

## KARTA KURSU DLA STUDIÓW PODYPLOMOWYCH

NAZWA	<b>Bezpieczeństwo informacji w sieci</b>
NAZWA W J. ANG.	Network security

PUNKTACJA ECTS*	3
-----------------	---

## OPIS KURSU (Cele kształcenia)

Celem kursu jest zapoznanie słuchaczy studiów podyplomowych z wybranymi aspektami bezpieczeństwa w sieci komputerowej.  
Kurs jest realizowany w języku polskim.

## EFEKTY KSZTAŁCENIA

	Efekt kształcenia dla kursu	Efekty kształcenia dla studiów podyplomowych
WIEDZA	Po zakończeniu kursu słuchacz studiów podyplomowych: W01: zna rodzaje zagrożeń związanych z użytkowaniem sieci komputerowej oraz sposobów zabezpieczania się przed nimi.	W05
	W02: ma wiedzę na przestępstw komputerowych.	W05

	Efekt kształcenia dla kursu	Efekty kształcenia dla studiów podyplomowych
UMIĘTNOŚCI	Po zakończeniu kursu słuchacz studiów podyplomowych: U01: rozróżnia i kategoryzuje zagrożenia sieciowe.	W05
	U02: potrafi wykonać podstawowe operacje konfiguracyjne na urządzeniach cyfrowych, w celu ich zabezpieczenia przez nieuprawnionym dostępem i innymi zagrożeniami.	

	Efekt kształcenia dla kursu	Efekty kształcenia dla studiów podyplomowych
KOMPETENCJE SPOŁECZNE	Po zakończeniu kursu słuchacz studiów podyplomowych: K01: rozumie konieczność stosowania zabezpieczeń podczas korzystania z sieci komputerowej.	K03

ORGANIZACJA							
FORMA ZAJĘĆ	WYKŁAD (W)	ZAJĘCIA W GRUPACH					
		A	K	L	S	P	EL
LICZBA GODZIN	-	12	-	-	-	-	-

## OPIS METOD PROWADZENIA ZAJĘĆ

Kurs składa się z ćwiczeń, podczas których omawiane są teoretyczne zagadnienia związane z zagrożeniami występującymi w sieci komputerowej. Wiedza ta poszerzona zostanie o praktyczne pokazy związane z konfiguracją aplikacji i urządzeń, której zadaniem jest zabezpieczanie przed zagrożeniami i nieuprawnionym dostępem.

## 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					X
W02					X			X					X
U01					X			X					X
U02					X			X					X
K01					X			X					

## TREŚCI MERYTORYCZNE (wykaz tematów)

1. Zagrożenia związane z użytkowaniem komputerów i sieci komputerowej – dlaczego zagrożony jest każdy „Jan Kowalski”?
  - a. Szkodliwe oprogramowanie (klasyfikacja, charakterystyka działania, sposoby wykrywania, ochrona)
  - b. Szkodliwe działania w sieci (sniffing, spoofing, hacking, cracking, phishing i inne)
  - c. Rodzaje ataków sieciowych
  - d. Socjotechniki
2. Bezpieczeństwo (w) sieci bezprzewodowej
  - a. Konfiguracja routera – konieczne działania (szyfrowanie, bezpieczne hasło, zasięg, adresy MAC itd.)
3. Bezpieczne zakupy
  - a. Szyfrowane transmisje i certyfikaty
  - b. Bezpieczeństwo płatności online
4. Portale społecznościowe
5. Zagrożenia związane z użytkowaniem urządzeń mobilnych.

## Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta)

Liczba godzin w kontakcie z prowadzącymi	Wykład	
	Konwersatorium (ćwiczenia, laboratorium itd.)	12
	Pozostałe godziny kontaktu studenta z prowadzącym	18
Liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	5
	Przygotowanie projektu zaliczeniowego	5
	Przygotowanie do zajęć (ćwiczenia w domu)	5
	Przygotowanie do zaliczenia	15
Ogółem bilans czasu pracy		60
Liczba punktów ECTS w zależności od przyjętego przelicznika		3