

Program przedmiotu

- Nazwa przedmiotu / moduł przedmiotowy: **Bezpieczeństwo systemów informatycznych**
- Język wykładowy: **Polski**
- Umiejscowienie przedmiotu w planach studiów:
 - Obszar lub obszary studiów: **Informatyka stosowana, Programowanie i technologie WWW**
 - Poziom studiów: **studia I stopnia**
 - Kierunek lub kierunki (realizacja wzorca efektów): **Informatyka**
- Nadzór nad realizacją przedmiotu:
 - Instytut/Inna jednostka: **Instytut Informatyki i Mechatroniki**
 - Osoba odpowiedzialna za przedmiot: **Kashuba Svetlana, dr inż.**
 - Osoby współpracujące przy opracowaniu programu przedmiotu:
- Liczba godzin i formy zajęć dydaktycznych dla poszczególnych systemów studiów oraz rygor zaliczenia

Zajęcia dydaktyczne z udziałem prowadzącego																					
Forma studiów	Forma zajęć	Zajęcia dydaktyczne z udziałem prowadzącego																		Razem	
		Wykład	PWS	ECTS	Zajęcia laboratoryjne	PWS	ECTS	...	PWS	ECTS	...	PWS	ECTS	...	PWS	ECTS	...	PWS	ECTS		
Stacjonarne		13	25	1,5	24	26	2														3,5
Niestacjonarne		10	28		16	34															
Rygor zaliczenia		...	egzamin			zaliczenie na ocenę															

- Nakład pracy studenta – bilans punktów ECTS
1 punkt ECTS odpowiada 25-30 godzinom pracy studenta potrzebnej do osiągnięcia zakładanych efektów uczenia się z uwzględnieniem pracy własnej studenta

Aktywność (należy podać prace właściwe dla przedmiotu)	Godzinowe obciążenie studenta (stacjonarne/niestacjonarne) [h]
Udział w wykładach	13/10
Udział w laboratorium	24/16
Samodzielne studiowanie tematyki przedmiotu	6/6
Przygotowanie do egzaminu	17/20
Przygotowanie się do zajęć laboratoryjnych	26/34
Udział w egzaminie /zaliczeniu	2/2
Sumaryczne obciążenie pracą studenta (NPS)	88/88
Punkty ECTS	3,5
* Obciążenie studenta związane z zajęciami praktycznymi	50/50
Obciążenie studenta na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich	37/26

- Uwagi realizacyjne: rekomendowana długość trwania (semestry), rekomendowane wymagania wstępne, relacje pomiędzy formami zajęć:

Nie ma

Rekomendowana długość trwania wynika z planu studiów

- Szczegółowe efekty uczenia się – wiedza, umiejętności i kompetencje społeczne

Szczegółowe efekty uczenia się dla przedmiotu		Forma zajęć	Metody kształcenia	Metody weryfikowania (sprawdzania, oceniania) efektów uczenia się
Symbol efektu	Opis efektu			
Wiedza				
K_W04	Zna i rozumie rolę zasad bezpieczeństwa systemów komputerowych, Ma fundamentalną wiedzę dotyczącą bezpieczeństwa siec. Zna i rozumie zasady działania zapór sieciowych oraz systemów wykrywania zagrożeń, Zna, potrafi rozpoznawać i sklasyfikować podstawowe zagrożenia bezpieczeństwa danych. Zna i rozumie podstawowe metody i usługi ochrony danych.	Wykład Zajęcia laboratoryjne	Metody podające, metody poszukujące	Egzamin pisemny, ocena wykonania ćwiczeń laboratoryjnych.

