

Politechnika Opolska
Wydział Elektrotechniki, Automatyki i Informatyki

Karta Opisu Przedmiotu

Studia podyplomowe		INFORMATYKA ŚLEDZCA		
Nazwa przedmiotu		Podstawy sieci komputerowych		
Subject Title		Computer networks		
Semestr		ECTS (pkt)	Tryb zaliczenia przedmiotu	Kod przedmiotu
1		2	Zaliczenie na ocenę	
Wymagania wstępne w zakresie przedmiotu	Wiedza	1. Ma podstawową wiedzę w zakresie systemu binarnego, decymalnego i heksadecymalnego.		
	Umiejętności	1. Potrafi dokonywać konwersji liczb w dowolnej konfiguracji w systemach: binarnym, decymalnym i heksadecymalnym.		
	Kompetencje społeczne	1. Potrafi współdziałać i pracować w grupie.		
Cele przedmiotu: Celem przedmiotu jest zdobycie szczegółowej wiedzy i umiejętności w zakresie działania sieci komputerowych oraz podstawowej wiedzy z zakresu funkcjonowania telefonii komórkowej GSM i systemów nawigacji satelitarnej GPS i glonass				
Program przedmiotu				
Forma zajęć	L. godz. zajęć w sem.	Prowadzący zajęcia (tytuł/stopień naukowy, imię i nazwisko)		
Wykład	10	dr inż. Mariusz Gola		
Ćwiczenia				
Laboratorium	10	dr inż. Mariusz Gola		
Projekt				
Seminarium				
Treści kształcenia				
Wykład		Sposób realizacji	Kształcenie na odległość	
Lp.	Tematyka zajęć			Liczba godzin
1.	Zakres wykładu, warunki zaliczenia, literatura. Wprowadzenie do sieci komputerowych.			1
2.	Wprowadzenie do sieci komputerowych: wykorzystanie sieci, zapewnienie jakości usług.			1
3.	Funkcjonalność i protokoły warstwy aplikacji: DNS, HTTP, SMTP, POP3, FTP.			1
4.	Warstwowy model sieci ISO/OSI. Warstwa transportowa modelu OSI: protokoły TCP i UDP.			1
5.	Warstwa sieci modelu OSI: protokół IPv4. Adresowanie sieci zgodnie z IPv4.			1
6.	Warstwa łącza danych OSI: dostęp do medium, adresowanie. Warstwa fizyczna modelu OSI: media transmisyjne i kodowanie sygnału.			1
7.	Elementy, funkcje i zasada działania sieci Ethernet, Okablowanie, planowanie i konfigurowanie sieci komputerowych.			1
8.	Testowanie i diagnostyka sieci komputerowych.			1
9.	Podstawy systemu telefonii komórkowej GSM, Podstawy systemów nawigacji satelitarnej GPS i glonass.			1

10.	Zaliczenie przedmiotu.	1		
Liczba godzin zajęć w semestrze		10		
Laboratorium	Sposób realizacji	Zajęcia praktyczne z komputerem		
Lp.	Tematyka zajęć	Liczba godzin		
1.	Zapoznanie z zasadami bezpieczeństwa obowiązującymi w laboratorium, potwierdzenie odbycia instruktażu. Zapoznanie się z regulaminem, zasadami pracy, omówienie warunków uzyskania zaliczenia oraz przedstawienie zagadnień poruszanych na zajęciach.	0,5		
2.	Prezentacja dostępnych programów narzędziowych, ćwiczenia z enkapsulacji jednostek danych protokołu modelu OSI przy pomocy programu przechwytyjącego.	1		
3.	Ćwiczenia przy pomocy programu przechwytyjącego w zakresie analizy działania protokołów warstwy transportowej modelu OSI: TCP i UDP.	1		
4.	Ćwiczenia przy pomocy programu przechwytyjącego w zakresie analizy działania protokołów warstwy sieci modelu OSI: IPv4.	1,5		
5.	Ćwiczenia z podstawowych poleceń konfiguracyjnych i diagnostycznych właściwości sieciowych w środowisku Windows.	1,5		
6.	Ethernet: analiza ramek z różnymi typami transmisji, analiza działania przełączników sieciowych, analiza działania protokołu ARP.	1,5		
7.	Praca z symulatorem: realizacja prostego modelu sieci.	1,5		
8.	Podstawowa konfiguracja przełączników i routerów.	1,5		
Liczba godzin zajęć w semestrze		10		
Efekty kształcenia dla przedmiotu - po zakończonym cyklu kształcenia		Odniesienie do kierunkowych efektów kształcenia	Formy realizacji (W, C, L, P, S)	Formy weryfikacji efektów kształcenia
Wiedza	1. ma uporządkowaną podbudowaną teoretycznie wiedzę dotyczącą sieci komputerowych,	P_W01	W	C,D
	2. ma szczegółową wiedzę w zakresie protokołów sieciowych i ich wzajemnych relacji,	P_W01	W	C,D
	3. ma podstawową wiedzę w zakresie działania systemu sieci komórkowej GSP, systemów nawigacji satelitarnej GPS i glonass.	P_W01	W	C,D
Umiejętności	1. potrafi skonfigurować i zdiagnozować prostą sieć komputerową,	P_U01	L	H
	2. potrafi zgodnie z obowiązującymi Polskimi Normami oraz ogólnoświatowymi standardami zaprojektować prostą sieć kampusową	P_U02	L	H
	3. potrafi skonfigurować i zdiagnozować prostą sieć komputerową,	P_U02	L	H
Kompetencje społeczne	1. ma świadomość odpowiedzialności za pracę własną oraz gotowość podporządkowania się zasadom pracy w zespole i ponoszenia odpowiedzialności za wspólnie realizowane zadania.	P_K03	L	H
Formy weryfikacji efektów kształcenia: A-egzamin pisemny, B-egzamin ustny, C-zaliczenie pisemne, D-zaliczenie ustne, E-na podstawie ocen cząstkowych z odpowiedzi ustnych, F-na podstawie ocen cząstkowych z odpowiedzi pisemnych, G-praca kontrolna, H-ocena ze sprawozdań, I-ocena z przebiegu ćwiczeń, J-ocena z przygotowania do ćwiczeń, K-ocena z przebiegu realizacji projektu, L-ocena pisemnej realizacji projektu, M-ocena z obrony projektu, N-ocena formy prezentacji, O-ocena treści prezentacji, P-observacja aktywności na zajęciach, R-observacja systematyczności.				

Metody dydaktyczne:

Wykład może być prowadzony z wykorzystaniem metod i technik kształcenia na odległość.

Laboratorium – metoda laboratoryjna problemowa, metoda zajęć praktycznych (środki: komputery, osprzęt sieciowy).

Forma i warunki zaliczenia przedmiotu:

Wykład – zaliczenie pisemne w formie testu na ocenę. Laboratorium – ocena na podstawie ocen cząstkowych z poszczególnych zadań do wykonania. Ocena odzwierciedlająca wiedzę, kreatywność i zdobyte umiejętności techniczne.

Literatura podstawowa:

- [1] Dye M. A., McDonald R.: Akademia sieci CISCO. CCNA Exploration. Semestr 1 Podstawy sieci, Wydawnictwo Naukowe PWN, 2011
- [2] Andrew S. Tanenbaum: Sieci komputerowe Wydawnictwo Helion S.A. ,2008

Literatura uzupełniająca:

- [1] Institute of Electrical and Electronics Engineers: IEEE 802.3, 2011
- [2] Defense Advanced Research Projects Agency: RFC 793 TRANSMISSION CONTROL PROTOCOL, 1982
- [3] J. Postel : RFC 768 User Datagram Protocol
- [4] Defense Advanced Research Projects Agency: RFC 791 INTERNET PROTOCOL
- [5] J. Postel : RFC 792 INTERNET CONTROL MESSAGE PROTOCOL
- [6] Strony internetowe: <http://www.standards.ieee.org/develop/regauth/oui/oui.txt>
- [7] Strony internetowe: <http://www.iana.org>: IEEE 802 Numbers, Protocol Numbers, Service Name and Transport Protocol Port Number Registry
- [8] Polska Norma PN-5173

* niewłaściwe przekreślić

.....
(kierownik jednostki organizacyjnej/bezpośredni przełożony:
pieczęć/podpis)

.....
(Dziekan Wydziału
pieczęć/podpis)

Politechnika Opolska
Wydział Elektrotechniki, Automatyki i Informatyki

Karta Opisu Przedmiotu

Studia podyplomowe		INFORMATYKA ŚLEDZCA	
Nazwa przedmiotu		Bezpieczeństwo systemów komputerowych i sieci	
Subject Title		Computer systems' and networks' security	
Semestr	ECTS (pkt)	Tryb zaliczenia przedmiotu	Kod przedmiotu
1	3	Egzamin	
Wymagania wstępne w zakresie przedmiotu	Wiedza	<ol style="list-style-type: none"> 1. Podstawowa wiedza z zakresu technologii informacyjnej 2. Podstawowa wiedza o zasadach funkcjonowania sieci LAN i WAN 	
	Umiejętności	<ol style="list-style-type: none"> 1. Potrafi obsługiwać komputer i system operacyjny 2. Potrafi samodzielnie dokonywać zmian konfiguracji systemu operacyjnego w zakresie instalacji oprogramowania oraz konfiguracji sieci 3. Zna składnię i przykładowe zastosowanie poleceń i narzędzi systemowych związanych z obsługą i diagnozą pracy sieci komputerowej 	
	Kompetencje społeczne	<ol style="list-style-type: none"> 1. Potrafi współdziałać i pracować w grupie 	
<p>Cele przedmiotu: Celem przedmiotu jest zdobycie podstawowej wiedzy i umiejętności w zakresie bezpieczeństwa sieciowego oraz przełamywania standardowych zabezpieczeń celem uzyskania dostępu do danych.</p>			
Program przedmiotu			
Forma zajęć	L. godz. zajęć w sem.	Prowadzący zajęcia (tytuł/stopień naukowy, imię i nazwisko)	
Wykład	10	mgr inż. Artur Kalinowski	
Ćwiczenia			
Laboratorium	15	mgr inż. Artur Kalinowski	
Projekt			
Seminarium			
Treści kształcenia			
Wykład	Sposób realizacji	Kształcenie na odległość	
Lp.	Tematyka zajęć		Liczba godzin
1.	Hasła logowania, ich omijanie oraz ujawnianie		1
2.	Sposoby zabezpieczania danych na dyskach i nośnikach wymiennych		1
3.	Zdalny dostęp do zaszyfrowanych danych użytkownika		1
4.	Wykorzystywanie sieciowych drukarek wielofunkcyjnych do ukrywania danych oraz pozyskiwania informacji o użytkownikach		1
5.	Techniki skanowania sieci		1
6.	Wykorzystanie narzędzia Scapy do badania środowiska sieciowego		1
7.	Sniffing i jego praktyczne zastosowanie w rozpoznaniu środowiska sieciowego		1
8.	Przechwytywanie informacji w sieci lokalnej		1
9.	Popularne ataki sieciowe		1

10.	Modyfikowanie danych przesyłanych w sieci Zaliczenie przedmiotu.	1			
Liczba godzin zajęć w semestrze		10			
Laboratorium		Sposób realizacji			
Lp.	Tematyka zajęć	Liczba godzin			
1.	Uzyskiwanie dostępu do danych użytkowników bez znajomości ich haseł logowania	1			
2.	Ustawienie tylnych drzwi w systemie	1			
3.	Ukrywanie danych w systemie plików oraz poza systemem plików	1			
4.	Ujawnianie obecności obszaru HPA i odczyt danych z obszaru HPA dysku	1			
5.	Automatyzacja wyszukiwania danych osobowych i informacji pomagających w identyfikacji użytkowników	1			
6.	Wykorzystanie narzędzi pakietu Sysinternals do wstępnej analizy działania programu oraz pozyskania danych przetwarzanych przez program	1			
7.	Praktyczne wykorzystanie tunelowania i kwestia bezpieczeństwa	1			
8.	Skanowanie sieci; ustalanie systemów operacyjnych oraz uruchomionych usług sieciowych na zdalnych maszynach	1			
9.	Praktyczne wykorzystanie narzędzia Scapy	1			
10.	Wykorzystanie sniffingu do ustalenia ilości i typów urządzeń obecnych w sieci oraz techniki wykrywania snifferów	1			
11.	Atak na sieć WiFi	1			
12.	Przechwytywanie haseł oraz danych przesyłanych w sieci lokalnej	1			
13.	Proste metody ataków sieciowych w celu uzyskania dostępu do danych	1			
14.	Rozpoznawanie struktury plików i katalogów strony WWW	1			
15.	Modyfikacja danych przesyłanych w sieci	1			
Liczba godzin zajęć w semestrze		15			
Efekty kształcenia dla przedmiotu - po zakończonym cyklu kształcenia					
		Odniesienie do kierunkowych efektów kształcenia	Formy realizacji (W, C, L, P, S)	Formy weryfikacji efektów kształcenia	
Wiedza	1.	Zna podstawowe luki w bezpieczeństwie systemów i sieci oraz zna techniki umożliwiające uzyskanie nieautoryzowanego dostępu do systemów i usług sieciowych.	P_W01	W	B
	2.	Ma podstawową wiedzę o trendach rozwojowych w informatyce i ich wpływie na bezpieczeństwo systemów i sieci komputerowych.	P_W05	W	B
Umiejętności	1.	Ma umiejętność samokształcenia się i wyszukiwania potrzebnych informacji	P_U04	L	H
	2.	Potrafi pozyskiwać i analizować dane, a także umiejętnie interpretować otrzymane wyniki	P_U06	L	H
Kompetencje społeczne	1.	1. Potrafi współdziałać i pracować w grupie, przyjmując w niej różne role.	P_K03	L	H
	2.	2. Potrafi odpowiednio określić priorytety służące realizacji określonego przez siebie lub innych zadania.	P_K03	L	H
Formy weryfikacji efektów kształcenia:					
A-egzamin pisemny, B-egzamin ustny, C-zaliczenie pisemne, D-zaliczenie ustne, E-na podstawie ocen cząstkowych z odpowiedzi ustnych, F-na podstawie ocen cząstkowych z odpowiedzi pisemnych, G-praca kontrolna, H-ocena ze sprawozdań, I-ocena z przebiegu ćwiczeń, J-ocena z przygotowania do ćwiczeń, K-ocena z przebiegu realizacji projektu, L-ocena pisemnej realizacji projektu, M-ocena z obrony projektu, N-ocena formy prezentacji, O-ocena treści prezentacji, P-obserwacja aktywności na zajęciach, R-obserwacja systematyczności.					

