Państwowa Wyższa Szkoła Zawodowa w Nowym Sączu

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2014/2015

Instytut Techniczny

Kierunek studiów: Informatyka

Profil: Ogólnoakademicki

Forma studiów: Stacjonarne

Kod kierunku: 11.3

Stopień studiów: I

Specjalności: Informatyka stosowana

1 Przedmiot

Nazwa przedmiotu	Kryptografia i teoria kodów
Kod przedmiotu	IT 11.3 AIS C11 14/15
Kategoria przedmiotu	Przedmioty specjalnościowe
Liczba punktów ECTS	2
Semestry	6

2 Rodzaj zajęć, liczba godzin w planie studiów

Semestr	wykład	ćwiczenia	laboratorium	projekt	seminarium
6				30	

3 Cele przedmiotu

Cel 1 Zapoznanie studenta z elementami algebraicznej teorii kodowania.

Cel 2 Zdobycie przez studenta wiedzy z zakresu operacji modularnych.

Cel 3 Obeznanie studenta ze strukturami algebraicznymi: pierścienie, ciała i grupy.

Cel 4 Nabycie przez studenta wiedzy o charakterystykach, typach, strukturze i zdolności detekcyjnej i korekcyjnej kodów korekcyjnych.

Cel 5 Zaznajomienie studenta z binarnymi kodami blokowymi liniowymi i cyklicznymi.

Cel 6 Pozyskanie przez studenta wiedzy w zakresie systemów kryptograficznych.

Cel 7 Zapoznanie studenta z kryptografią klucza publicznego.

Cel 8 Uzyskanie przez studenta wiedzy z zakresu technik kryptografii symetrycznej.

4 Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

a Matematyka dyskretna.

b Metody probabilistyczne i statystyka.

c Podstawy programowania.

d Języki i paradygmaty programowania.

5 Efekty kształcenia

EK1 Wiedza: Student opisuje i zaprezentuje elementy algebraicznej teorii kodowania.

EK2 Wiedza: Student powiązuje, wybiera i argumentuje operacje modularne i w ciałach skończonych.

EK3 Wiedza: Student objaśnia struktury algebraiczne: pierścienie, ciała i grupy.

EK4 Wiedza: Student definiuje, wyjaśnia i porównuje charakterystyki, typy, struktury i zdolności detekcyjne i korekcyjne kodów korekcyjnych.

EK5 Wiedza: Student uogólnia, używa i porównuje binarne kody blokowe liniowe i cykliczne.

EK6 Wiedza: Student objaśnia działanie systemów kryptograficznych.

EK7 Wiedza: Student powie, zaklasyfikuje, interpretuje i uzasadnia kryptografię klucza publicznego.

EK8 Wiedza: Student rozpoznaje, kategoryzuje i ocenia techniki kryptografii symetrycznej.

6 Treści programowe

PROJEKT

Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
P1	Projekt systemu kryptograficznego klucza publicznego.	8
P2	Projekt systemu kryptograficznego na podstawie algorytmów symetrycznych.	8
P3	Projekt systemu bezpieczeństwa IT w opraciu o metody kryptograficzne.	8
P4	Projekt uwzględniający: 1. Elementy algebraicznej teorii kodowania. Arytmetykę modularna. 2. Struktury algebraiczne: pierścienie, ciała i grupy. 3. Charakterystykę, typy, strukturę oraz zdolność detekcyjna i korekcyjna kodów korekcyjnych, metody kodowego zabezpieczenia przed błędami w transmisji. 4. Binarne kody blokowe liniowe i cykliczne, kody Hamminga, generację kodów, realizację techniczną. Kody uwierzytelniania.	6
	Razem	**30**

7 Metody dydaktyczne

M1 Prezentacje multimedialne

M2 Ćwiczenia projektowe

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	1
Egzaminy i zaliczenia w sesji	0
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	7
Opracowanie wyników	0
Przygotowanie raportu, projektu, prezentacji, dyskusji	12
Sumaryczna liczba godzin dla przedmiotu wynikająca z całego nakładu pracy studenta	**50**
Sumaryczna liczba punktów ECTS dla przedmiotu	2

9 Sposoby oceny

Po zakończeniu wykładu przeprowadza się dyskusja kierowana na omawiany temat. Prowadzący ocenia odpowiedzi udzielone przez studentów na postawione pytania.

