Załącznik nr 9
do Zarządzenia Rektora Nr 35/19
z dnia 12 czerwca 2019 r.

IV. Opis programu studiów

3. KARTA PRZEDMIOTU

Kod przedmiotu	
Nazwa przedmiotu	**Bezpieczeństwo systemów komputerowych**
Nazwa przedmiotu w języku angielskim	**Computer systems security**
Obowiązuje od roku akademickiego	**2019/20**

USYTUOWANIE MODUŁU W SYSTEMIE STUDIÓW

Kierunek studiów	**Informatyka**
Poziom kształcenia	**I stopień**
Profil studiów	**Ogólnoakademicki**
Forma i tryb prowadzenia studiów	**Studia niestacjonarne**
Zakres	**Systemy Informacyjne**
Jednostka prowadząca przedmiot	**Katedra Systemów Informatycznych**
Koordynator przedmiotu	**dr inż. Andrzej Kułakowski**
Zatwierdził	**Dziekan Wydziału Elektrotechniki Automatyki i Informatyki Dr hab. inż. Antoni Różowicz, prof. PŚk**

OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

Przynależność do grupy/bloku przedmiotów	**Przedmiot specjalnościowy**
Status przedmiotu	**Wybieralny**
Język prowadzenia zajęć	**Polski**
Usytuowanie modułu w planie studiów - semestr	**Semestr VII**
Wymagania wstępne	**Programowanie**
Egzamin (TAK/NIE)	**Nie**
Liczba punktów ECTS	**3**

Forma prowadzenia zajęć	**wykład**	**ćwiczenia**	**laboratorium**	**projekt**	**Inne**
Liczba godzin w semestrze	**18**	**0**	**18**	**0**	**0**

EFEKTY UCZENIA SIĘ

Kategoria	Symbol efektu	Efekty kształcenia	Odniesienie do efektów kierunkowych
Wiedza	W01	Zna podstawowe zagrożenia bezpieczeństwa systemów operacyjnych i aplikacji oraz narzędzia do przeciwdziałania im.	INF1_W27, INF1_W28, INF1_W29
	W02	Zna podstawowe zagrożenia bezpieczeństwa infrastruktury sieciowej i usług sieciowych oraz narzędzia do przeciwdziałania im.	INF1_W27, INF1_W28, INF1_W29
	W03	Dysponuje podstawową wiedzą z obszaru kryptografii symetrycznej i asymetrycznej.	INF1_W02
Umiejętności	U01	Umie wykorzystać implementacje algorytmów szyfrowania danych w wybranych problemach kryptograficznych.	INF1_U08
	U02	Potrafi poprawnie konfigurować system operacyjny w celu osiągnięcia zakładanego poziomu bezpieczeństwa danych lokalnych.	INF1_U31
	U03	Potrafi poprawnie konfigurować serwery sieciowe w celu osiągnięcia zakładanego poziomu bezpieczeństwa danych w sieci.	INF1_U31
Kompetencje społeczne	K01	Rozumie znaczenie bezpieczeństwa systemów komputerowych i jego wpływu na pozatechniczne aspekty działalności inżynierskiej.	INF1_K02

TREŚCI PROGRAMOWE

Forma zajęć	Treści programowe
wykład	Elementy kryptografii. Wybrane strategie i rozwiązania aplikacyjne. Zagrożenia systemów komputerowych. Polityka bezpieczeństwa w zarysie. Podzielność liczb całkowitych. Liczby pierwsze i liczby złożone. Kongruencje. Problemy numeryczne spotykane w kryptografii. Kryptosystemy symetryczne. Szyfry afiniczne i monoalfabetyczne. Homomorficzne szyfry podstawieniowe. Polialfabetyczne szyfry podstawieniowe. Kaskadowe algorytmy szyfrowania danych. Kryptosystemy asymetryczne.Algorytm RSA i jego bezpieczeństwo. Złożoność obliczeniowa algorytmu RSA. Kryptosystemy hybrydowe w zarysie. Generatory liczb pseudolosowych.Generatory liniowe, bitowe, bazujące na odejmowaniu z pożyczką i mnożeniu z przeniesieniem. Bezpieczeństwo generatorów. Testy generatorów – test Pi, wartości oczekiwanej, wariancji, itp. Zmiana funkcji rozkładu gęstości prawdopodobieństwa generatora. Wprowadzenie do funkcji mieszających. Mieszanie szeregowe i równoległe. Algorytmy MD5 i SHA-1. Mieszanie bazujące na kryptosystemach. Wybrane elementy bezpieczeństwa systemów operacyjnych. Złośliwe oprogramowanie: wirusy, konie trojańskie, itp. Oprogramowanie zabezpieczające: zapory ogniowe, antywirusowe, itp. Uprawnienia użytkowników. Wybrane elementy bezpieczeństwa infrastruktury sieciowej. Sieci VPN typu użytkownik – serwer oraz serwer - serwer. Protokoły PPTP, L2TP i SSTP. Protokół IPSec. Certyfikaty bezpieczeństwa. Serwery proxy. Wybrane elementy bezpieczeństwa usług sieciowych. Bezpieczeństwo usług WWW, poczty elektronicznej, komunikatorów internetowych, itp. Protokoły SSH i SSL. Tunelowanie portów. Wybrane elementy bezpieczeństwa aplikacji. Bezpieczne programowanie. Ochrona przed błędami. Ochrona aplikacji przed nieuprawnionym kopiowaniem. Bezpieczeństwo operacji finansowych – wykorzystanie stałoprzecinkowych reprezentacji liczb rzeczywistych.