Metody dydaktyczne:

Wykład może być prowadzony z wykorzystaniem metod i technik kształcenia na odległość.

Laboratorium – metoda laboratoryjna problemowa, metoda zajęć praktycznych (środki: komputery, spreparowane pliki opracowane przez prowadzącego, urządzenia sieciowe).

Forma i warunki zaliczenia przedmiotu:

Wykład – zaliczenie pisemne na ocenę.

Laboratorium – ocena na podstawie ocen cząstkowych z poszczególnych zadań do wykonania. Ocena odzwierciedlająca wiedzę, kreatywność i zdobyte umiejętności techniczne.

Literatura podstawowa:

- [1] Sklyarov I., *Hakerskie łamigłówki*, ISBN: 83-246-0422-7, Helion, 2006
- [2] Hope P., Walter B., *Testowanie bezpieczeństwa aplikacji internetowych. Receptury.*, ISBN: 978-83-246-2208-5, Helion, 2010
- [3] Fry Ch., Nystrom M., *Monitoring i bezpieczeństwo sieci.*, ISBN: 978-83-246-2552-9, Helion, 2010
- [4] Erickson J., *Hacking. Sztuka penetracji.*, ISBN: 83-7361-418-4, Helion, 2004

Literatura uzupełniająca:

- [1] Barrett J. D., Silverman R. E., Byrnes R. G., *Linux. Bezpieczeństwo. Receptury.*, ISBN: 83-7361-249-1, Helion, 2003
- [2] Zalewski M., *Splątana sieć. Przewodnik po bezpieczeństwie nowoczesnych aplikacji WWW.*, ISBN: 978-83-246-4477-3, Helion, 2012

* niewłaściwe przekreślić

.....
(kierownik jednostki organizacyjnej/bezpośredni przełożony:
pieczęć/podpis)

.....
(Dziekan Wydziału
pieczęć/podpis)

Politechnika Opolska
Wydział Elektrotechniki, Automatyki i Informatyki

Karta Opisu Przedmiotu

Studia podyplomowe		INFORMATYKA ŚLEDZCZA	
Nazwa przedmiotu		Techniczne aspekty bezpieczeństwa danych	
Subject Title		Data security	
Semestr	ECTS (pkt)	Tryb zaliczenia przedmiotu	Kod przedmiotu
1	3	Zaliczenie na ocenę	
Wymagania wstępne w zakresie przedmiotu	Wiedza	1. Podstawowa wiedza z zakresu technologii informacyjnej	
	Umiejętności	1. Potrafi obsługiwać komputer i system operacyjny	
	Kompetencje społeczne	1. Potrafi współdziałać i pracować w grupie	
<p>Cele przedmiotu: Celem przedmiotu jest zdobycie podstawowej wiedzy i umiejętności w zakresie analizowania i wykorzystywania wycieków danych do pozyskiwania wymaganych informacji oraz eliminowania potencjalnego zagrożenia związanego z wyciekiem danych.</p>			
Program przedmiotu			
Forma zajęć	L. godz. zajęć w sem.	Prowadzący zajęcia (tytuł/stopień naukowy, imię i nazwisko)	
Wykład	10	mgr inż. Artur Kalinowski	
Ćwiczenia			
Laboratorium	15	mgr inż. Artur Kalinowski	
Projekt			
Seminarium			
Treści kształcenia			
Wykład		Sposób realizacji	Kształcenie na odległość
Lp.	Tematyka zajęć		Liczba godzin
1.	Pojęcie wycieku danych i typy wycieków danych		1
2.	Zdalne pozyskiwanie informacji o użytkowniku i komputerze		1
3.	Identyfikacja użytkowników w serwisach internetowych, ich zainteresowań i geolokalizacji		1
4.	Analiza metadanych		1
5.	Metody ujawniania wycieków danych		1
6.	Metody zapobiegania wyciekom danych		1
7.	Techniki wykradania danych i ich skuteczność		1
8.	Wykorzystanie rygorystycznej polityki bezpieczeństwa z punktu widzenia intruzów		1
9.	Zabezpieczanie nośników danych przed niepowołanym odczytem		1
10.	Bezpieczne usuwanie danych z nośników Zaliczenie przedmiotu.		1

Liczba godzin zajęć w semestrze				10	
Laboratorium		Sposób realizacji	Zajęcia praktyczne z komputerem		
Lp.	Tematyka zajęć			Liczba godzin	
1.	Wykorzystanie harvesterów do pozyskiwania danych o użytkownikach i komputerach			1	
2.	Zastosowanie wyrażeń regularnych do wyszukiwania danych określonego typu			1	
3.	Analiza informacji ujawnianych przez przeglądarki internetowe i pozyskiwanie danych o komputerze użytkownika			1	
4.	Praktyczne wykorzystanie wycieku danych z aplikacji użytkownika			1	
5.	Wykorzystywanie błędów w logice działania aplikacji sieciowych do pozyskiwania danych			1	
6.	Techniki inżynierii społecznej i ich wykorzystanie			1	
7.	Pozyskiwanie informacji o użytkowniku na podstawie metadanych			1	
8.	Wykorzystanie serwisu Google do niejawnego pozyskiwania istotnych danych			1	
9.	Praktyczne wykorzystanie protokołu SNMP w celu przeprowadzenia ataku na urządzenie sieciowe			1	
10.	Pozyskiwanie danych tekstowych i binarnych z plików pagefile.sys oraz hiberfil.sys w celu odnalezienia poszukiwanych informacji o działaniach użytkownika			1	
11.	Komunikacja i wykradanie danych z użyciem protokołu ICMP			1	
12.	Pozyskiwanie informacji o użytkownikach w sieci lokalnej, pozyskiwanie listy loginów oraz komputerów na których pracują użytkownicy z danym loginem			1	
13.	Tworzenie skanerów użytkowników i haseł			1	
14.	Odzyskiwanie skasowanych i zmodyfikowanych plików			1	
15.	Techniki fałszowania i szybkiego zamazywania danych na nośnikach			1	
Liczba godzin zajęć w semestrze				15	
Efekty kształcenia dla przedmiotu - po zakończonym cyklu kształcenia			Odniesienie do kierunkowych efektów kształcenia	Formy realizacji (W, C, L, P, S)	Formy weryfikacji efektów kształcenia
Wiedza	1.	Zna podstawowe metody i narzędzia pomagające wykryć wyciek danych.	P_W03	W	C,D
	2.	Dysponuje wiedzą o wykorzystywaniu błędów w logice działania aplikacji do pozyskiwania danych.	P_W03	W	C,D
	3.	Zna i rozumie podstawowe pojęcia i zasady z zakresu ochrony danych oraz potrafi ustalić stopień bezpieczeństwa swoich danych.	P_W01	W	C,D
Umiejętności	1.	Ma umiejętność samokształcenia się	P_U04	L	H,K
	2.	Potrafi posługiwać się technikami informacyjno-komunikacyjnymi właściwymi do realizacji zadań związanych z analizą bezpieczeństwa i wycieku danych	P_U05	L	H
Kompetencje społeczne	1.	Potrafi współdziałać i pracować w grupie, przyjmując w niej różne role.	P_K03	L	H
	2.	Prawidłowo identyfikuje i rozstrzyga dylematy związane z wykonywaniem zawodu.	P_K02	L	H
Formy weryfikacji efektów kształcenia: A-egzamin pisemny, B-egzamin ustny, C-zaliczenie pisemne, D-zaliczenie ustne, E-na podstawie ocen cząstkowych z odpowiedzi ustnych, F-na podstawie ocen cząstkowych z odpowiedzi pisemnych, G-praca kontrolna, H-ocena ze sprawozdań, I-ocena z przebiegu ćwiczeń, J-ocena z przygotowania do ćwiczeń, K-ocena z przebiegu realizacji projektu, L-ocena pisemnej realizacji projektu, M-ocena z obrony projektu, N-ocena formy prezentacji, O-ocena treści prezentacji, P-observacja aktywności na zajęciach, R-observacja systematyczności.					

Metody dydaktyczne:

Wykład – wykład konwencjonalny, wykład problemowy, dyskusja (wykład może być prowadzony z wykorzystaniem metod i technik kształcenia na odległość.).

Laboratorium – metoda laboratoryjna problemowa, metoda zajęć praktycznych (środki: komputery, spreparowane pliki opracowane przez prowadzącego).

Forma i warunki zaliczenia przedmiotu:

Wykład – zaliczenie pisemne na ocenę.

Laboratorium – ocena na podstawie ocen cząstkowych z poszczególnych zadań do wykonania. Ocena odzwierciedlająca wiedzę, kreatywność i zdobyte umiejętności techniczne.

Literatura podstawowa:

- [1] Viega J., *Mity bezpieczeństwa IT. Czy na pewno nie masz czego się bać?*, ISBN: 978-83-246-2588-8, Helion, 2012
[2] [2] Erickson J., *Hacking. Sztuka penetracji.*, ISBN: 83-7361-418-4, Helion, 2004

Literatura uzupełniająca:

- [1] Lockhart A., *125 sposobów na bezpieczeństwo sieci.*, ISBN: 978-83-246-0986-4, Helion, 2007
[2] [2] Ross J., *Bezpieczne programowanie. Aplikacje hakeroodporne.*, ISBN: 978-83-246-2405-8, Helion, 2009

* niewłaściwe przekreślić

.....
(kierownik jednostki organizacyjnej/bezpośredni przełożony:
pieczęć/podpis)

.....
(Dziekan Wydziału
pieczęć/podpis)

Politechnika Opolska
Wydział Elektrotechniki, Automatyki i Informatyki

Karta Opisu Przedmiotu

Studia podyplomowe		INFORMATYKA ŚLEDZCA	
Nazwa przedmiotu		Aspekty prawne informatyki śledczej w Kodeksie Karnym	
Subject Title		Legal Basis for Computer Forensics in Penal Code	
Semestr	ECTS (pkt)	Tryb zaliczenia przedmiotu	Kod przedmiotu
1	2	Zaliczenie na ocenę	
Wymagania wstępne w zakresie przedmiotu	Wiedza	1. Podstawowa wiedza o przebiegu procesu karnego 2. Podstawowa wiedza o znaczeniu dowodów elektronicznych w procesie karnym	
	Umiejętności	Potrafi obsługiwać komputer i system operacyjny	
	Kompetencje społeczne	Potrafi współdziałać i pracować w grupie	
Cele przedmiotu: Celem przedmiotu jest zdobycie podstawowej wiedzy i umiejętności w zakresie gromadzenia oraz wykorzystania dowodów elektronicznych.			
Program przedmiotu			
Forma zajęć	L. godz. zajęć w sem.	Prowadzący zajęcia (tytuł/stopień naukowy, imię i nazwisko)	
Wykład	8	DR HAB. ARKADIUSZ LACH, PROF. UMK	
Ćwiczenia			
Laboratorium	8	MRG INŻ. WOJCIECH ZIMOCH, PODINSP.KAS	
Projekt			
Seminarium			
Treści kształcenia			
Wykład		Sposób realizacji	Kształcenie na odległość
Lp.	Tematyka zajęć		Liczba godzin
1.	Terminologia prawna, pojęcie i klasyfikacja dowodów elektronicznych		0,5
2.	Przeszukanie systemu informatycznego		0,5
3.	Zatrzymanie danych informatycznych		0,5
4.	Gromadzenie dowodów elektronicznych w czasie rzeczywistym		1
5.	Ograniczenia prawne w gromadzeniu dowodów elektronicznych		1
6.	Udział biegłego i specjalisty w gromadzeniu dowodów elektronicznych		1
7.	Prywatne gromadzenie dowodów elektronicznych		1
8.	Poszlakowy charakter dowodów elektronicznych		1
9.	Ocena wartości dowodowej dowodów elektronicznych		1
10.	Uzyskiwanie dowodów elektronicznych z zagranicy Zaliczenie przedmiotu.		0,5
Liczba godzin zajęć w semestrze			8

