Państwowa Wyższa Szkoła Zawodowa w Nowym Sączu

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2013/2014

Instytut Techniczny

Kierunek studiów: Informatyka

Profil: Ogólnoakademicki

Forma studiów: Stacjonarne

Kod kierunku: 11.3

Stopień studiów: I

Specjalności: Informatyka stosowana

1 Przedmiot

Nazwa przedmiotu	Bezpieczeństwo technologii informatycznych
Kod przedmiotu	IT 11.3 AIS C9 13/14
Kategoria przedmiotu	Przedmioty specjalnościowe
Liczba punktów ECTS	3
Semestry	6

2 Rodzaj zajęć, liczba godzin w planie studiów

Semestr	wykład	ćwiczenia	laboratorium	projekt	seminarium
6	15			30	

3 Cele przedmiotu

Cel 1 Zapoznanie studenta z podstawami zabezpieczenia technologii informatycznych i sieciowymi protokółami zabezpieczającymi.

Cel 2 Nabycie przez studenta wiedzy o metodach kryptoanalitycznych.

Cel 3 Wykształcenie umiejętności określenia przydatności algorytmów kryptograficznych z kluczem publicznym i symetrycznych, oraz wybierania i stosowania właściwych trybów działań algorytmów symetrycznych do rozwiązywania prostych zadań bezpieczeństwa technologii informatycznych.

Cel 4 Wykształcenie umiejętności oceny przydatności i sposobu działania, istniejących rozwiązań zabezpieczenia dostępu do informacji, w tym przy pomocy kart elektronicznych i metod biometrycznych.

Cel 5 Wykształcenie umiejętności projektowania prostych układów i aplikacji w zakresie systemów kryptograficznych oraz ich konfigurowania i administrowania.

4 Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

a Matematyka dyskretna.

b Metody probabilistyczne i statystyka.

c Podstawy elektroniki i miernictwa.

d Języki i paradygmaty programowania.

e Technologia sieciowa.

5 Efekty kształcenia

EK1 Wiedza: Student zna i opisuje podstawy zabezpieczenia technologii informatycznych i sieciowe protokóły zabezpieczające.

EK2 Wiedza: Student objaśnia metody kryptoanalityczne.

EK3 Umiejętności: Student potrafi określić przydatność i użyć algorytmy kryptograficzne z kluczem publicznym i symetryczne, oraz dobrać właściwy tryb działań algorytmów symetrycznych do rozwiązywania prostych zadań bezpieczeństwa technologii informatycznych.

EK4 Umiejętności: Student ocenia przydatność i sposób działania, istniejące rozwiązania zabezpieczenia dostępu do informacji, w tym przy pomocy kart elektronicznych i metod biometrycznych.

EK5 Kompetencje społeczne: Student potrafi określić cele ekonomiczne i podejmować nowe wyzwania projektowe i biznesowe w zakresie inżynierii bezpieczeństwa technologii i systemów informatycznych z uwzględnieniem algorytmów kryptograficznych.

6 Treści programowe

wykład

Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W1	Podstawy bezpieczeństwa technologii informatycznych. Kryptograficzne systemy zabezpieczenia technologii informatycznych.	2
W2	Algorytm RSA oraz inne algorytmy z kluczem publicznym. Sposoby generowania i zastosowania sekwencji pseudolosowych.	2
W3	Kryptograficzne algorytmy symetryczne DES, TDES, Twofish, Blowfish, CAST, GOST, IDEA, RC5, AES.	2
W4	Tryby działań algorytmów symetrycznych.	1
W5	Administracja kluczami i protokoły uzgadniania kluczy. Sieciowe protokóły zabezpieczające.	2
W6	Zabezpieczenia dostępu do informacji. Karty elektroniczne. Systemy steganograficzne.	2
W7	Zabezpieczające metody biometryczne. Poziomy bezpieczeństwa systemów kryptograficznych.	2
W8	Techniki i metody kryptoanalityczne.	2
	Razem	**15**

