

## KARTA OPISU PRZEDMIOTU

STUDIA PODYPLOMOWE	<b>INFORMATYKA Z ELEMENTAMI INFORMATYKI ŚLEDZCZEJ</b>
--------------------	-------------------------------------------------------

NAZWA PRZEDMIOTU	TECHNIKI POZYSKIWANIA DANYCH		
SUBJECT TITLE	DATA MINING		
SEMESTR STUDIÓW	ECTS (pkt.)	TRYB ZALICZENIA PRZEDMIOTU	KOD PRZEDMIOTU
2	3	ZALICZENIE NA OCENĘ *)	
Wymagania wstępne w zakresie przedmiotu	Nazwy przedmiotów	-	
	Wiedza	1. Podstawowa wiedza z zakresu ochrony danych, elektrotechniki i statystyki	
	Umiejętności	1. Potrafi stosować komputer dla modelowania układów technicznych	
	Kompetencje społeczne	1. Potrafi współdziałać i pracować w grupie	

PROGRAM PRZEDMIOTU		
FORMA ZAJĘĆ	LICZBA GODZIN ZAJĘĆ W SEMESTRZE	PROWADZĄCY ZAJĘCIA (tytuł/stopień naukowy, imię i nazwisko)
WYKŁAD	10	PROF. DR HAB. INŻ. WOŁODYMYR KHOMA
ĆWICZENIA		
LABORATORIUM		
PROJEKT		
SEMINARIUM	15	PROF. DR HAB. INŻ. WOŁODYMYR KHOMA

TREŚCI KSZTAŁCENIA (PROGRAM NAUCZANIA)			
WYKŁAD	SPOSÓB REALIZACJI:	WYKŁAD Z WYKORZYSTANIEM RZUTNIKA	
Lp.	Tematyka zajęć		Liczba godzin
1.	Wprowadzenie do przedmiotu. Pozyskiwanie danych a bezpieczeństwo informacji. Przegląd legalnych i nielegalnych metod pozyskiwania danych. Obszary i możliwości zastosowań		1
2.	Wywiad sygnałów (signals intelligence). Promieniowanie elektromagnetyczne. Źródła emisji ujawniającej		1
3.	Zabezpieczenia przed emisją ujawniającą. Pasywne i aktywne środki ochrony. Technologia TEMPEST		1
4.	Informacja w postaci akustycznej. Metody i technika podsłuchu. Metody wykrywania i ochrona przed podsłuchem. Bezpieczeństwo usług telefonicznych		2
5.	Technologii Firewall, IDS, Honey Pot, ochrona antywirusowa jako przykłady legalnych metod pozyskiwania danych		2
6.	Zarządzanie bezpieczeństwem i ryzykiem. Standard ISO 27000. System zarządzania incydentami bezpieczeństwa netForensics. Analityka logów		1
7.	Metody eksploracji danych. Sieci neuronowe i ich zastosowanie w zagadnieniach Data Mining		1
8.	Zaliczenie przedmiotu		1
RAZEM GODZIN W SEMESTRZE			10
Sposoby sprawdzenia zamierzonych efektów kształcenia		Test sprawdzający wiedzę	