Laboratorium		Sposób realizacji	Warsztaty komputerowe / wykład multimedialny / ćwiczenia praktyczne		
Lp.	Tematyka zajęć				Liczba godzin
1.	Praktyczne aspekty wykonywania czynności procesowych				1
2.	Procedury w informatyce śledczej				1
3.	Dokumentowanie czynności procesowych				2
4.	Wykorzystanie dowodów cyfrowych w postępowaniu karnym				1,5
5.	Elementy analizy kryminalnej				1
6.	Prowadzenie analizy ryzyka na podstawie danych cyfrowych				1
7.	Zaliczenie przedmiotu.				0,5
8.					
9.					
Liczba godzin zajęć w semestrze					8
Efekty kształcenia dla przedmiotu - po zakończonym cyklu kształcenia					
			Odniesienie do kierunkowych efektów kształcenia	Formy realizacji (W, C, L, P, S)	Formy weryfikacji efektów kształcenia
Wiedza	1.	Ma wiedzę o podstawowych instytucjach prawa dowodowego związanych z dowodami elektronicznymi	P_W06	W	C,D
	2.	Zna problemy prawne związane z gromadzeniem i wykorzystaniem dowodów elektronicznych	P_W06	W,L	C,D,K,P
Umiejętności	1.	Potrafi operować terminologią prawa dowodowego	P_U01	W	C,D
	2.	Potrafi stosować w praktyce przepisy prawne związane z uzyskiwaniem dowodów elektronicznych	P_U05	L	K,P
	3.	Potrafi przygotować, redagować i prezentować zwarte prace	P_U01	W	C,D
Kompetencje społeczne	1.	Potrafi współdziałać i pracować w grupie, przyjmując w niej różne role	P_K03	L	K,P
	2.	Prawidłowo identyfikuje i rozstrzyga dylematy związane z wykonywaniem zawodu	P_K02	L	K,P
Formy weryfikacji efektów kształcenia: A-egzamin pisemny, B-egzamin ustny, C-zaliczenie pisemne, D-zaliczenie ustne, E-na podstawie ocen częściowych z odpowiedzi ustnych, F-na podstawie ocen częściowych z odpowiedzi pisemnych, G-praca kontrolna, H-ocena ze sprawozdań, I-ocena z przebiegu ćwiczeń, J-ocena z przygotowania do ćwiczeń, K-ocena z przebiegu realizacji projektu, L-ocena pisemnej realizacji projektu, M-ocena z obrony projektu, N-ocena formy prezentacji, O-ocena treści prezentacji, P-observacja aktywności na zajęciach, R-observacja systematyczności.					

Metody dydaktyczne:

Wykład – wykład konwencjonalny, wykład problemowy, dyskusja (wykład może być prowadzony z wykorzystaniem metod i technik kształcenia na odległość.).

Laboratorium – Warsztaty komputerowe / wykład multimedialny / ćwiczenia praktyczne

Forma i warunki zaliczenia przedmiotu:

Zaliczenie na ocenę

Literatura podstawowa:

- [1] A. Lach, Dowody elektroniczne w procesie karnym, Toruń 2004
- [2] A. Lach, Gromadzenie dowodów elektronicznych po nowelizacji k.p.k., Prokuratura i Prawo, nr 10/2003

Literatura uzupełniająca:

- [1] A. Adamski, Prawo karne komputerowe, Warszawa 2000
- [2] A. Gaberle, Dowody w sądowym procesie karnym, Warszawa 2010
- [3] T. Grzegorzczak, J. Tylman, Polskie postępowanie karne, Warszawa 2011

* niewłaściwe przekreślić

(kierownik jednostki organizacyjnej/bezpośredni przełożony:
pieczęć/podpis)

(Dziekan Wydziału
pieczęć/podpis)

Politechnika Opolska
Wydział Elektrotechniki, Automatyki i Informatyki

Karta Opisu Przedmiotu

Studia podyplomowe		INFORMATYKA ŚLEDZCA	
Nazwa przedmiotu		Aspekty prawne informatyki śledczej w Kodeksie Cywilnym	
Subject Title		Legal Basis for Computer Forensics in Civil Code	
Semestr	ECTS (pkt)	Tryb zaliczenia przedmiotu	Kod przedmiotu
1	1	Zaliczenie na ocenę	
Wymagania wstępne w zakresie przedmiotu	Wiedza	1. Podstawowa wiedza o przebiegu procesu karnego 2. Podstawowa wiedza o znaczeniu dowodów elektronicznych w procesie karnym	
	Umiejętności	Potrafi obsługiwać komputer i system operacyjny	
	Kompetencje społeczne	Potrafi współdziałać i pracować w grupie	
Cele przedmiotu: Celem przedmiotu jest zdobycie podstawowej wiedzy i umiejętności w zakresie gromadzenia oraz wykorzystania dowodów elektronicznych.			
Program przedmiotu			
Forma zajęć	L. godz. zajęć w sem.	Prowadzący zajęcia (tytuł/stopień naukowy, imię i nazwisko)	
Wykład	8	mgr Jarosław Góra	
Ćwiczenia			
Laboratorium			
Projekt			
Seminarium			
Treści kształcenia			
Wykład		Sposób realizacji	Kształcenie na odległość
Lp.	Tematyka zajęć		Liczba godzin
1.	Aspekty prawne informatyki śledczej – wiadomości ogólne, źródła prawa.		0,5
2.	Prawo dowodowe – procedura karna, cywilna.		1
3.	Specyfika elektronicznego materiału dowodowego. Dowody elektroniczne – rola biegłego.		0,5
4.	Dowody elektroniczne – problemy prawne i praktyczne, <i>Post mortem ca. Live forensic</i> – aspekty prawne. Ocena elektronicznego materiału dowodowego przez polskie sądy.		0,5
5.	Prywatne gromadzenie materiału dowodowego - problematyka. Prawne aspekty monitoringu, problematyka dopuszczalności monitoringu pracowników.		1
6.	Przestępstwa komputerowe – przestępstwa przeciwko bezpieczeństwu informacji.		1,5
7.	Przestępstwa komputerowe – przestępstwa związane z treścią informacji.		1
8.	Przestępstwa komputerowe – przestępstwa związane z wykorzystaniem sieci i systemów informatycznych.		1
9.	Przestępstwa komputerowe – kradzież tożsamości, cyberstalking.		0,5
10.	Cyberprzestępczość		0,5
Liczba godzin zajęć w semestrze			8

Efekty kształcenia dla przedmiotu - po zakończonym cyklu kształcenia		Odniesienie do kierunkowych efektów kształcenia	Formy realizacji (W, C, L, P, S)	Formy weryfikacji efektów kształcenia	
Wiedza	1.	Ma wiedzę o podstawowych instytucjach prawa dowodowego związanych z dowodami elektronicznymi	P_W06	W	C,D
	2.	Zna problemy prawne związane z gromadzeniem i wykorzystaniem dowodów elektronicznych	P_W06	W	C,D
Umiejętności	1.	Potrafi operować terminologią prawa dowodowego	P_U01	W	C,D
	2.	Potrafi stosować w praktyce przepisy prawne związane z uzyskiwaniem dowodów elektronicznych	P_U05	W	C,D
	3.	Potrafi przygotować, redagować i prezentować zwarte prace	P_U01	W	C,D
Kompetencje społeczne	1.	Potrafi współdziałać i pracować w grupie, przyjmując w niej różne role	P_K03	W	C,D
	2.	Prawidłowo identyfikuje i rozstrzyga dylematy związane z wykonywaniem zawodu	P_K02	W	C,D

Formy weryfikacji efektów kształcenia:

A-egzamin pisemny, B-egzamin ustny, C-zaliczenie pisemne, D-zaliczenie ustne, E-na podstawie ocen cząstkowych z odpowiedzi ustnych, F-na podstawie ocen cząstkowych z odpowiedzi pisemnych, G-praca kontrolna, H-ocena ze sprawozdań, I-ocena z przebiegu ćwiczeń, J-ocena z przygotowania do ćwiczeń, K-ocena z przebiegu realizacji projektu, L-ocena pisemnej realizacji projektu, M-ocena z obrony projektu, N-ocena formy prezentacji, O-ocena treści prezentacji, P-obszerwacja aktywności na zajęciach, R-obszerwacja systematyczności.

Metody dydaktyczne:

Wykład – wykład konwencjonalny, wykład problemowy, dyskusja (wykład może być prowadzony z wykorzystaniem metod i technik kształcenia na odległość.).

Forma i warunki zaliczenia przedmiotu:

Zaliczenie na ocenę

Literatura podstawowa:

- [1] A. Lach, Dowody elektroniczne w procesie karnym, Toruń 2004
- [2] A. Lach, Gromadzenie dowodów elektronicznych po nowelizacji k.p.k., Prokuratura i Prawo, nr 10/2003

Literatura uzupełniająca:

- [1] A. Adamski, Prawo karne komputerowe, Warszawa 2000
- [2] A. Gaberle, Dowody w sądowym procesie karnym, Warszawa 2010
- [3] T. Grzegorzczak, J. Tylman, Polskie postępowanie karne, Warszawa 2011

* niewłaściwe przekreślić

.....
(kierownik jednostki organizacyjnej/bezpośredni przełożony:
pieczęć/podpis)

.....
(Dziekan Wydziału
pieczęć/podpis)

Politechnika Opolska
Wydział Elektrotechniki, Automatyki i Informatyki

Karta Opisu Przedmiotu

Studia podyplomowe		INFORMATYKA ŚLEDZCA	
Nazwa przedmiotu		Informatyka śledcza	
Subject Title		Computer Forensics	
Semestr	ECTS (pkt)	Tryb zaliczenia przedmiotu	Kod przedmiotu
1	3	Egzamin	
Wymagania wstępne w zakresie przedmiotu	Wiedza	1. Podstawowa wiedza z zakresu technologii informacyjnej	
	Umiejętności	1. Potrafi obsługiwać komputer i system operacyjny 2. Potrafi samodzielnie dokonywać zmian konfiguracji sprzętowej zestawu komputerowego 3. Potrafi myśleć analitycznie i przewidywać z dużym wyprzedzeniem konsekwencje podejmowanych działań	
	Kompetencje społeczne	1. Potrafi współdziałać i pracować w grupie	
Cele przedmiotu: Celem przedmiotu jest zdobycie podstawowej wiedzy i umiejętności w zakresie zabezpieczania nośników danych oraz analizy danych pozyskanych z zabezpieczonych nośników pod kątem wykorzystania ich jako materiał dowodowy.			
Program przedmiotu			
Forma zajęć	L. godz. zajęć w sem.	Prowadzący zajęcia (tytuł/stopień naukowy, imię i nazwisko)	
Wykład	10	mgr inż. Artur Kalinowski	
Ćwiczenia			
Laboratorium	15	mgr inż. Artur Kalinowski	
Projekt			
Seminarium			
Treści kształcenia			
Wykład		Sposób realizacji	Kształcenie na odległość
Lp.	Tematyka zajęć		Liczba godzin
1.	Cele, podstawowe zasady i obszar działań informatyki śledczej		0,5
2.	Tworzenie zaplecza technicznego		0,5
3.	Klasyfikacja typów danych i miejsca ich występowania		0,5
4.	Metody pozyskiwania i zabezpieczania materiału do analizy		0,5
5.	Budowa popularnych systemów plików		0,5
6.	Miejsca przechowywania istotnych danych w popularnych systemach operacyjnych		1
7.	Wstępna analiza danych z utworzonych obrazów nośników i zrzutów pamięci		0,5
8.	Lokalizacja i odzyskiwanie usuniętych plików		0,5
9.	Analiza obszarów slack space oraz RAM slack		1
10.	Wyodrębnianie ciągów tekstowych z plików binarnych oraz danych binarnych z plików nieokreślonego typu oraz nośników		0,5