PROJEKT

Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
P1	Zarządzanie i konfigurowanie dostępu lokalnego do systemu Windows, konfigurowanie mechanizmów podnoszących bezpieczeństwo systemu.	2
P2	Zarządzanie i konfigurowanie dostępu lokalnego do systemu Linux, konfigurowanie mechanizmów podnoszących bezpieczeństwo systemu.	2
P3	Metody zarządzania bezpieczeństwem serwerowych systemów operacyjnych Linux.	2
P4	Metody zarządzania bezpieczeństwem serwerowych systemów operacyjnych Windows.	2
P5	Stosowanie metod kryptograficznych do ochrony przesyłanych informacji w warstwie aplikacji.	2
P6	Stosowanie bezpiecznych protokołów sieciowych. Tworzenie sieci VPN.	2
P7	Budowa i konfiguracja zapory sieciowej (firewall).	2
P8	Integracja mechanizmów kryptograficznych z usługami pocztowymi.	2
P9	Metody wykrywania intruzów w sieciach komputerowych.	4
P10	Budowa i konfiguracja zabezpieczeń usług aplikacyjnych (np. www).	2
P11	Testy penetracyjne - techniki skanowania, sniffing, spoofing, ataki odmowy usługi (Denial of Service).	4
P12	Ograniczenie środowiska wykonywania aplikacji, powłoki środowisk serwerowych, delegacja uprawnień administracyjnych.	2
P13	Procedury tworzenia polityki bezpieczeństwa.	2
	Razem	**30**

7 Metody dydaktyczne

M1 Wykłady

M2 Prezentacje multimedialne

M3 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	45
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	21
Opracowanie wyników	0
Przygotowanie raportu, projektu, prezentacji, dyskusji	8
Sumaryczna liczba godzin dla przedmiotu wynikająca z całego nakładu pracy studenta	**75**
Sumaryczna liczba punktów ECTS dla przedmiotu	3

9 Sposoby oceny

Ocena formująca

F1 Odpowiedź ustna

F2 Aktywność na zajęciach

F3 Projekt indywidualny

F4 Projekt zespołowy

Kryteria oceny

Efekt kształcenia 1		Miejsce weryfikacji	Opis weryfikacji EK 1
Na ocenę 3	Student nazywa i opisuje podstawy zabezpieczenia technologii informatycznych i sieciowe protokóły zabezpieczające, ale z błędami.	wykład, projekt	Ocena z odpowiedzi ustnych, aktywności na zajęciach i ćwiczeń projektowych.
Na ocenę 4	Student zna motywacje badań nad zabezpieczeniem technologii informatycznych, interpretuje sieciowe protokóły zabezpieczające, z drobnymi nieścisłościami.		
Na ocenę 5	Student ze znawstwem opisuje podstawy zabezpieczenia technologii informatycznych i bezbłędnie prezentuje sieciowe protokóły zabezpieczające.		
Efekt kształcenia 2		Miejsce weryfikacji	Opis weryfikacji EK 2
Na ocenę 3	Student nazywa i rozróżnia metody kryptoanalityczne, ale nie potrafi objaśnić ich sedna.	wykład, projekt	Ocena z odpowiedzi ustnych, aktywności na zajęciach i ćwiczeń projektowych.
Na ocenę 4	Student rozpoznaje, kategoryzuje i ocenia metody kryptoanalityczne, z drobnymi nieścisłościami.		
Na ocenę 5	Student ze znawstwem rozpoznaje, kategoryzuje i ocenia metody kryptoanalityczne. Podaje przykłady.		
Efekt kształcenia 3		Miejsce weryfikacji	Opis weryfikacji EK 3
Na ocenę 3	Student, popełniając błędy, określa przydatność i używa algorytmy kryptograficzne z kluczem publicznym i symetryczne, oraz dobiera właściwy tryb działań algorytmów symetrycznych do rozwiązywania prostych zadań bezpieczeństwa technologii informatycznych.	projekt	Ocena z ćwiczeń projektowych.
Na ocenę 4	Student określa przydatność i używa algorytmy kryptograficzne z kluczem publicznym i symetryczne, oraz dobiera właściwy tryb działań algorytmów symetrycznych do rozwiązywania prostych zadań bezpieczeństwa technologii informatycznych, ale z drobnymi nieścisłościami.		