Program przedmiotu

K_W09	Zna i rozumie zasady i techniki tworzenia zabezpieczonych systemów informatycznych i wie jak klasyfikować główne czynniki bezpieczeństwa informacji. Wie jak klasyfikować różne kategorie ataków, biorąc pod uwagę ich definicje i zasady ich realizacji oraz mechanizm ataku. Potrafi podać przykładowe współczesne algorytmy kryptograficzne.			
Umiejętności				
K_U03	Umie zidentyfikować podstawowe zagrożenia dla bezpieczeństwa aplikacji internetowych. Potrafi poprawnie zabezpieczyć systemy MS Windows oraz Unix na podstawie konfiguracji systemu operacyjnego i systemu zarządzania użytkownikami, poszukiwanie intruzów do tych systemów operacyjnych.	Zajęcia laboratoryjne	Metody podające, metody poszukujące	Egzamin pisemny, ocena wykonania ćwiczeń laboratoryjnych.
K_U04	Potrafi zbudować wirtualną sieć prywatną (VPN) w celu ochrony danych cyfrowych			
K_U16	Potrafi dobrać odpowiednią metodę ochrony w celu zapewnienia bezpieczeństwa systemu. Potrafi wraz z zespołem zaprojektować, a następnie stworzyć politykę bezpieczeństwa informacji, zasad metodologii jej rozwoju, tworzenia, wdrażania i skuteczność wykorzystania			
Kompetencje społeczne				

9. Zasady/kryteria oceniania dla każdej formy kształcenia i poszczególnych ocen

Punktacja:

0% - 50%	ndst	81% - 90%	db
51% - 70%	dst	91% - 93%	db+
71% - 80%	dst+	94% - 100%	bdb

Laboratorium:

Aktywność	Oceny	Obliczenia	Do końcowej
Realizacja zadań na zajęciach	bdb (5)	5*90%	4,5
Obecność	na 80% zajęć	5*10%	0,5
Wynik końcowy			5

10. Treści kształcenia wraz z formą zajęć, na której są realizowane

1. Wprowadzenie. (Wykład)
2. Narzędzia kryptograficzne. (Wykład, Laboratorium)
3. Uwierzytelnianie użytkownika. (Wykład, Laboratorium)
4. Kontrolowanie dostępu. (Wykład, Laboratorium)
5. Bezpieczeństwo baz i centrów danych. (Wykład, Laboratorium)
6. Malware — szkodliwe oprogramowanie. (Wykład, Laboratorium)
7. Ataki polegające na odmowie świadczenia usług. (Wykład, Laboratorium)
8. Wykrywanie włamań. (Wykład, Laboratorium)
9. Zapory sieciowe i systemy zapobiegania włamaniom. (Wykład, Laboratorium)
10. Przepętnienie bufora. (Wykład, Laboratorium)

Program przedmiotu

11. Bezpieczeństwo oprogramowania. (Wykład, Laboratorium)
12. Bezpieczeństwo systemów operacyjnych. (Wykład, Laboratorium)
13. Bezpieczeństwo chmur obliczeniowych. (Wykład)
14. Programowe i sprzętowe zabezpieczenia urządzeń w systemach IOT, IIOT i IOMT. (Wykład, Laboratorium)
15. Zagadnienie redundancji w systemach informatycznych. (Wykład)
16. Zabezpieczenia w systemach informatycznych w świetle przepisów prawa krajowego i międzynarodowego. (Wykład)

11. Wymagane środki dydaktyczne

Wykład – projektor multimedialny
Laboratorium – laboratorium specjalistyczne

12. Literatura przedmiotu:

a. Literatura podstawowa:

- Marian Molski, Małgorzata Łacheta, Bezpieczeństwo i audyt systemów informatycznych, Wydawnictwo uczelniane Wyższej
- Szkoły Gospodarki w Bydgoszczy, Bydgoszcz 2009, WSG, 254 s.
- J. Stokłosa, T. Bliski, T. Pankowski, Bezpieczeństwo danych w systemach informatycznych. PWN, 2001, 282 s/
- Jacek Ross. Bezpieczne programowanie. Aplikacje hakeroodporne. 2009.– 313 s.

a. Literatura uzupełniająca:

- W. R. Cheswick. Firewallle i bezpieczeństwo w sieci. Helion, 2003, 252 s
- Schetina E., Green K., Carlson J. Bezpieczeństwo w sieci. Helion 2002 – 440 s.

b. Netografia:

13. Dostępne materiały dydaktyczne z podziałem na formy zajęć (autorskie zestawienia materiałów dydaktycznych, materiały e-learningowe, itp.)

14. Osoby realizujące poszczególne formy kształcenia

Forma kształcenia	Imię i nazwisko
1. Wykład	Kashuba Svetlana, dr inż.
2. Zajęcia laboratoryjne	Kashuba Svetlana, dr inż.
3. Ćwiczenia	
4. Zajęcia projektowe	
5. Zajęcia warsztatowe	
6. Gra symulacyjna	
7. Lektorat językowy	
8. Praktyki	