11.	Określanie lokalizacji poszukiwanych danych na nośniku	1
12.	Przeprowadzanie analizy czasowej	1
13.	Ukrywanie danych na nośnikach poza widoczną strukturą systemu plików	1
14.	Ukrywanie danych w systemie plików	0,5
15.	Analiza pliku binarnego w celu określenia struktury zawartych w nim danych Zaliczenie przedmiotu.	0,5
Liczba godzin zajęć w semestrze		10

Ćwiczenia		Sposób realizacji	Zajęcia praktyczne z komputerem
Lp.	Tematyka zajęć		Liczba godzin
1.	Tworzenie obrazów nośników z wykorzystaniem blokerów sprzętowych i programowych		1
2.	Porównanie metod tworzenia obrazów nośników oraz ich wad i zalet		1
3.	Zabezpieczanie danych ulotnych		1
4.	Zabezpieczanie plików z danymi		1
5.	Zabezpieczanie danych z wykorzystaniem sieci komputerowej		1
6.	Pozyskiwanie oraz analiza danych z przeglądarek internetowych, programów pocztowych i komunikatorów		1
7.	Podłączanie obrazu nośnika i przeglądanie zgromadzonych na nim danych		1
8.	Odzyskiwanie usuniętych plików z dysków i kart pamięci		1
9.	Pozyskiwanie danych z obszaru slack space		1
10.	Wyodrębnianie ciągów tekstowych oraz znanych typów danych binarnych z obrazu nośnika lub z pliku		1
11.	Określanie fizycznej lokalizacji poszukiwanych danych na dysku (lub w obrazie nośnika) oraz powiązanego z tymi danymi pliku i sąsiadującego obszaru danych		1
12.	Wykorzystanie terminala dyskowego		1
13.	Przeprowadzanie analizy czasowej		1
14.	Tworzenie bazy sygnatur i wyszukiwanie danych w oparciu o bazę sygnatur		1
15.	Analiza pliku nieznanego typu w edytorze szesnastkowym		1
Liczba godzin zajęć w semestrze			15

Efekty kształcenia dla przedmiotu - po zakończonym cyklu kształcenia			Odniesienie do kierunkowych efektów kształcenia	Formy realizacji (W, C, L, P, S)	Formy weryfikacji efektów kształcenia
Wiedza	1.	Zna podstawowe metody, techniki, narzędzia i materiały stosowane przy zabezpieczaniu elektronicznego materiału dowodowego.	P_W06	W	A,B
	2.	Ma podstawową wiedzę o trendach rozwojowych w informatyce i ich wpływie na przetwarzanie i magazynowanie danych w komputerach PC.	P_W05	W	A,B
Umiejętności	1.	Ma umiejętność samokształcenia się i wyszukiwania potrzebnych informacji	P_U04	L	H
	2.	Potrafi pozyskiwać i analizować dane, a także umiejętnie interpretować otrzymane wyniki	P_U06	L	H
Kompetencje społeczne	1.	Potrafi współdziałać i pracować w grupie, przyjmując w niej różne role.	P_K03	L	H
	2.	Potrafi odpowiednio określić priorytety służące realizacji określonego przez siebie lub innych zadania.	P_K03	L	H

Formy weryfikacji efektów kształcenia:
A-egzamin pisemny, B-egzamin ustny, C-zaliczenie pisemne, D-zaliczenie ustne, E-na podstawie ocen cząstkowych z odpowiedzi ustnych, F-na podstawie ocen cząstkowych z odpowiedzi pisemnych, G-praca kontrolna, H-ocena ze sprawozdań, I-ocena z przebiegu ćwiczeń, J-ocena z przygotowania do ćwiczeń, K-ocena z przebiegu realizacji projektu, L-ocena pisemnej realizacji projektu, M-ocena z obrony projektu, N-ocena formy prezentacji, O-ocena treści prezentacji, P-observacja aktywności na zajęciach, R-observacja systematyczności.

Metody dydaktyczne:

Wykład – wykład konwencjonalny, wykład problemowy, dyskusja (wykład może być prowadzony z wykorzystaniem metod i technik kształcenia na odległość.).

Laboratorium – metoda laboratoryjna problemowa, metoda zajęć praktycznych (środki: komputery, spreparowane pliki opracowane przez prowadzącego, blokery).

Forma i warunki zaliczenia przedmiotu:

Wykład – zaliczenie pisemne na ocenę. Laboratorium – ocena na podstawie ocen cząstkowych z poszczególnych zadań do wykonania. Ocena odzwierciedlająca wiedzę, kreatywność i zdobyte umiejętności techniczne.

Literatura podstawowa:

- [1] Kalinowski A., *Metody Inwigilacji i Elementy Informatyki Śledczej.*, ISBN: 978-83-923745-4-1, CSH, 2011
- [2] Mueller S., *Rozbudowa i naprawa komputerów PC. Wydanie XVIII.*, ISBN: 978-83-246-1511-7, Helion, 2009

Literatura uzupełniająca:

- [1] Metzger P., *GIMP. Anatomia PC. Wydanie XI.*, ISBN: 83-246-1119-3, Helion, 2007
- [2] [Danowski B., Chabiński A., *Montaż komputera PC. Ilustrowany przewodnik.*, ISBN: 83-246-0693-9 , Helion, 2007
- [3] Lal K., Rak T., *Linux. Komendy i polecenia. Praktyczne przykłady.*, ISBN: 83-7361-994-1 , Helion, 2005
- [4] [Ward B., *Jak działa Linux.*, ISBN: 83-7361-753-1 , Helion, 2005

* niewłaściwe przekreślić

.....
(kierownik jednostki organizacyjnej/bezpośredni przełożony:
pieczęć/podpis)

.....
(Dziekan Wydziału
pieczęć/podpis)

Politechnika Opolska
Wydział Elektrotechniki, Automatyki i Informatyki

Karta Opisu Przedmiotu

Studia podyplomowe		INFORMATYKA ŚLEDZCA	
Nazwa przedmiotu		Techniki analizy obrazu	
Subject Title		Image processing and analysis	
Semestr	ECTS (pkt)	Tryb zaliczenia przedmiotu	Kod przedmiotu
1	2	Zaliczenie na ocenę	
Wymagania wstępne w zakresie przedmiotu	Wiedza	1. Podstawowa wiedza z zakresu fizyki (optyka) 2. Podstawowa wiedza z zakresu technologii informacyjnej	
	Umiejętności	1. Potrafi obsługiwać komputer 2. Potrafi obsługiwać podstawowe aplikacje do edycji obrazów rastrowych	
	Kompetencje społeczne	1. Potrafi współdziałać i pracować w grupie	
Cele przedmiotu: Celem przedmiotu jest zdobycie podstawowej wiedzy i umiejętności w zakresie przetwarzania obrazów cyfrowych oraz analizy obrazów cyfrowych, również ocena autentyczności oraz metody wyszukiwania i pozyskiwania.			
Program przedmiotu			
Forma zajęć	L. godz. zajęć w sem.	Prowadzący zajęcia (tytuł/stopień naukowy, imię i nazwisko)	
Wykład	10	dr inż. Michał Podpora	
Ćwiczenia			
Laboratorium			
Projekt	10	dr inż. Michał Podpora	
Seminarium			
Treści kształcenia			
Wykład		Sposób realizacji	Kształcenie na odległość
Lp.	Tematyka zajęć		Liczba godzin
1.	Grafika rastrowa – pojęcia, przestrzenie barw		1
2.	Metody akwizycji danych, obraz cyfrowy		1
3.	Jakość obrazu cyfrowego		1
4.	Rodzaje korekcji, (korekcja barwna, przekształcenia geometryczne)		1
5.	Metody weryfikacji autentyczności obrazu cyfrowego.		1
6.	Metody weryfikacji autentyczności skanów dokumentów.		1
7.	Narzędzia i metody analizy strumienia wideo.		1
8.	Wyszukiwanie obrazów, wyszukiwanie obrazem, porównywanie.		1
9.	Zasady działania autonomicznych systemów rozpoznawania obrazu.		1
10.	Zasady działania autonomicznych systemów zwiadowczych. Zaliczenie przedmiotu.		1
Liczba godzin zajęć w semestrze			10

Projekt		Sposób realizacji	Metoda projektu		
Lp.	Tematyka zajęć				Liczba godzin
1.	Zajęcia organizacyjne: tematy projektów, zakres opracowania, PSO.				1
2.	Wstępne omówienie tematów projektów.				1
3.	Szczegółowe omówienie tematów projektów, deklaracja wyboru tematu, terminu.				1
4.	Ocena wstępnych opracowań.				1
5.	Obrony poszczególnych oddawanych przez studentów projektów.				5
6.	Zajęcia podsumowujące, wpisy.				1
Liczba godzin zajęć w semestrze					10
Efekty kształcenia dla przedmiotu - po zakończonym cyklu kształcenia			Odniesienie do kierunkowych efektów kształcenia	Formy realizacji (W, C, L, P, S)	Formy weryfikacji efektów kształcenia
Wiedza	1.	Zna podstawowe parametry i formaty obrazów rastrowych, metody i narzędzia ich korekcji.	P_W02	W	C,D
	2.	Rozumie wpływ modyfikacji obrazu na jego wiarygodność, zna cechy obrazu świadczące o jego autentyczności.	P_W02	W	C,D
	3.	Zna możliwości i zastosowania komercyjnych aplikacji analizy śledczej obrazu.	P_W02	W	C,D
Umiejętności	1.	Ma umiejętność samokształcenia się	P_U04	L	H,K
	2.	Potrafi posługiwać się technikami informacyjno-komunikacyjnymi właściwymi do realizacji zadań związanych z analizą obrazu	P_U03	L	
Kompetencje społeczne	1.	Potrafi odpowiednio określić priorytety służące realizacji określonego przez siebie lub innych zadania.	P_K03	L	H
	2.	Prawidłowo identyfikuje i rozstrzyga dylematy związane z wykonywaniem zawodu.	P_K02	L	H
Formy weryfikacji efektów kształcenia: A-egzamin pisemny, B-egzamin ustny, C-zaliczenie pisemne, D-zaliczenie ustne, E-na podstawie ocen cząstkowych z odpowiedzi ustnych, F-na podstawie ocen cząstkowych z odpowiedzi pisemnych, G-praca kontrolna, H-ocena ze sprawozdań, I-ocena z przebiegu ćwiczeń, J-ocena z przygotowania do ćwiczeń, K-ocena z przebiegu realizacji projektu, L-ocena pisemnej realizacji projektu, M-ocena z obrony projektu, N-ocena formy prezentacji, O-ocena treści prezentacji, P-observacja aktywności na zajęciach, R-observacja systematyczności.					

Metody dydaktyczne:

Wykład – wykład konwencjonalny, wykład problemowy, dyskusja (wykład może być prowadzony z wykorzystaniem metod i technik kształcenia na odległość.).

Forma i warunki zaliczenia przedmiotu:

Wykład – zaliczenie pisemne na ocenę. Projekt – ocena na podstawie ocen cząstkowych z poszczególnych etapów projektu.