Ocena formująca

F1 Odpowiedź ustna

F2 Projekt indywidualny

F3 Projekt zespołowy

Kryteria oceny

Efekt kształcenia 1		Miejsce weryfikacji	Opis weryfikacji EK 1
Na ocenę 3	Student nazywa i opisuje podstawowe elementy algebraicznej teorii kodowania, ale z błędami.	wykład	Ocena z aktywności na zajęciach, odpowiedzi ustnych i referatu.
Na ocenę 4	Student zna motywacje badań nad algebraiczną teorią kodowania i potrafi poprawnie wymienić oraz krótko scharakteryzować podstawowe elementy algebraicznej teorii kodowania.		
Na ocenę 5	Student doskonale opisuje oraz ze znawstwem i bezbłędnie prezentuje wszystkie zawarte na wykładzie elementy algebraicznej teorii kodowania.		
Efekt kształcenia 2		Miejsce weryfikacji	Opis weryfikacji EK 2
Na ocenę 3	Student nazywa i powiązuje wybrane operacje modularne i w ciałach skończonych, ale z błędami.	wykład	Ocena z aktywności na zajęciach, odpowiedzi ustnych i referatu.

Na ocenę 4	Student powiązuje, wybiera i argumentuje podstawowe operacje modularne i w ciałach skończonych, z drobnymi nieścisłościami.		
Na ocenę 5	Student objaśnia ze znawstwem operacje modularne i w ciałach skończonych, podając i charakteryzując przykłady.		
Efekt kształcenia 3		Miejsce weryfikacji	Opis weryfikacji EK 3
Na ocenę 3	Student definiuje pojęcia struktur algebraicznych: pierścieni, ciał i grup, ale z błędami.	wykład	Ocena z aktywności na zajęciach, odpowiedzi ustnych i referatu.
Na ocenę 4	Student prawidłowo objaśnia struktury algebraiczne: pierścienie, ciała i grupy.		
Na ocenę 5	Student doskonale objaśnia struktury algebraiczne, posługując się definicjami pierścieni, ciał i grup oraz potrafi wskazać i scharakteryzować przykłady.		
Efekt kształcenia 4		Miejsce weryfikacji	Opis weryfikacji EK 4
Na ocenę 3	Student definiuje i wyjaśnia wybrane charakterystyki, typy, struktury i zdolności detekcyjne i korekcyjne kodów korekcyjnych.	wykład	Ocena z aktywności na zajęciach, odpowiedzi ustnych i referatu.
Na ocenę 4	Student definiuje, wyjaśnia i porównuje podstawowe charakterystyki, typy, struktury i zdolności detekcyjne i korekcyjne kodów korekcyjnych, z drobnymi nieścisłościami.		
Na ocenę 5	Student doskonale definiuje, wyjaśnia i porównuje podstawowe charakterystyki, typy, struktury i zdolności detekcyjne i korekcyjne kodów korekcyjnych. Podaje i charakteryzuje przykłady.		
Efekt kształcenia 5		Miejsce weryfikacji	Opis weryfikacji EK 5
Na ocenę 3	Student uogólnia i porównuje binarne kody blokowe liniowe i cykliczne, ale z błędami.	wykład	Ocena z aktywności na zajęciach, odpowiedzi ustnych i referatu.
Na ocenę 4	Student uogólnia i porównuje binarne kody blokowe liniowe i cykliczne, ale z błędami, z drobnymi nieścisłościami.		
Na ocenę 5	Student doskonale uogólnia i porównuje ze znawstwem binarne kody blokowe liniowe i cykliczne oraz potrafi ich użyć.		
Efekt kształcenia 6		Miejsce weryfikacji	Opis weryfikacji EK 6
Na ocenę 3	Student definiuje pojęcie systemu kryptograficznego, ale z błędami. Wymienia tylko niektóre elementy systemu kryptograficznego.	wykład	Ocena z aktywności na zajęciach, odpowiedzi ustnych i referatu.
Na ocenę 4	Student prawidłowo definiuje pojęcie systemu kryptograficznego i objaśnia poprawnie jego działanie.		

