Załącznik nr 7 do Zarządzenia Nr…….

KARTA KURSU (realizowanego w module specjalności)

Stosunki Międzynarodowe
Polityka zagraniczna i bezpieczeństwo międzynarodowe
(nazwa specjalności)

Nazwa	**BEZPIECZEŃSTWO INFORMACJI I SYSTEMÓW INFORMACYJNYCH**
Nazwa w j. ang.	**Security of Information and information systems**

Kod		Punktacja ECTS*	4

Koordynator	Prof. dr hab. Marek R. Ogiela	Zespół dydaktyczny prof. dr hab. Marek Ogiela

Opis kursu (cele kształcenia)

Celem przedmiotu jest przekazanie podstawowej wiedzy związanej z technikami gwarantowania poufności informacji w systemach komputerowych, a także aspektów bezpieczeństwa funkcjonowania protokołów transmisji danych teleinformatycznych. Kurs jest prowadzony w języku polskim.

Efekty kształcenia

	Efekt kształcenia dla kursu	Odniesienie do efektów dla specjalności (określonych w karcie programu studiów dla modułu specjalnościowego)
Wiedza	W01: zna klasyczne koncepcje kryptograficzne oparte na technikach podstawieniowych i przestawieniowych	. **Sp2bm_W03, Sp2bm_W04**
	W02: omawia wybrane algorytmy gwarantowania poufności i integralności danych	**Sp2bm_W04**
	W03: wymienia standardowe algorytmy szyfrowania danych	**Sp2bm_W04**

	Efekt kształcenia dla kursu	Odniesienie do efektów dla specjalności (określonych w karcie programu studiów dla modułu specjalność)
Umiejętności	U01: potrafi omawiać proste algorytmy szyfrujące U02: objaśnia zasady funkcjonowania infrastruktury klucza publicznego. U03: charakteryzuje standardowe algorytmy szyfrowania danych	**Sp2bm_U01,** **Sp2bm_U02** **Sp2bm_U02** **Sp2bm_U02**

	Efekt kształcenia dla kursu	Odniesienie do efektów dla specjalności (określonych w karcie programu studiów dla modułu specjalnościowego)
Kompetencje społeczne	K01: rozumie potrzebę kształcenia ustawicznego i śledzenia na bieżąco zmian w zakresie standardów odnoszących się nowoczesnych algorytmów szyfrujących i bezpieczeństwa danych	**Sp2bm_K01,** **Sp2bm_K02,** **Sp2bm_K03**

Organizacja												
Forma zajęć	Wykład (W)	Ćwiczenia w grupach										
		A		K		L		S		P		E
Liczba godzin	15	15										

Opis metod prowadzenia zajęć

Kurs składa się z wykładu i ćwiczeń audytoryjnych. W ramach audytoriów studenci opracowują przykłady oraz rozwiązują problemy przedstawione przez prowadzącego zajęcia. Dodatkowo w trakcie kursu studenci otrzymują do rozwiązania krótkie zadania problemowe oraz opracowują indywidualnie lub w grupach referat/prezentację (*tematykę wskazuje prowadzący*).
Na ćwiczeniach audytoryjnych na bieżąco weryfikowana będzie wiedza przekazywana podczas wykładów.

Formy sprawdzania efektów kształcenia

	E – learning	Gry dydaktyczne	Ćwiczenia w szkole	Zajęcia terenowe	Praca laboratoryjna	Projekt indywidualny	Projekt grupowy	Udział w dyskusji	Referat	Praca pisemna (esej)	Egzamin ustny	Egzamin pisemny	Inne
W01					X	X							
W02					X	X							
U01					X	X							
U02					X	X							
K01					X	X							
K02					x	X							
...													

Kryteria oceny	Ocena końcowa jest zależna od uczestnictwa na wykładach i zajęciach audytoryjnych. Ocenę dobrą i bardzo dobrą może uzyskać student, który: • zna sposoby wykorzystania sygnatur cyfrowych, autoryzacji stron oraz protokoły współdzielenia informacji. • Zna techniki utajniania informacji. orientuje się w podstawowych problemach i wyzwaniach systemów bezpieczeństwa danych

Uwagi	

Treści merytoryczne (wykaz tematów)

1. Klasyczne koncepcje kryptograficzne m.in. szyfry monoalfabetyczne, polialfabetyczne, XOR, schemat Vernama.
2. Algorytmy gwarantowania poufności i integralności danych.
3. Mechanizmy tworzenia bezpiecznych kanałów komunikacyjnych w sieciach teleinformatycznych.
4. Funkcjonowanie infrastruktury klucza publicznego.
5. Mechanizmy tworzenia sygnatur cyfrowych, autoryzacji stron oraz protokoły współdzielenia informacji i przekazywania istotnych danych.
6. Standardowe algorytmy szyfrowania danych i systemów plików.

Wykaz literatury podstawowej

1. Marek R. Ogiela, *Bezpieczeństwo systemów komputerowych*, AGH, Kraków 2002
2. Marek R. Ogiela, *Systemy utajniania informacji - od algorytmów do kryptosystemów szyfrujących*, Wydawnictwa AGH, Kraków 2003
3. Jonathan Katz, Yehuda Lindell, *Introduction to modern cryptography*, CRC Press, 2007

Wykaz literatury uzupełniającej

Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno, Cryptography Engineering: Design Principles and Practical Applications, J. Wiley, 2010

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta)

Ilość godzin w kontakcie z prowadzącymi	Wykład	15
	Konwersatorium (ćwiczenia, laboratorium itd.)	15
	Pozostałe godziny kontaktu studenta z prowadzącym	5
Ilość godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	25
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	15
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	10
	Przygotowanie do egzaminu	20
Ogółem bilans czasu pracy		
Ilość punktów ECTS w zależności od przyjętego przelicznika		4