Literatura podstawowa:

- [1] Malina W., Smiatacz M., *Metody cyfrowego przetwarzania obrazów*, ISBN: 83-87674-93-1, EXIT, 2005
- [2] Mokrzycki W., *Wprowadzenie do przetwarzania informacji wizualnej Tom1 Percepcja akwizycja wizualizacja*, ISBN: 978-83-60434-76-5, EXIT, 2010
- [3] Welk P., *Podstawy montażu i przetwarzania obrazu*, dostępne on-line (2013-02-01): <http://www.medialarts.pl/download/skrypty/Podstawy-montazu-i-przetwarzania-obrazu.pdf>

Literatura uzupełniająca:

- [1] Tadeusiewicz R., Korohoda P., *Komputerowa analiza i przetwarzanie obrazów*, ISBN: 83-86476-15-X, fpt, 1997, dostępne on-line (2013-02-01): http://winntbg.bg.agh.edu.pl/skrypty2/0098/komputerowa_analiza.pdf
- [2] Gajda W., *GIMP. Ćwiczenia praktyczne.*, ISBN: 978-83-246-2787-5, Helion, 2011

* niewłaściwe przekreślić

.....
(kierownik jednostki organizacyjnej/bezpośredni przełożony:
pieczęć/podpis)

.....
(Dziekan Wydziału
pieczęć/podpis)

Politechnika Opolska
Wydział Elektrotechniki, Automatyki i Informatyki

Karta Opisu Przedmiotu

Studia podyplomowe		INFORMATYKA ŚLEDZCZA	
Nazwa przedmiotu		Techniki gromadzenia informacji z serwisów www	
Subject Title		TECHNIQUES FOR INFORMATION RETRIEVAL FROM THE WEB	
Semestr	ECTS (pkt)	Tryb zaliczenia przedmiotu	Kod przedmiotu
1	3	Zaliczenie na ocenę	
Wymagania wstępne w zakresie przedmiotu	Wiedza	1. zna zasady funkcjonowania Internetu	
	Umiejętności	1. potrafi korzystać z przeglądarek internetowych 2. potrafi poprawnie instalować i konfigurować programy	
	Kompetencje społeczne	1. Potrafi współdziałać i pracować w grupie	
Cele przedmiotu: Celem przedmiotu jest zdobycie podstawowej wiedzy i umiejętności w zakresie uzyskiwania informacji z Internetu oraz poprawnej ich interpretacji, a także korzystania z wybranych przykładowych systemów wspomagających uzyskiwanie informacji.			
Program przedmiotu			
Forma zajęć	L. godz. zajęć w sem.	Prowadzący zajęcia (tytuł/stopień naukowy, imię i nazwisko)	
Wykład	10	dr hab. inż. Jerzy Kosiński	
Ćwiczenia			
Laboratorium	10	mgr inż. Tomasz Turba	
Projekt	5	mgr inż. Tomasz Turba	
Seminarium			
Treści kształcenia			
Wykład		Sposób realizacji	Kształcenie na odległość
Lp.	Tematyka zajęć		Liczba godzin
1.	Pojęcie białego wywiadu internetowego		1
2.	Mechanizmy funkcjonowania wyszukiwarek, metadane (FOCA), weryfikacja źródeł		1
3.	Wyszukiwanie treści, ludzi, wyszukiwanie stron usuniętych, zmienionych		1
4.	Internetowe bazy danych		1
5.	Wspólnoty wirtualne		1
6.	„Deep Web” – P2P, Grupy binarne, Gigatribe		1
7.	„Dark Web” – TOR, Freenet		1
8.	System informatyczne (Maltego, Silobreaker, ...)		2
9.	Zaliczenie przedmiotu.		1
Liczba godzin zajęć w semestrze			10

Laboratorium		Sposób realizacji	Zajęcia praktyczne z komputerem
Lp.	Tematyka zajęć		Liczba godzin
1.	Pojęcie i techniki wywiadu internetowego		1
2.	Mechanizmy funkcjonowania wyszukiwarek, meta dane (FOCA), weryfikacja źródeł		1
3.	Wyszukiwanie treści, ludzi, wyszukiwanie stron usuniętych, zmienionych		1
4.	Internetowe bazy danych		1
5.	Wirtualne społeczności, wywiad socjotechniczny		1
6.	„Deep Web” – P2P, Grupy binarne, Gigatribe, TOR, Freenet		1
7.	Wyszukiwanie podatności oprogramowania i sprzętu		1
8.	System informatyczne (Maltego, Silobreaker, ...)		2
9.	Zaliczenie przedmiotu.		1

Liczba godzin zajęć w semestrze	10
--	-----------

Projekt		Sposób realizacji	Metoda projektu
Lp.	Tematyka zajęć		Liczba godzin
1.	Zajęcia organizacyjne: tematy projektów, zakres opracowania, PSO. Wstępne omówienie tematów projektów.		1
2.	Obrony poszczególnych oddawanych przez studentów projektów. Dyskusja, podsumowanie, wpisy.		4

Liczba godzin zajęć w semestrze	5
--	----------

Efekty kształcenia dla przedmiotu - po zakończonym cyklu kształcenia			Odniesienie do kierunkowych efektów kształcenia	Formy realizacji (W, C, L, P, S)	Formy weryfikacji efektów kształcenia
Wiedza	1.	Zna podstawowe portale, metody, techniki i narzędzia wykorzystywane przy gromadzeniu informacji w ramach białego wywiadu, zna metodykę przeprowadzania białego wywiadu	P_W04	W	C,D
	2.	Zna wybrane narzędzia usprawniające/wizualizujące dedykowane wyszukiwaniu informacji w ramach białego wywiadu	P_W03	W	C,D
Umiejętności	1.	Potrafi pozyskiwać i analizować dane, a także umiejętnie interpretować otrzymane wyniki	P_U06	L,P	E
	2.	Potrafi użyć ogólnodostępnych narzędzi, m.in. wyszukiwarek internetowych i portali społecznościowych, jako źródła danych operacyjnych	P_U06	L,P	E
Kompetencje społeczne	1.	Ma świadomość odpowiedzialności za pracę własną oraz gotowość podporządkowania się zasadom pracy w zespole i ponoszenia odpowiedzialności za wspólnie realizowane zadania	P_K03	L,P	K,L,M
	2.	Prawidłowo identyfikuje i rozstrzyga dylematy związane z wykonywaniem zawodu	P_K02	L,P	K,L,M
	3.	Rozumie potrzebę ciągłego pogłębiania wiedzy	P_K01	L,P	K,L,M

Formy weryfikacji efektów kształcenia:
A-egzamin pisemny, B-egzamin ustny, C-zaliczenie pisemne, D-zaliczenie ustne, E-na podstawie ocen cząstkowych z odpowiedzi ustnych, F-na podstawie ocen cząstkowych z odpowiedzi pisemnych, G-praca kontrolna, H-ocena ze sprawozdań, I-ocena z przebiegu ćwiczeń, J-ocena z przygotowania do ćwiczeń, K-ocena z przebiegu realizacji projektu, L-ocena pisemnej realizacji projektu, M-ocena z obrony projektu, N-ocena formy prezentacji, O-ocena treści prezentacji, P-observacja aktywności na zajęciach, R-observacja systematyczności.

Metody dydaktyczne:

Wykład – wykład konwencjonalny, wykład problemowy, dyskusja (wykład prowadzony z wykorzystaniem metod i technik kształcenia na odległość).

Laboratorium – metoda laboratoryjna problemowa, metoda zajęć praktycznych (środki: komputery z łączem do Internetu, rzutnik).

Projekt – metoda projektu, dyskusja

Forma i warunki zaliczenia przedmiotu:

Wykład – zaliczenie pisemne na ocenę. Laboratorium – ocena na podstawie ocen cząstkowych z poszczególnych zadań do wykonania. Ocena odzwierciedlająca wiedzę, kreatywność i zdobyte umiejętności techniczne. Projekt – ocena na podstawie opracowanych raportów i prezentacji.

Literatura podstawowa:

- [1] Appel E.J., *Internet Searches for Vetting, Investigations, and Open-Source Intelligence*, ISBN: 978-1-4398-2751-2, CRCPress, 2011
- [2] Bazzell M., *Hiding from the Internet*, ISBN: 978-1478277293, CCI Publishing, 2013
- [3] Calishain T., Dornfest R., *Google hacks. Tips & tools for smarter searching*, ISBN: 0-596-00857-0, O'Reilly, 2005
- [4] Filipkowski W., Mądrzejowski W. red., *Biały wywiad. Otwarte źródła informacji wokół teorii i praktyki*, ISBN: 978-83-255-3425-7, C.H. Beck, 2011
- [5] Long J., *Google Hacking for Penetration Testers*, ISBN: 9781931836364, Syngress Media Inc., 2001

Literatura uzupełniająca:

- [1] Ahearn F.M., *Wyrażenia regularne.*, ISBN: 978-83-246-6868-7, Helion, 2013
- [2] Fitzgerald M., *How to disappear*, ISBN: 978-1-59921-977-6, Lyons Press, 2010
- [3] Kalinowski A., *Metody inwigilacji i elementy informatyki śledczej*, ISBN: 978-83-923745-4-1, CSH, 2011
- [4] Kosiński J. red., *Przestępczość teleinformatyczna*, ISBN: 978-83-7462-197-7, WSPol, 2008
- [5] Kosiński J. red., *Przestępczość teleinformatyczna 2013*, ISBN: 978-83-934456-2-2, WSPol, 2013
- [6] Liedel K., Serafin T., *Otwarte źródła informacji w działalności wywiadowczej*, ISBN: 978-83-7641-406-5, Difin, 2011
- [7] Stiekema H., *Break out! Living In the new reality*, ISBN: 978-1-4457-7966-9, Colofon, 2010
- [8] Von Kokswijk J., *Digital ego. Social and legal aspects of virtual identity*, ISBN: 978-90-5972-203-3, Eburon AP, 2007

* niewłaściwe przekreślić

.....
(kierownik jednostki organizacyjnej/bezpośredni przełożony:
pieczęć/podpis)

.....
(Dziekan Wydziału
pieczęć/podpis)

Politechnika Opolska
Wydział Elektrotechniki, Automatyki i Informatyki

Karta Opisu Przedmiotu

Studia podyplomowe		INFORMATYKA ŚLEDZCA	
Nazwa przedmiotu		Techniki odzyskiwania danych	
Subject Title		Data recovery	
Semestr	ECTS (pkt)	Tryb zaliczenia przedmiotu	Kod przedmiotu
1	2	Zaliczenie na ocenę	
Wymagania wstępne w zakresie przedmiotu	Wiedza	1. Podstawowa wiedza z zakresu technologii informacyjnej 2. Podstawowa znajomość budowy i działania nośników danych stosowanych w komputerach osobistych	
	Umiejętności	1. W podstawowym zakresie potrafi obsługiwać następujące systemy operacyjne: DOS, Linux/Unix, Windows 2. Potrafi uruchamiać komputer z zewnętrznego nośnika oraz edytować ustawienia uruchamiania	
	Kompetencje społeczne	1. Potrafi współdziałać i pracować w grupie	
Cele przedmiotu: Celem przedmiotu jest zdobycie podstawowej wiedzy i umiejętności w zakresie odzyskiwania danych usuniętych oraz uszkodzonych.			
Program przedmiotu			
Forma zajęć	L. godz. zajęć w sem.	Prowadzący zajęcia (tytuł/stopień naukowy, imię i nazwisko)	
Wykład	4	dr inż. Michał Podpora	
Ćwiczenia			
Laboratorium	14	dr inż. Michał Podpora	
Projekt			
Seminarium			
Treści kształcenia			
Wykład	Sposób realizacji	Kształcenie na odległość	
Lp.	Tematyka zajęć		Liczba godzin
1.	Systemy plików – wprowadzenie. Struktura danych na dysku, semantyka plików.		1
2.	Zasady pracy z blokerami sprzętowymi, kopia dysku/nośnika, obraz dysku/nośnika. Specyfika procedur odzyskiwania danych dla różnych typów nośników.		1
3.	Narzędzia systemowe konserwacji systemów plików. Narzędzia darmowe konserwacji systemów plików. Narzędzia profesjonalne niskopoziomowej edycji systemu plików i odzyskiwania danych.		1
4.	Odzyskiwanie danych z urządzeń mobilnych. Zaliczenie przedmiotu.		1
Liczba godzin zajęć w semestrze			4

Laboratorium		Sposób realizacji	Zajęcia praktyczne		
Lp.	Tematyka zajęć				Liczba godzin
1.	Odzyskiwanie danych usuniętych z dysku, odzyskiwanie danych ze sformatowanego nośnika, odzyskiwanie danych z innych nośników. Praca z blokerami sprzętowymi. Procedury, raportowanie.				6
2.	Odzyskiwanie danych z nośników z błędami systemów plików, odzyskiwanie danych z nośników z błędami fizycznymi. Procedury, raportowanie.				6
3.	Odzyskiwanie danych z nośników USB, CompactFlash, SDHC, innych. Pozyskiwanie danych z pamięci EEPROM.				2
Liczba godzin zajęć w semestrze					14
Efekty kształcenia dla przedmiotu - po zakończonym cyklu kształcenia			Odniesienie do kierunkowych efektów kształcenia	Formy realizacji (W, C, L, P, S)	Formy weryfikacji efektów kształcenia
Wiedza	1.	Zna możliwości i zastosowania darmowych oraz komercyjnych aplikacji do odzyskiwania danych	P_W01	W	C,D
	2.	Zna procedury, zasady oraz specyfikę postępowania z materiałem dowodowym w postaci nośników elektronicznych	P_W06	W	C,D
Umiejętności	1.	Potrafi oceniać przydatność danych do realizacji wybranego zadania	P_U06	L	E,I
	2.	Ma umiejętność samokształcenia się i wyszukiwania potrzebnych informacji	P_U04	L	E,I
	3.	Potrafi wybrać i zastosować odpowiednią metodę i narzędzie odzyskiwania danych	P_U05	L	E,I
Kompetencje społeczne	1.	Potrafi odpowiednio określić priorytety służące realizacji określonego przez siebie lub innych zadania	P_K03	L	E,I
	2.	Prawidłowo identyfikuje i rozstrzyga dylematy związane z wykonywaniem zawodu	P_K03	L	E,I
	3.	Rozumie potrzebę ciągłego pogłębiania wiedzy	P_K01	L	E,I
Formy weryfikacji efektów kształcenia: A-egzamin pisemny, B-egzamin ustny, C-zaliczenie pisemne, D-zaliczenie ustne, E-na podstawie ocen cząstkowych z odpowiedzi ustnych, F-na podstawie ocen cząstkowych z odpowiedzi pisemnych, G-praca kontrolna, H-ocena ze sprawozdań, I-ocena z przebiegu ćwiczeń, J-ocena z przygotowania do ćwiczeń, K-ocena z przebiegu realizacji projektu, L-ocena pisemnej realizacji projektu, M-ocena z obrony projektu, N-ocena formy prezentacji, O-ocena treści prezentacji, P-observacja aktywności na zajęciach, R-observacja systematyczności.					