Na ocenę 5	Student definiuje ze znawstwem pojęcie systemu kryptograficznego i doskonale objaśnia jego działanie, posługując się pojęciami technicznymi, oraz potrafi wskazać zastosowanie systemu kryptograficznego.		
Efekt kształcenia 7		Miejsce weryfikacji	Opis weryfikacji EK 7
Na ocenę 3	Student podaje definicję i określa podstawowe cechy kryptografii klucza publicznego, ale z błędami.	wykład	Ocena z aktywności na zajęciach, odpowiedzi ustnych i referatu.
Na ocenę 4	Student zna, klasyfikuje, interpretuje i uzasadnia kryptografię klucza publicznego, z drobnymi nieścisłościami.		
Na ocenę 5	Student powie ze znawstwem o kryptografii klucza publicznego, podaje jej klasyfikację, doskonale uzasadniając i interpretując jej zastosowanie.		
Efekt kształcenia 8		Miejsce weryfikacji	Opis weryfikacji EK 8
Na ocenę 3	Student nazywa i rozpoznaje techniki kryptografii symetrycznej, ale z błędami.	wykład	Ocena z aktywności na zajęciach, odpowiedzi ustnych i referatu.
Na ocenę 4	Student rozpoznaje, kategoryzuje i ocenia techniki kryptografii symetrycznej, z drobnymi nieścisłościami.		
Na ocenę 5	Student doskonale rozpoznaje, kategoryzuje i ocenia techniki kryptografii symetrycznej. Podaje przykłady.		

Ocena do indeksu (ocena podsumowująca)

Średnia ważona ocen cząstkowych uzyskanych za poszczególne efekty kształcenia.

Warunki zaliczenia przedmiotu

a Zaliczenie na podstawie aktywnego udziału w wykładach i obecności, oraz wyników oceny referatu.

10 Macierz realizacji przedmiotu

Efekty kształcenia dla przedmiotu	Odniesienie do efektów kierunkowych	Cele przedmiotu	Treści programowe	Metody dydaktyczne
EK1	INF_W01	Cel1	P1, P2, P3, P4	M1, M2
EK2	INF_W16, INF_W01	Cel2	P1, P2, P3, P4	M1, M2
EK3	INF_W16, INF_W01	Cel3	P1, P2, P3, P4	M1, M2
EK4	INF_W01	Cel4	P1, P2, P3, P4	M1, M2
EK5	INF_W01	Cel5	P1, P2, P3, P4	M1, M2
EK6	INF_W16	Cel6	P1, P2, P3, P4	M1, M2

Efekty kształcenia dla przedmiotu	Odniesienie do efektów kierunkowych	Cele przedmiotu	Treści programowe	Metody dydaktyczne
EK7	INF_W16	Cel7	P1, P2, P3, P4	M1, M2
EK8	INF_W16	Cel8	P1, P2, P3, P4	M1, M2

11 Wykaz literatury

Literatura podstawowa:

[1] Foryś W., Foryś M. — *Teoria języków formalnych i automatów*, Warszawa, 2005, AOW EXIT

[2] Karbowski M. — *Podstawy kryptografii. Wydanie II*, Gliwice, 2007, HELION

[3] Karpiński M. — *Bezpieczeństwo informacji*, Warszawa, 2012, PAK

[4] Mochnacki W. — *Kody korekcyjne i kryptografia*, Wrocław, 2000, Oficyna Wydawnicza

[5] Stinson D.R. — *Kryptografia w teorii i w praktyce*, Warszawa, 2004, WNT

Literatura uzupełniająca:

[1] Blake I., Seroussi G., Smart N. — *Krzywe eliptyczne w kryptografii*, Warszawa, 2004, WNT

[2] Bauer F. L. — *Sekrety kryptografii. Metody i zasady kryptografii*, Gliwice, 2003, HELION

[3] Koblitz N. — *Wykład z teorii liczb i kryptografii*, Warszawa, 2006, WNT

[4] Kościelny C., Kurkowski M., Srebrny M. — *Kryptografia - teoretyczne podstawy i praktyczne*, Warszawa, 2009, Polsko-Japońska Wyższa Szkoła Technik Komputerowych

[5] Welschenbach M. — *Kryptografia w C i C++*, Warszawa, 2002, MIKOM

[6] Karpiński M., Kurytnik I.P. — *Sieci komputerowe: Bezpieczeństwo. Część 1 Metody i systemy kryptograficzne*, Bielsko-Biała, 2006, ATH

12 Informacje o nauczycielach akademickich

Osoba odpowiedzialna za kartę

prof. dr hab. inż. Oleksandr Petrov (kontakt: asp1951@gmail.com)

Osoby prowadzące przedmiot

prof. dr hab. inż. Mikołaj Karpiński (kontakt: mkarpinski@ath.bielsko.pl)

dr inż. Ihor Pazdriy (kontakt: irpazdriy@gmail.com)

mgr Grzegorz Litawa (kontakt: glitawa@poczta.onet.pl)

13 Zatwierdzenie karty przedmiotu do realizacji

(miejscowość, data) (odpowiedzialny za przedmiot) (kierownik zakładu) (dyrektor instytutu)

Przyjmuję do realizacji (data i podpisy osób prowadzących przedmiot)

.....

.....

.....