	Podsumowanie. Kolokwium.
laboratorium	Projekt symetrycznego systemu kryptograficznego. Implementacja programu komputerowego do szyfrowania/deszyfrowania danych z wykorzystaniem wybranego kryptosystemu symetrycznego. Projekt asymetrycznego systemu kryptograficznego. Implementacja programu komputerowego do szyfrowania/deszyfrowania danych z wykorzystaniem wybranego kryptosystemu asymetrycznego. Badanie funkcji skrótu i generatorów liczb pseudolosowych. Implementacja programu komputerowego do wyznaczania wartości funkcji skrótu z wiadomości oraz przeprowadzenie symulacji dotyczących odporności funkcji na tzw. atak urodzinowy. Przeprowadzenie testów wybranych generatorów liczb pseudolosowych (test wartości oczekiwanej, wariancji, Pi) Projekt bezpiecznej stacji roboczej. Projekt konfiguracji kont użytkowników stacji roboczej i zabezpieczenia ich przed nieuprawnionym dostępem do danych. Projekt bezpiecznego połączenia VPN typu klient-klient. Projekt konfiguracji bezpiecznego połączenia pomiędzy komputerami w ramach sieci VPN (połączenie serwera i stacji roboczej) z wykorzystaniem systemu operacyjnego . Projekt bezpiecznego połączenia VPN typu serwer-serwer. Projekt konfiguracji bezpiecznego połączenia pomiędzy komputerami w ramach sieci VPN (połączenie dwóch serwerów) z wykorzystaniem systemu operacyjnego . Konfiguracja zapór ogniowych. Projekt bezpiecznego serwera usług sieciowych (FTP, HTTP, POP3, IMAP, SMTP, i inne), w tym konfiguracja zapory ogniowej z wykorzystaniem systemu operacyjnego .
	Prezentacja i ocena wykonywanych zadań. Zaliczenie

METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ

Symbol efektu	Metody sprawdzania efektów uczenia się					
	Egzamin ustny	Egzamin pisemny	Kolokwium	Projekt	Sprawozdanie	Inne
W01			x		x	
W02			x		x	
W03			x		x	
U01					x	
U02					x	
U03					x	
K01			x		x	

FORMA I WARUNKI ZALICZENIA

Forma zajęć	Forma zaliczenia	Warunki zaliczenia
wykład	zaliczenie z oceną	Uzyskanie pozytywnej oceny z zajęć laboratoryjnych lub co najmniej 50% punktów z kolokwium.
laboratorium	zaliczenie z oceną	Uzyskanie łącznie co najmniej 50% punktów z realizacji zadań laboratoryjnych.

NAKŁAD PRACY STUDENTA

Bilans punktów ECTS								
Lp.	**Rodzaj aktywności**	**Obciążenie studenta**					**Jednostka**	
1.	Udział w zajęciach zgodnie z planem studiów	W	C	L	P	S	h	
		18		18				
2.	Inne (konsultacje, egzamin)	2		2			h	
3.	**Razem przy bezpośrednim udziale nauczyciela akademickiego**	**40**					h	
4.	**Liczba punktów ECTS, którą student uzyskuje przy bezpośrednim udziale nauczyciela akademickiego**	**1,6**					ECTS	
5.	**Liczba godzin samodzielnej pracy studenta**	**35**					h	
6.	**Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy**	**1,4**					ECTS	
7.	**Nakład pracy związany z zajęciami o charakterze praktycznym**	**40**					h	
8.	**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym**	**1,6**					ECTS	
9.	**Sumaryczne godzinowe obciążenie pracą studenta**	**75**					h	
10.	**Punkty ECTS za moduł** *1 punkt ECTS=25 godzin obciążenia studenta*	**3**						

LITERATURA

1. Pieprzyk J., Hardjono T., Seberry J., Teoria bezpieczeństwa systemów komputerowych, Helion, 2005.
2. Stallings W., Network Security Essentials. Prentice Hall, 2003.
3. Stokłosa J., Bliski T., Pankowski T., Bezpieczeństwo danych w systemach informatycznych. PWN, 2001.
4. Ferguson N., Schneier B., Kryptografia w praktyce., Helion, 2004.
5. Cheswick W. R. Firewalle i bezpieczeństwo w sieci. Helion, 2003.
6. http://wazniak.mimuw.edu.pl/index.php?title=Bezpiecze%C5%84stwo_system%C3%B3w_komputerowych

7. Inne aktualne materiały internetowe.