Metody dydaktyczne:

Wykład – wykład konwencjonalny, wykład problemowy, dyskusja (wykład prowadzony z wykorzystaniem metod i technik kształcenia na odległość). Laboratorium – metoda laboratoryjna problemowa, metoda zajęć praktycznych (środki: komputery, spreparowane pliki i nośniki opracowane przez prowadzącego: dyski twarde, nośniki USB, pamięci EEPROM, inne).

Forma i warunki zaliczenia przedmiotu:

Wykład – zaliczenie pisemne na ocenę. Laboratorium – ocena na podstawie ocen cząstkowych z poszczególnych zadań do wykonania. Ocena odzwierciedlająca wiedzę, kreatywność i zdobyte umiejętności techniczne.

Literatura podstawowa:

- [1] Carvey H., *Analiza śledcza i powłamaniowa. Zaawansowane techniki prowadzenia analizy w systemie Windows 7*, ISBN: 978-83-246-6652-2, Helion, 2013
- [2] Preston W.C., *Archiwizacja i odzyskiwanie danych*, ISBN: 978-83-246-1182-9, Helion 2008
- [3] Nelson S., *Profesjonalne tworzenie kopii zapasowych*, ISBN: 978-83-246-3417-0, Helion 2012
- [4] Watson D., Jones A., *Digital Forensics Processing and Procedures: Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements*, ISBN: 9781597497428, Syngress Publishing, 2013

Literatura uzupełniająca:

- [1] Metzger P., *Anatomia PC*, ISBN: 83-246-1119-3, Helion 2007,
- [2] Pelc M., *Linux – praktyka administracji*, ISBN: 83-89529-07-6, Nakom 2005

* niewłaściwe przekreślić

.....
(kierownik jednostki organizacyjnej/bezpośredni przełożony:
pieczęć/podpis)

.....
(Dziekan Wydziału
pieczęć/podpis)

Politechnika Opolska
Wydział Elektrotechniki, Automatyki i Informatyki

Karta Opisu Przedmiotu

Studia podyplomowe		INFORMATYKA ŚLEDZCA		
Nazwa przedmiotu		Zabezpieczanie i analiza danych z urządzeń mobilnych		
Subject Title		Mobile devices data security and recovery		
Semestr		ECTS (pkt)	Tryb zaliczenia przedmiotu	Kod przedmiotu
2		3	Egzamin	
Wymagania wstępne w zakresie przedmiotu	Wiedza	1. Podstawowa wiedza z zakresu systemów operacyjnych. 2. Elementarna znajomość popularnych technologii telekomunikacyjnych. 3. Podstawowa wiedza o formatach zapisu danych.		
	Umiejętności	1. Umiejętność obsługi komputera i czytania ze zrozumieniem		
	Kompetencje społeczne	1. Potrafi współdziałać i pracować w grupie.		
Cele przedmiotu: Celem przedmiotu jest zdobycie podstawowej wiedzy i umiejętności w zakresie zabezpieczania i analizy danych z urządzeń mobilnych na potrzeby informatyki śledczej.				
Program przedmiotu				
Forma zajęć	L. godz. zajęć w sem.	Prowadzący zajęcia (tytuł/stopień naukowy, imię i nazwisko)		
Wykład	4	mgr inż. Julian Horoszkiewicz		
Ćwiczenia				
Laboratorium	20	mgr inż. Julian Horoszkiewicz, mgr inż. Marcin Dyda, mgr inż. Jarosław Białoskórski		
Projekt				
Seminarium				
Treści kształcenia				
Wykład		Sposób realizacji	Wykład z wykorzystaniem rzutnika lub na odległość	
Lp.	Tematyka zajęć			Liczba godzin
1.	Definicja, klasyfikacja i rola urządzeń mobilnych. Systemy operacyjne i aplikacje użytkowe urządzeń mobilnych, rodzaje nośników danych, systemy plików. Procedury zabezpieczania nośników urządzeń mobilnych na potrzeby dowodowe.			1
2.	Identyfikacja danych istotnych z punktu widzenia informatyki śledczej. Analiza danych dowodowych.			1
3.	Metody pozyskiwania ulotnych danych. Odzyskiwanie danych ukrytych, usuniętych i zaszyfrowanych.			1
4.	Biały wywiad w zastosowaniu wobec urządzeń mobilnych. Czarny wywiad w zastosowaniu wobec urządzeń mobilnych.			1
5.				
6.				
7.				
8.				

9.					
10.					
Liczba godzin zajęć w semestrze			4		
Laboratorium		Sposób realizacji	ZAJĘCIA PRAKTYCZNE Z KOMPUTEREM		
Lp.	Tematyka zajęć		Liczba godzin		
1.	Wprowadzenie, zapoznanie z listą zadań, sprzętem, oprogramowaniem, zasadami zaliczenia.		2		
2.	Zabezpieczenie i przygotowanie do analizy danych z tradycyjnego telefonu komórkowego.		2		
3.	Identyfikacja danych stanowiących materiał dowodowy na podstawie wcześniej zabezpieczonej kopii.		2		
4.	Analiza pozyskanych w poprzednim ćwiczeniu danych.		2		
5.	Odzyskiwanie danych ulotnych ze smartfona z systemem Android.		3		
6.	Odzyskiwanie usuniętych danych z tradycyjnego telefonu komórkowego.		2		
7.	Odzyskiwanie usuniętych danych ze smartfona z systemem Android.		2		
8.	Odzyskiwanie zaszyfrowanych danych ze smartfona z systemem Android.		2		
9.	Przechwycenie i zabezpieczenie transmisji danych ze smartfona z systemem Android.		3		
Liczba godzin zajęć w semestrze			20		
Efekty kształcenia dla przedmiotu - po zakończonym cyklu kształcenia					
		Odniesienie do kierunkowych efektów kształcenia	Formy realizacji (W, C, L, P, S)		
		Formy weryfikacji efektów kształcenia			
Wiedza	1.	Ma podstawową wiedzę o trendach rozwojowych w informatyce i ich wpływie na bezpieczeństwo systemów i sieci komputerowych.	P_W05	W	A,B
	2.	Zna procedury, zasady oraz specyfikę postępowania z materiałem dowodowym w postaci nośników elektronicznych.	P_W06	W	A,B
	3.	Ma podstawową wiedzę z zakresu analizy danych zapisanych w urządzeniach mobilnych oraz odzyskiwania usuniętych danych.	P_W01	W	A,B
Umiejętności	1.	Ma umiejętność samokształcenia się i wyszukiwania potrzebnych informacji.	P_U04	L	H
	2.	Potrafi wybrać i zastosować odpowiednią metodę i narzędzie odzyskiwania danych.	P_U05	L	H
	3.	Potrafi znaleźć i odczytać dane zgromadzone na urządzeniu mobilnym.	P_U05	L	H
Kompetencje społeczne	1.	Potrafi odpowiednio określić priorytety służące realizacji określonego przez siebie lub innych zadania.	P_K03	L	H
	2.	Prawidłowo identyfikuje i rozstrzyga dylematy związane z wykonywaniem zawodu.	P_K02	L	H
Formy weryfikacji efektów kształcenia:					
A-egzamin pisemny, B-egzamin ustny, C-zaliczenie pisemne, D-zaliczenie ustne, E-na podstawie ocen cząstkowych z odpowiedzi ustnych, F-na podstawie ocen cząstkowych z odpowiedzi pisemnych, G-praca kontrolna, H-ocena ze sprawozdań, I-ocena z przebiegu ćwiczeń, J-ocena z przygotowania do ćwiczeń, K-ocena z przebiegu realizacji projektu, L-ocena pisemnej realizacji projektu, M-ocena z obrony projektu, N-ocena formy prezentacji, O-ocena treści prezentacji, P-observacja aktywności na zajęciach, R-observacja systematyczności.					

Metody dydaktyczne:

Wykład – wykład konwencjonalny, wykład problemowy, dyskusja (wykład prowadzony częściowo z wykorzystaniem metod i technik kształcenia na odległość.)

Laboratorium – metoda zajęć praktycznych (środki: komputery, urządzenia mobilne (telefony komórkowe, smartfony), spreparowane pliki i nośniki – opracowane przez prowadzącego

Forma i warunki zaliczenia przedmiotu:

Wykład – zaliczenie pisemne na ocenę.

Laboratorium – ocena na podstawie ocen cząstkowych z poszczególnych zadań do wykonania. Ocena odzwierciedlająca wiedzę, kreatywność i zdobyte umiejętności techniczne.

Literatura podstawowa:

- [1] Leigland R., *A Formalization of Digital Forensics*, University of Idaho , 2004
- [2] Craiger J. P., *Computer Forensics Procedures and Methods (draft for Handbook of Information Security, Key Concepts, Infrastructure, Standards, and Protocols*, John Wiley and Sons, 2006)
- [3] , CERIAS, Purdue University, West Lafayette [4] Casadei F., Savoldi A., Gubian P., *Forensics and SIM cards: an Overview*, University of Brescia, 2006
- [4] Lessard J., Kessler G.C., *Android Forensics: Simplifying Cell Phone Examinations* , SMALL SCALE DIGITAL DEVICE FORENSICS JOURNAL VOL. 4, NO.1, SEPTEMBER 2010, ISSN# 1941-6164

Literatura uzupełniająca:

- [1] Alessandro Distefano A, Me G., Pace F. *Android anti-forensics through a local paradigm*, Computer Science, Systems and Production Department University of Rome Tor Vergata, Via del Politecnico 1 00133 and IAC-CNR, Istituto per le Applicazioni del Calcolo, Viale Manzoni 30, Rome, Italy
- [2] Peron C.S.J., Legary M., *Digital Anti-Forensics:Emerging trends in data transformation techniques*, Securis Labs, 2005
- [3] Geiger M., *Evaluating Commercial Counter-Forensic Tools*, Carnegie Mellon University, 2006
- [4] Jansen W.A., Delaitre A., *REFERENCE MATERIAL FOR ASSESSING FORENSIC SIM TOOLS*, National Institute of Standards and Technology, Paper No. ICCST 2007-74
- [5] [Hunt A., *Pragmatical Thinking and Learning.*, ISBN-10: 1-934356-05-0, Pragmatic Bookshelf, 2008

* niewłaściwe przekreślić

.....
(kierownik jednostki organizacyjnej/bezpośredni przełożony:
pieczęć/podpis)

.....
(Dziekan Wydziału
pieczęć/podpis)

Politechnika Opolska
Wydział Elektrotechniki, Automatyki i Informatyki

Karta Opisu Przedmiotu

Studia podyplomowe		INFORMATYKA Z ELEMENTAMI INFORMATYKI ŚLEDZCZEJ		
Nazwa przedmiotu		Praca operacyjna z urządzeniami firmy Apple		
Subject Title		Apple devices in operational work		
Semestr		ECTS (pkt)	Tryb zaliczenia przedmiotu	Kod przedmiotu
2		2	Zaliczenie na ocenę	
Wymagania wstępne w zakresie przedmiotu	Wiedza	1. Podstawowa wiedza o systemach operacyjnych komputerów 2. Podstawowa wiedza o urządzeniach mobilnych 3. Znajomość problematyki związanej z sieciami komputerowymi, w tym sieciami bezprzewodowymi		
	Umiejętności	1. Potrafi sprawnie posługiwać się komputerem i jego systemem operacyjnym 2. Umie wykorzystać urządzenie mobilne w podstawowym zakresie		
	Kompetencje społeczne	1. Potrafi współdziałać i pracować w grupie		
Cele przedmiotu: Celem przedmiotu jest zdobycie podstawowej wiedzy i umiejętności w zakresie obsługi urządzeń firmy Apple, w tym zarządzania tymi urządzeniami.				
Program przedmiotu				
Forma zajęć	L. godz. zajęć w sem.	Prowadzący zajęcia (tytuł/stopień naukowy, imię i nazwisko)		
Wykład	8	dr inż. Michał Podpora		
Ćwiczenia				
Laboratorium	10	dr inż. Michał Podpora		
Projekt				
Seminarium				
Treści kształcenia				
Wykład		Sposób realizacji	Wykład w sali lub kształcenie na odległość	
Lp.	Tematyka zajęć			Liczba godzin
1.	Budowa systemu OS X, konta użytkowników.			1
2.	System uprawnień do plików na dysku systemowym, bezpieczeństwo danych na dysku.			0,5
3.	Instalacja i podstawowe usługi OS X Server.			1
4.	Profile urządzeń, użytkowników, grup i grup urządzeń.			0,5
5.	Zarządzanie profilami i instalacja profili na urządzeniu.			1
6.	System iOS, jego podstawowe cechy użytkowe.			0,5
7.	Zarządzanie urządzeniem mobilnym Apple za pomocą programu iTunes.			1
8.	Wykorzystanie programu Apple Configurator do zarządzania urządzeniami mobilnymi.			0,5
9.	Wykorzystanie OS X Server do zarządzania urządzeniami mobilnymi.			1
10.	Bezpieczeństwo danych na urządzeniach mobilnych Apple. Zaliczenie przedmiotu.			1
Liczba godzin zajęć w semestrze				8