LABORATORIUM		SPOSÓB REALIZACJI:	ZAJĘCIA PRAKTYCZNE Z KOMPUTEREM
Lp.	Tematyka zajęć		Liczba godzin
1.	Kanały techniczne ucieczki informacji: przechwycenie Wim van Ecka i Markusa Kuhna, łamanie zabezpieczeń kryptograficznych przez analizę kanałów ubocznych		1
2.	Ochrona przed emisją ujawniającą: wykrywanie podsłuchów, klatki Faradaja, filtry blokujące, generatory szumu maskującego		1
3.	Metody data mining w systemach biometrycznych i rozpoznawaniu mowy		2
4.	Eksploracja danych w sieciach komputerowych: systemy IDS/IPS, analiza kontekstowa proxy ochrona przed atakami DOS/DDOS, ochrona antywirusowa		2
5.	Wykorzystanie technik pozyskiwania danych w systemach uwierzytelniania, autoryzacji i rozliczania w sieciach komputerowych. Technologia RFID		2
6.	Eksploracja tekstu i sieci WWW: Pozyskiwanie informacji z dokumentów tekstowych, filtrowanie zawartości internetowej, ochrona poczty elektronicznej i ograniczanie spamu		2
7.	Pozyskiwanie danych w kryptoanalizie i steganoanalizie. Cyfrowe znaki wodne		1
8.	Wykorzystanie metod data mining w wybranych przykładach zastosowań		3
9.	Zaliczenie przedmiotu		1
RAZEM GODZIN W SEMESTRZE			15
Sposoby sprawdzenia zamierzonych efektów kształcenia:		Wykonanie zadań wyznaczonych w trakcie zajęć	

Efekty kształcenia dla przedmiotu – po zakończonym cyklu kształcenia	Wiedza	1. Zna podstawowe metody i techniki pozyskiwania i ochrony danych
	Umiejętności	1. Potrafi wykonywać analizę danych z wykorzystaniem technik i metod signals intelligence oraz data mining
	Kompetencje społeczne	1. Potrafi współdziałać i pracować w grupie, przyjmując w niej różne role

#### ZAŁOŻENIA I CELE PRZEDMIOTU:

Celem przedmiotu jest zdobycie podstawowej wiedzy i umiejętności w zakresie technik i metod eksploracji sygnałów i danych, w celu wykorzystania ich do monitoringu bezpieczeństwa i ochrony informacji w sieciach komputerowych.

#### METODY DYDAKTYCZNE:

Wykład – wykład konwencjonalny, wykład problemowy, dyskusja (środki: rzutnik, komputer, prezentacje).  
Seminarium – metoda przygotowania i ogłoszenia prezentacji według podanego tematu, uzupełniającego program przedmiotu (środki: komputery, dedykowane oprogramowanie).

#### FORMA I WARUNKI ZALICZENIA PRZEDMIOTU:

Wykład – zaliczenie pisemne na ocenę (w formie testu sprawdzającego wiedzę). Seminarium – ocena na podstawie ogłoszenia prezentacji (odzwierciedlająca wiedzę, opanowanie tematem odpowiedzi na pytania w dyskusji).

#### LITERATURA PODSTAWOWA:

- [1] Podstawy bezpieczeństwa systemów mteleinformatycznych. Praca zbiorowa pod redakcją Andrzeja Białasa. Gliwice: Wyd. Pracowni Komputerowej Jacka Skalmierskiego, 2002.
- [2] E. Schetina, K. Green, J. Carlson. Bezpieczeństwo w sieci. Gliwice: Wyd. HELION, 2002.
- [3] Wesley J. Noonan. Ochrona infrastruktury sieciowej. Kraków: Wyd. "EDITION 2000", 2004.
- [4] David H., Heikki M., Padhraic S., Eksploracja danych, ISBN 83-204-3053-4, WNT, Warszawa 2005.
- [5] Jesús Mena, Investigative Data Mining for security and criminal detection, ISBN: 0-7506-7613-2, Elsevier Science, 2003.

#### LITERATURA UZUPEŁNIAJĄCA:

- [1] Stallings William. Network security essentials. Applications and standarts. Prentice HALL: 2000.
- [2] Eksploracja danych (materiały dydaktyczne MIMUW na studia informatyczne II stopnia) [<http://wazniak.mimuw.edu.pl/>]
- [3] Han J., Kamber M., Pei J., Morgan Kaufmann Data Mining: Concepts and Techniques, 3rd ed., 2011.

\*) niewłaściwe przekreślić

.....  
/Kierownik studiów podyplomowych/

.....  
/autor – osoba prowadząca wykład/

.....  
/Kierownik jednostki organizacyjnej:  
pieczęć i podpis/

.....  
/Dziekan Wydziału WEAiI:  
pieczęć i podpis/