Na ocenę 5	Student prawidłowo określa przydatność i używa algorytmy kryptograficzne z kluczem publicznym i symetryczne, oraz bezbłędnie dobiera właściwy tryb działań algorytmów symetrycznych do rozwiązywania prostych zadań bezpieczeństwa technologii informatycznych.		
Efekt kształcenia 4		Miejsce weryfikacji	Opis weryfikacji EK 4
Na ocenę 3	Student , popełniając błędy, jest w stanie ocenić przydatność i sposób działania, istniejące rozwiązania zabezpieczenia dostępu do informacji, w tym przy pomocy kart elektronicznych i metod biometrycznych.	projekt	Ocena z ćwiczeń projektowych.
Na ocenę 4	Student ocenia przydatność i sposób działania, istniejące rozwiązania zabezpieczenia dostępu do informacji, w tym przy pomocy kart elektronicznych i metod biometrycznych, ale z drobnymi nieścisłościami.		
Na ocenę 5	Student ocenia ze znawstwem przydatność i sposób działania, istniejące rozwiązania zabezpieczenia dostępu do informacji, w tym przy pomocy kart elektronicznych i metod biometrycznych.		
Efekt kształcenia 5		Miejsce weryfikacji	Opis weryfikacji EK 5
Na ocenę 3	Student potrafi z trudem i cząstkowo określić cele ekonomiczne i podejmować nowe wyzwania projektowe i biznesowe w zakresie inżynierii bezpieczeństwa technologii i systemów informatycznych z uwzględnieniem algorytmów kryptograficznych.	projekt	Ocena z ćwiczeń projektowych.
Na ocenę 4	Student potrafi niektóre określić cele ekonomiczne i podejmować nowe wyzwania projektowe i biznesowe w zakresie inżynierii bezpieczeństwa technologii i systemów informatycznych z uwzględnieniem algorytmów kryptograficznych.		
Na ocenę 5	Student potrafi w pełni określić cele ekonomiczne i podejmować nowe wyzwania projektowe i biznesowe w zakresie inżynierii bezpieczeństwa technologii i systemów informatycznych z uwzględnieniem algorytmów kryptograficznych.		

Ocena do indeksu (ocena podsumowująca)

Średnia ważona ocen cząstkowych uzyskanych za poszczególne efekty kształcenia.

Warunki zaliczenia przedmiotu

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

10 Macierz realizacji przedmiotu

Efekty kształcenia dla przedmiotu	Odniesienie do efektów kierunkowych	Cele przedmiotu	Treści programowe	Metody dydaktyczne
EK1	INF_W16	Cel1	W1, W5, P1, P2, P6, P13	M1, M2, M3
EK2	INF_W16	Cel2	W8, P11	M1, M2, M3
EK3	INF_UB06	Cel3	W2, W3, W4, P5, P8	M1, M2, M3
EK4	INF_UB01	Cel4	W6, W7, P3, P4, P7, P9, P10, P12	M1, M2, M3
EK5	INF_K06	Cel5	W1, W5, W6, W7, P5, P6, P7, P13	M1, M2, M3

11 Wykaz literatury

Literatura podstawowa:

[1] **Grzywak A.** — *Bezpieczeństwo systemów komputerowych*, Gliwice, 2000, Pracownia Komputerowa Jacka Skalmierskiego

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

[3] **Majwald E.** — *Bezpieczeństwo w sieci kurs podstawowy*, Kraków, 2001, Edition

[4] **Schneider B.** — *Kryptografia dla praktyków. Wyd. 2 zm. i rozsz.*, Warszawa, 2002, WNT

[5] **Strebe B.** — *Bezpieczeństwo sieci*, Warszawa, 2005, MIKOM

Literatura uzupełniająca:

[1] **Wobst R.** — *Budowa i łamanie zabezpieczeń*, Warszawa, 2002, READ ME

[2] **x** — *Bezpieczeństwo systemów komputerowych*, Warszawa, 2012, http://wazniak.mimuw.edu.pl/index.php?title=Bezpiecze%C

[3] **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. Mikołaj Karpiński (kontakt: mkarpinski@ath.bielsko.pl)

Osoby prowadzące przedmiot

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

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)

.....

.....