Laboratorium		Sposób realizacji	
Lp.	Tematyka zajęć		Liczba godzin
1.	Konfiguracja i użytkowanie OS X, tworzenie kont użytkowników		1
2.	Zmiana uprawnień do plików. Praca z dyskami szyfrowanymi.		1
3.	Instalacja i konfiguracja OS X Server w celu budowy serwera zarządzającego urządzeniami i użytkownikami.		1
4.	Profile Manager i tworzenie różnych profili.		1
5.	Instalacja profilu na urządzeniu, uaktualnienie i usunięcie profilu.		1
6.	Konfiguracja urządzenia z iOS, Apple ID i korzystanie z iTunes Store.		1
7.	iTunes, jako program zarządzający urządzeniem – backup, synchronizacja danych.		1
8.	Przygotowanie i zainstalowanie konfiguracji urządzeń za pomocą Apple Configurator.		1
9.	Tworzenie profili urządzeń w Profile Manager, instalacja na urządzeniu.		1
10.	Porównanie różnych metod zarządzania urządzeniami mobilnymi.		1
Liczba godzin zajęć w semestrze			10

Efekty kształcenia dla przedmiotu - po zakończonym cyklu kształcenia		Odniesienie do kierunkowych efektów kształcenia	Formy realizacji (W, C, L, P, S)	Formy weryfikacji efektów kształcenia	
Wiedza	1.	Ma wiedzę dotyczącą budowy systemu OS X oraz iOS.	P_W01	W	C,D
	2.	Zna podstawowe metody zarządzania urządzeniami i użytkownikami.	P_W01	W	C,D
Umiejętności	1.	Potrafi wybrać i zastosować odpowiednią metodę zarządzania urządzeniem lub użytkownikiem	P_U05	L	H
	2.	Potrafi użyć programów do zarządzania urządzeniami	P_U01	L	H
Kompetencje społeczne	1.	Potrafi współdziałać i pracować w grupie, przyjmując w niej różne role.	P_K03	L	H

Formy weryfikacji efektów kształcenia:

A-egzamin pisemny, B-egzamin ustny, C-zaliczenie pisemne, D-zaliczenie ustne, E-na podstawie ocen cząstkowych z odpowiedzi ustnych, F-na podstawie ocen cząstkowych z odpowiedzi pisemnych, G-praca kontrolna, H-ocena ze sprawozdań, I-ocena z przebiegu ćwiczeń, J-ocena z przygotowania do ćwiczeń, K-ocena z przebiegu realizacji projektu, L-ocena pisemnej realizacji projektu, M-ocena z obrony projektu, N-ocena formy prezentacji, O-ocena treści prezentacji, P-observacja aktywności na zajęciach, R-observacja systematyczności.

Metody dydaktyczne:

Wykład – wykład konwencjonalny, wykład problemowy, dyskusja (wykład prowadzony częściowo z wykorzystaniem metod i technik kształcenia na odległość.)

Laboratorium – metoda zajęć praktycznych (środki: komputer, urządzenia mobilne).

Forma i warunki zaliczenia przedmiotu:

Wykład – zaliczenie ustne na ocenę. Laboratorium – ocena na podstawie ocen cząstkowych z poszczególnych zajęć.

Literatura podstawowa:

[1] <http://krypted.com/mac-os-x-server/a-guide-to-using-mac-os-x-server-10-8/>

[2] [2] <http://arstechnica.com/apple/2012/07/the-server-simplified-a-power-users-guide-to-os-x-server/>

Literatura uzupełniająca:

[1] Kevin White, Gordon Davisson, *OS X Support Essentials* ISBN: 9780133156126, Pearson Education, 2012

[2] [2] Arek Dreyer, Ben Greisler, *OS X Server Essentials: Using and Supporting OS X Server on Mountain Lion* ISBN: 9780133156690, Pearson Education, 2012

* niewłaściwe przekreślić

.....
(kierownik jednostki organizacyjnej/bezpośredni przełożony:
pieczęć/podpis)

.....
(Dziekan Wydziału
pieczęć/podpis)

Politechnika Opolska
Wydział Elektrotechniki, Automatyki i Informatyki

Karta Opisu Przedmiotu

Studia podyplomowe		INFORMATYKA ŚLEDZCA	
Nazwa przedmiotu		Kryptografia i steganografia	
Subject Title		Cryptography and Steganography	
Semestr	ECTS (pkt)	Tryb zaliczenia przedmiotu	Kod przedmiotu
2	3	Egzamin	
Wymagania wstępne w zakresie przedmiotu	Wiedza	1. Podstawowa wiedza z zakresu technologii informacji	
	Umiejętności	1. Potrafi obsługiwać komputer i system operacyjny	
	Kompetencje społeczne	1. Potrafi współdziałać i pracować w grupie	
Cele przedmiotu: Celem przedmiotu jest zdobycie podstawowej wiedzy i umiejętności w zakresie rozpoznawania wybranych typów szyfrów i typów kodowania informacji oraz podstawowych umiejętności w zakresie kryptoanalizy i steganalizy.			
Program przedmiotu			
Forma zajęć	L. godz. zajęć w sem.	Prowadzący zajęcia (tytuł/stopień naukowy, imię i nazwisko)	
Wykład	10	mgr inż. Artur Kalinowski	
Ćwiczenia			
Laboratorium	15	mgr inż. Artur Kalinowski	
Projekt			
Seminarium			
Treści kształcenia			
Wykład		Sposób realizacji	Kształcenie na odległość
Lp.	Tematyka zajęć		Liczba godzin
1.	Pojęcie kryptografii i steganografii		1
2.	Różnice między szyfrowaniem a kodowaniem informacji		1
3.	Przegląd popularnych algorytmów szyfrowania		1
4.	Jednokierunkowe funkcje skrótu jako element zwiększający bezpieczeństwo		1
5.	Kodowanie i szyfrowanie danych jako element zabezpieczeń		1
6.	Podstawowe metody kryptoanalizy		1
7.	Szyfrowanie asymetryczne i metoda ataku		1
8.	Steganografia z wykorzystaniem plików tekstowych		1
9.	Steganografia z wykorzystaniem plików binarnych		1
10.	Steganaliza (ujawnianie ukrytych danych) Zaliczenie przedmiotu.		1

Liczba godzin zajęć w semestrze		10
Laboratorium	Sposób realizacji	
Lp.	Tematyka zajęć	Liczba godzin
1.	Wykorzystanie standardowych funkcji kryptograficznych systemu operacyjnego i aplikacji	2
2.	Kodowanie i dekodowanie informacji, rozpoznawanie typów funkcji skrótu oraz metod szyfrowania	2
3.	Generowanie tęczowych tablic i wykorzystywanie baz skrótów (hash)	2
4.	Łamanie haseł zaszyfrowanych archiwów z wykorzystaniem systemu Linux	2
5.	Ujawnianie treści zakodowanej strony oraz zakodowanych danych w pliku cookies celem modyfikacji i podniesienia uprawnień	2
6.	Wybrane metody szyfrowania i ataków na szyfrogramy	1
7.	Test Kasiskiego	1
8.	Ukrywanie danych tekstowych i binarnych w plikach tekstowych	1
9.	Ukrywanie danych tekstowych i binarnych w plikach binarnych	1
10.	Analiza LSB jako technika ujawniania zakamuflowanych danych	1
Liczba godzin zajęć w semestrze		15

Efekty kształcenia dla przedmiotu - po zakończonym cyklu kształcenia		Odniesienie do kierunkowych efektów kształcenia	Formy realizacji (W, C, L, P, S)	Formy weryfikacji efektów kształcenia
Wiedza	1. Zna podstawowe metody, techniki, narzędzia i materiały stosowane przy rozwiązywaniu prostych zadań inżynierskich z zakresu kryptografii, kryptoanalizy oraz steganografii	P_W03	W	A,B
	2. Zna i rozumie podstawowe pojęcia i zasady z zakresu ochrony danych	P_W01	W	A.B
Umiejętności	1. Ma umiejętność samokształcenia się i wyszukiwania potrzebnych informacji	P_U04	W,L	H
	2. Potrafi pozyskiwać i analizować dane, oraz interpretować otrzymane wyniki	P_U06	L	H
Kompetencje społeczne	1. Potrafi współdziałać i pracować w grupie, przyjmując w niej różne role.	P_K03	L	H
	2. Potrafi odpowiednio określić priorytety służące realizacji określonego przez siebie lub innych zadania.	P_K03	L	H

Formy weryfikacji efektów kształcenia:
A-egzamin pisemny, B-egzamin ustny, C-zaliczenie pisemne, D-zaliczenie ustne, E-na podstawie ocen cząstkowych z odpowiedzi ustnych, F-na podstawie ocen cząstkowych z odpowiedzi pisemnych, G-praca kontrolna, H-ocena ze sprawozdań, I-ocena z przebiegu ćwiczeń, J-ocena z przygotowania do ćwiczeń, K-ocena z przebiegu realizacji projektu, L-ocena pisemnej realizacji projektu, M-ocena z obrony projektu, N-ocena formy prezentacji, O-ocena treści prezentacji, P-observacja aktywności na zajęciach, R-observacja systematyczności.

Metody dydaktyczne:

Wykład – wykład konwencjonalny, wykład problemowy, dyskusja (wykład może być prowadzony z wykorzystaniem metod i technik kształcenia na odległość.)

Laboratorium – metoda laboratoryjna problemowa, metoda zajęć praktycznych (środki: komputery, spreparowane pliki opracowane przez prowadzącego).

Forma i warunki zaliczenia przedmiotu:

Wykład – zaliczenie pisemne na ocenę.

Laboratorium – ocena na podstawie ocen cząstkowych z poszczególnych zadań do wykonania. Ocena odzwierciedlająca wiedzę, kreatywność i zdobyte umiejętności techniczne.

Literatura podstawowa:

- [1] Karbowski M., *Podstawy kryptografii*. ISBN: 978-83-246-1215-4, Helion, 2007
- [2] Pieprzyk J., Hardjono T., Seberry J., *Teoria bezpieczeństwa systemów komputerowych.*, ISBN: 83-7361-678-0, Helion, 2005
- [3] Stallings W., *Kryptografia i bezpieczeństwo sieci komputerowych. Matematyka szyfrów i techniki kryptologii.*, ISBN: 978-83-246-2986-2, 2011

Literatura uzupełniająca:

* niewłaściwe przekreślić

.....
(kierownik jednostki organizacyjnej/bezpośredni przełożony:
pieczęć/podpis)

.....
(Dziekan Wydziału
pieczęć/podpis)

Politechnika Opolska
Wydział Elektrotechniki, Automatyki i Informatyki

Karta Opisu Przedmiotu

Studia podyplomowe		INFORMATYKA Z ELEMENTAMI INFORMATYKI ŚLEDZCZEJ	
Nazwa przedmiotu		Pozyskiwanie danych z systemów mikroprocesorowych	
Subject Title		Data recovery from microprocessors systems	
Semestr	ECTS (pkt)	Tryb zaliczenia przedmiotu	Kod przedmiotu
2	1	Zaliczenie na ocenę	
Wymagania wstępne w zakresie przedmiotu	Wiedza	1. Podstawowa wiedza z zakresu technologii informacyjnej	
	Umiejętności	1. W podstawowym zakresie potrafi obsługiwać system operacyjny Windows	
	Kompetencje społeczne	1. Potrafi współdziałać i pracować w grupie	
Cele przedmiotu: Celem przedmiotu jest zdobycie podstawowej wiedzy i umiejętności w zakresie odzyskiwania i zabezpieczania danych w systemach mikroprocesorowych			
Program przedmiotu			
Forma zajęć	L. godz. zajęć w sem.	Prowadzący zajęcia (tytuł/stopień naukowy, imię i nazwisko)	
Wykład	6	Dr hab inż. Mirosław Szmajda, prof. PO	
Ćwiczenia			
Laboratorium	6	dr inż. Krzysztof Górecki	
Projekt			
Seminarium			
Treści kształcenia			
Wykład		Sposób realizacji	Kształcenie na odległość
Lp.	Tematyka zajęć		Liczba godzin
1.	Wprowadzenie do techniki mikroprocesorowej		2
2.	Wprowadzenie do języka assembler		2
3.	Inżynieria odwrotna		2
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			

13.					
14.					
15.					
Liczba godzin zajęć w semestrze			6		
Laboratorium		Sposób realizacji	Zajęcia praktyczne		
Lp.	Tematyka zajęć		Liczba godzin		
1.	Wprowadzenie do środowiska programistycznego		1		
2.	Przykład programowania w języku asembler		2		
3.	Deasemblacja.		1		
4.	Zabezpieczenia przeciw inżynierii odwrotnej		2		
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					
15.					
Liczba godzin zajęć w semestrze			6		
Efekty kształcenia dla przedmiotu - po zakończonym cyklu kształcenia			Odniesienie do kierunkowych efektów kształcenia Formy realizacji (W, C, L, P, S) Formy weryfikacji efektów kształcenia		
Wiedza	1.	Posiada wiedzę w zakresie ochrony danych w systemach mikroprocesorowych	P_W01	W	D
	2.				
	3.				
	...				
Umiejętności	1.	Potrafi pozyskiwać informacje z literatury, baz danych oraz innych właściwie dobranych źródeł, także w języku obcym w zakresie informatyki, a także integrować uzyskane informacje, dokonywać ich analizy i interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie.	P_U01	L	H
	2.	Potrafi posługiwać się technikami, narzędziami właściwymi do realizacji zadań związanych z ochroną danych w systemach mikroprocesorowych.	PU_05	W, L	D, I
	3.				
	...				
Kompetencje społeczne	1.	Rozumie konieczność przestrzegania zasad etyki zawodowej i konkurencji.	P_K02	W, L	D
	2.				
	3.				
	...				

