna szczegółowo algorytmy wybranych systemów kryptograficznych symetrycznych i niesymetrycznych, zna podstawy algorytmu funkcji skrótu i podpisu elektronicznego. Potrafi podać przykłady dla wybranych systemów kryptograficznych. Rozumie matematyczne podstawy tych systemów. Student zna metody ochrony informacji, lub zabezpieczania aplikacji lub systemów typu Chmurowego.
Na ocenę 4.5	Student zna szczegółowo algorytmy wybranych systemów kryptograficznych symetrycznych i niesymetrycznych, zna podstawy algorytmu funkcji skrótu i podpisu elektronicznego. Potrafi podać przykłady dla wybranych systemów kryptograficznych. Rozumie matematyczne podstawy tych systemów. Student zna metody ochrony informacji, zabezpieczania aplikacji lub systemów typu Chmurowego.

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. Student zna metody ochrony informacji, zabezpieczania aplikacji oraz systemów typu Chmurowego.
Efekt kształcenia 2	
Na ocenę 2.0	Student nie potrafi wykonać poprawnie trzech z następujących zadań: zrealizować programowo wybrany algorytm szyfru symetrycznego. Student nie potrafi zidentyfikować wybranych zagrożeń bezpieczeństwa aplikacji webowej . Student nie potrafi wymienić głównych zagrożeń pod względem bezpieczeństwa użytkownika wskazany system typu Chmurowego
Na ocenę 3.0	Student potrafi zaimplementować wybrany algorytm szyfru symetrycznego, niesymetrycznego. Student potrafi trafnie zidentyfikować wybrane zagrożenia bezpieczeństwa aplikacji webowej . Student potrafi ocenić pod względem bezpieczeństwa użytkownika wskazany system typu Chmurowego.
Na ocenę 3.5	Student potrafi zaimplementować wybrany algorytm szyfru symetrycznego, niesymetrycznego, funkcje skrótu. Student potrafi zidentyfikować wybrane zagrożenia bezpieczeństwa aplikacji webowej . Student potrafi ocenić pod względem bezpieczeństwa użytkownika wskazany system typu Chmurowego.
Na ocenę 4.0	Student potrafi zaimplementować wybrany algorytm szyfru symetrycznego, niesymetrycznego, funkcji skrótu. Student potrafi posługiwać się jedną wybrana biblioteką kryptograficzną. Student potrafi trafnie zidentyfikować główne zagrożenia bezpieczeństwa aplikacji webowej . Student potrafi krytycznie ocenić pod względem bezpieczeństwa użytkownika wskazany system typu Chmurowego.
Na ocenę 4.5	Student potrafi zaimplementować wybrany algorytm szyfru symetrycznego, niesymetrycznego, funkcji skrótu, oraz podpisu cyfrowego. Student potrafi posługiwać się jedną wybrana biblioteką kryptograficzną. Student potrafi trafnie zidentyfikować główne zagrożenia bezpieczeństwa aplikacji webowej. Student potrafi krytycznie ocenić pod względem bezpieczeństwa użytkownika, danych oraz systemu wskazany system typu Chmurowego.
Na ocenę 5.0	Student potrafi zaimplementować wybrany algorytm szyfru symetrycznego, niesymetrycznego, funkcji skrótu oraz podpisu cyfrowego. Student potrafi posługiwać się dwoma wybranymi bibliotekami kryptograficznymi. Student potrafi trafnie zidentyfikować główne zagrożenia bezpieczeństwa aplikacji webowej oraz podać sposoby podniesienie bezpieczeństwa aplikacji. Student potrafi krytycznie ocenić pod względem bezpieczeństwa użytkownika, danych oraz systemu wskazany system typu Chmurowego.
Efekt kształcenia 3	
Na ocenę 2.0	Student nie potrafi współdziałać w grupie laboratoryjnej. Student nie potrafi wyciągnąć wniosków z dyskusji oraz uwag zgłaszanych przez pozostałych uczestników zajęć.
Na ocenę 3.0	Student potrafi współdziałać w grupie laboratoryjnej w celu wspólnej identyfikacji głównych cech wybranych bibliotek kryptograficznych.

Na ocenę 3.5	Student potrafi współdziałać w grupie laboratoryjnej w celu wspólnej identyfikacji głównych cech wybranych bibliotek kryptograficznych, wspólnej identyfikacji podstawowych zagrożeń bezpieczeństwa informacji.
Na ocenę 4.0	Student potrafi współdziałać w grupie laboratoryjnej w celu wspólnej identyfikacji głównych cech wybranych bibliotek kryptograficznych, wspólnej identyfikacji podstawowych zagrożeń bezpieczeństwa informacji oraz aplikacji internetowej.
Na ocenę 4.5	Student potrafi współdziałać w grupie laboratoryjnej w celu wspólnej identyfikacji głównych cech wybranych bibliotek kryptograficznych, wspólnej identyfikacji podstawowych zagrożeń bezpieczeństwa informacji oraz aplikacji internetowej oraz podstawowych elementów bezpieczeństwa systemów Chmurowych.
Na ocenę 5.0	Student potrafi współdziałać w grupie laboratoryjnej w celu wspólnej identyfikacji głównych cech wybranych bibliotek kryptograficznych, identyfikacji podstawowych zagrożeń bezpieczeństwa informacji, aplikacji oraz systemów typu Chmurowego.
Efekt kształcenia 4	
Na ocenę 2.0	Student nie potrafi wskazać i przeanalizować międzynarodowych normy, standardów oraz regulacji dotyczących bezpieczeństwa i ochrony danych oraz systemów informatycznych
Na ocenę 3.0	Student potrafi wskazać i przeanalizować międzynarodowe normy, standardy oraz regulacje dotyczące bezpieczeństwa i ochrony danych
Na ocenę 4.0	Student potrafi wskazać i przeanalizować międzynarodowe normy, standardy oraz regulacje dotyczące bezpieczeństwa i ochrony danych oraz aplikacji
Na ocenę 5.0	Student potrafi wskazać i przeanalizować międzynarodowe normy, standardy oraz regulacje dotyczące bezpieczeństwa i ochrony danych oraz systemów informatycznych, włącznie z systemami typu Chmury Obliczeniowej

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	Cel 1	W1 W2 W3 L1 L2	N1 N3	F1 F2
EK2	I2_W03 I2_W06	Cel 2	W1 W2 W3 W4 W5	N1 N2 N3	F1 F2

Efekt kształcenia	Odniesienie danego efektu do szczegółowych efektów zdefiniowanych dla programu	Cele przedmiotu	Treści programowe	Narzędzia dydaktyczne	Sposoby oceny
EK3	I2_W03	Cel 1 Cel 2 Cel 3	W6 W7 L3 L4 L5	N1 N2 N3	F1 F2
EK4	I2_W03	Cel 3	W1 W6 W7 L4 L5	N1 N2 N4	F1 F2

11 Wykaz literatury

Literatura podstawowa

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

Literatura uzupełniająca

[1] J. Pieprzyk, T. Hardjono, J. Seeberry — *Teoria bezpieczenstwa systemów komputerowych*, Gliwice, 2017, 2004

Literatura dodatkowa

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

12 Informacje o nauczycielach akademickich

Osoba odpowiedzialna za kartę

dr Agnieszka Jakóbik (kontakt: akrok@pk.edu.pl)

13 Zatwierdzenie karty przedmiotu do realizacji

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