Formy weryfikacji efektów kształcenia:

A-egzamin pisemny, B-egzamin ustny, C-zaliczenie pisemne, D-zaliczenie ustne, E-na podstawie ocen częściowych z odpowiedzi ustnych, F-na podstawie ocen częściowych z odpowiedzi pisemnych, G-praca kontrolna, H-ocena ze sprawozdań, I-ocena z przebiegu ćwiczeń, J-ocena z przygotowania do ćwiczeń, K-ocena z przebiegu realizacji projektu, L-ocena pisemnej realizacji projektu, M-ocena z obrony projektu, N-ocena formy prezentacji, O-ocena treści prezentacji, P-observacja aktywności na zajęciach, R-observacja systematyczności.

Metody dydaktyczne:

Wykład – wykład konwencjonalny i dyskusja, prowadzone z wykorzystaniem modułów startowych, wyposażonych w mikroprocesory.

Laboratorium – metoda zajęć praktycznych (środki: komputery, moduły startowe z mikroprocesorami, spreparowane pliki).

Forma i warunki zaliczenia przedmiotu:

Wykład – zaliczenie ustne na ocenę. Laboratorium – ocena na podstawie ocen cząstkowych z poszczególnych zadań do wykonania. Ocena odzwierciedlająca wiedzę, kreatywność i zdobyte umiejętności techniczne.

Literatura podstawowa:

- [1] MSP430 Teaching ROM
- [2] HADAM P.: Projektowanie systemów mikroprocesorowych. Wyd. BTC, 2004.
- [3] BORKOWSKI P. AVR&ARM7, programowanie mikrokontrolerów. Wyd. Helion, 2010.
- [4] KALISZ J.: Podstawy elektroniki cyfrowej, WKiŁ, Warszawa 2007.

Literatura uzupełniająca:

- [1] DAVIES J. H.: MSP430 Microcontroller Basics. Elsevier 2008.
- [2] <http://www.easy-soft.net.pl/artykuly/techniki-technologie-dla-elektronikow/atak-na-mikrokontrolery>

* niewłaściwe przekreślić

.....
(kierownik jednostki organizacyjnej/bezpośredni przełożony:
pieczęć/podpis)

.....
(Dziekan Wydziału
pieczęć/podpis)

Politechnika Opolska
Wydział Elektrotechniki, Automatyki i Informatyki

Karta Opisu Przedmiotu

Studia podyplomowe		INFORMATYKA ŚLEDZCA		
Nazwa przedmiotu		Techniki pozyskiwania danych		
Subject Title		Data Mining		
Semestr	ECTS (pkt)	Tryb zaliczenia przedmiotu	Kod przedmiotu	
2	2	Zaliczenie na ocenę		
Wymagania wstępne w zakresie przedmiotu	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		
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.				
Program przedmiotu				
Forma zajęć	L. godz. zajęć w sem.	Prowadzący zajęcia (tytuł/stopień naukowy, imię i nazwisko)		
Wykład	8	prof. dr hab. inż. Volodymyr Khoma		
Ćwiczenia				
Laboratorium	11	mgr inż. Tomasz Turba		
Projekt				
Seminarium				
Treści kształcenia				
Wykład		Sposób realizacji	Wykład w sali audytorijnej lub kształcenie na odległość	
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			1
5.	Technologii Firewall, IDS, Honey Pot, ochrona antywirusowa jako przykłady legalnych metod pozyskiwania danych			1
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			1

	Mining				
8.	Zaliczenie przedmiotu			1	
Liczba godzin zajęć w semestrze				8	
Laboratorium		Sposób realizacji			
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			1	
4.	Eksploracja danych w sieciach komputerowych: systemy IDS/IPS, analiza kontekstowa proxy ochrona przed atakami DOS/DDOS, ochrona antywirusowa			1	
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			1	
9.	Zaliczenie przedmiotu			1	
Liczba godzin zajęć w semestrze				11	
Efekty kształcenia dla przedmiotu - po zakończonym cyklu kształcenia					
				Odniesienie do kierunkowych efektów kształcenia	
				Formy realizacji (W, C, L, P, S)	
				Formy weryfikacji efektów kształcenia	
Wiedza	1.	Zna podstawowe metody i techniki pozyskiwania i ochrony danych	P_W04	W	C,D
Umiejętności	1.	Potrafi wykonywać analizę danych z wykorzystaniem technik i metod signals intelligence oraz data mining	P_U06	L	H
Kompetencje społeczne	1.	Potrafi współdziałać i pracować w grupie, przyjmując w niej różne role	P_K03	L	H
Formy weryfikacji efektów kształcenia:					
A-egzamin pisemny, B-egzamin ustny, C-zaliczenie pisemne, D-zaliczenie ustne, E-na podstawie ocen cząstkowych z odpowiedzi ustnych, F-na podstawie ocen cząstkowych z odpowiedzi pisemnych, G-praca kontrolna, H-ocena ze sprawozdań, I-ocena z przebiegu ćwiczeń, J-ocena z przygotowania do ćwiczeń, K-ocena z przebiegu realizacji projektu, L-ocena pisemnej realizacji projektu, M-ocena z obrony projektu, N-ocena formy prezentacji, O-ocena treści prezentacji, P-observacja aktywności na zajęciach, R-observacja systematyczności.					

Metody dydaktyczne:

Wykład – wykład konwencjonalny, wykład problemowy, dyskusja (wykład prowadzony częściowo z wykorzystaniem metod i technik kształcenia na odległość.)

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.

.....
(kierownik jednostki organizacyjnej/bezpośredni przełożony:
pieczęć/podpis)

.....
(Dziekan Wydziału
pieczęć/podpis)

Politechnika Opolska
Wydział Elektrotechniki, Automatyki i Informatyki

Karta Opisu Przedmiotu

Studia podyplomowe		INFORMATYKA ŚLEDZCA		
Nazwa przedmiotu		Praca końcowa		
Subject Title		Final Project		
Semestr		ECTS (pkt)	Tryb zaliczenia przedmiotu	Kod przedmiotu
2		4	Zaliczenie na ocenę	
Wymagania wstępne w zakresie przedmiotu	Wiedza	Ma uporządkowaną, ogólną wiedzę dotyczącą wybranych zagadnień z obszaru studiowanego kierunku studiów i dobre przygotowanie w zakresie języka polskiego.		
	Umiejętności	Potrafi posługiwać się technikami i narzędziami naukowo-inżynierskimi do rozwiązywania zadań z zakresu informatyki śledczej.		
	Kompetencje społeczne	Potrafi odpowiednio określić priorytety służące rozwiązywaniu zadań. Rozumie potrzebę ciągłego pogłębiania wiedzy,		
Cele przedmiotu: Pogłębienie umiejętności przygotowania i redagowania zwartych prac zwartych.				
Program przedmiotu				
Forma zajęć	L. godz. zajęć w sem.	Prowadzący zajęcia (tytuł/stopień naukowy, imię i nazwisko)		
Wykład				
Ćwiczenia				
Laboratorium				
Projekt				
Seminarium	20	Dr hab. inż. Jan Sadecki, prof. PO, dr inż. Aleksandra Kawala		
Treści kształcenia				
Seminarium		Sposób realizacji	Zajęcia projektowe, dyskusja w grupie z wykorzystaniem projektora multimedialnego	
Lp.	Tematyka zajęć			Liczba godzin
1.	Wybór obszaru tematycznego pracy końcowej i sformułowanie tematu. Metodyka pracy koncepcyjnej.			4
2.	Omówienie różnych form pracy końcowej, ogólna systematyka, cechy charakterystyczne poszczególnych prac końcowych. Sposób cytowania literatury.			3
3.	Praca studialna: wymagania merytoryczne, sposób jej pisania, cytowania, analiza danych literaturowych.			2
4.	Praca końcowa badawcza: metodyka i zakres badań, opis stanowiska badawczego, analiza i opis rezultatów.			2
5.	Praca końcowa projektowa: wstępne rozeznanie literaturowe, koncepcja projektu (technologia, urządzenia). Opis projektu, propozycja dokumentacji.			2
6.	Sposób realizacji czynności operacyjnych w kontekście eksperymentów pomiarowo-doświadczalnych.			3
7.	Aproksymacja danych doświadczalnych. Wnioskowanie na podstawie danych doświadczalnych.			2
8.	Analiza ekonomiczna. Ocena ewentualnych kosztów inwestycyjnych i eksploatacyjnych.			2

Liczba godzin zajęć w semestrze				20	
Efekty kształcenia dla przedmiotu - po zakończonym cyklu kształcenia			Odniesienie do kierunkowych efektów kształcenia	Formy realizacji (W, C, L, P, S)	Formy weryfikacji efektów kształcenia
Wiedza	1.	Posiada wiedzę związaną z prezentacją trendów i osiągnięć	P_W06	S	L,M,N,O
	Umiejętności	1.	Potrafi wykorzystywać nabytą metodologię, terminologię i techniki podczas pisania pracy.	P_U01	S
2.		Potrafi przygotować, redagować i prezentować zwarte prace	P_U01	S	L,M,N,O
Kompetencje społeczne	1.	Rozumie potrzebę ciągłego pogłębiania wiedzy	P_K01	S	L,M,N,O
	2.	Potrafi odpowiednio określić priorytety służące realizacji określonego przez siebie lub innych zadania	P_K03	S	L,M,N,O
Formy weryfikacji efektów kształcenia: A-egzamin pisemny, B-egzamin ustny, C-zaliczenie pisemne, D-zaliczenie ustne, E-na podstawie ocen cząstkowych z odpowiedzi ustnych, F-na podstawie ocen cząstkowych z odpowiedzi pisemnych, G-praca kontrolna, H-ocena ze sprawozdań, I-ocena z przebiegu ćwiczeń, J-ocena z przygotowania do ćwiczeń, K-ocena z przebiegu realizacji projektu, L-ocena pisemnej realizacji projektu, M-ocena z obrony projektu, N-ocena formy prezentacji, O-ocena treści prezentacji, P-observacja aktywności na zajęciach, R-observacja systematyczności.					

Metody dydaktyczne:

Referowanie opracowanego materiału. Praca koncepcyjna i problemowa. Zastosowanie metod kształcenia na odległość.

Definiowanie pojęć, twórcze rozwiązywanie problemów, metody aktywizujące (dyskusje, projekty i inne).

Forma i warunki zaliczenia przedmiotu:

Przygotowanie pracy końcowej oraz jej prezentacja.

Literatura podstawowa:

- [1] K. Wójcik; Poradnik dla autorów akademickich prac promocyjnych (licencjackich, magisterskich, doktorskich); Oficyna Wydawnicza SGH, Warszawa 2002.

[2]

Literatura uzupełniająca:

- [1] Kreatywna praca dyplomowa. Jak stworzyć fascynujący tekst naukowy; Joanna Wrycza-Bekier, Helion, ISBN: 978-83-246-3351-7

* niewłaściwe przekreślić

.....
(kierownik jednostki organizacyjnej/bezpośredni przełożony:
pieczęć/podpis)

.....
(Dziekan Wydziału
pieczęć/podpis)