KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Informatyka śledcza [S2Inf1E-CYB>DIGF]

Przedmiot

Kierunek studiów
Informatyka/Computing

Rok/Semestr
1/1

Studia w zakresie (specjalność)
Cyberbezpieczeństwo

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
angielski

Forma studiów
stacjonarne

Wymagalność
obligatoryjny

Liczba godzin

Wykład
15

Laboratorium
0

Inne
0

Ćwiczenia
0

Projekty/seminaria
0

Liczba punktów ECTS

1,00

Koordynatorzy

dr inż. Michał Weissenberg
michal.weissenberg@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student rozpoczynający ten kurs powinien posiadać podstawową wiedzę z zakresu cyberbezpieczeństwa, sieci teleinformatycznych oraz posiadać podstawowe umiejętności programowania. Powinien także posiadać umiejętność pozyskiwania informacji ze wskazanych źródeł. Student powinien wykazywać takie cechy jak uczciwość, odpowiedzialność, wytrwałość, ciekawość poznawcza, kreatywność, kultura osobista, szacunek dla drugiego człowieka. Student powinien wykazywać takie cechy jak uczciwość, odpowiedzialność, wytrwałość, ciekawość poznawcza, kreatywność, kultura osobista, szacunek dla drugiego człowieka oraz gotowość do pracy w grupie.

Cel przedmiotu

1. Zapewnienie studentom teoretycznych podstaw dotyczących kryminalistyki cyfrowej. 2. Zapoznanie studentów z teoretycznymi informacjami na temat cyberprzestępczości, zbierania dowodów i gromadzenia danych. 3. Zapoznanie studentów z typowymi narzędziami stosowanymi w kryminalistyce cyfrowej oraz metodami analizy najpopularniejszych systemów operacyjnych. 4. Przedstawienie studentom społecznych, etycznych i prawnych aspektów cyberprzestępczości.

Przedmiotowe efekty uczenia się

Wiedza:
student posiada uporządkowaną i podbudowaną teoretycznie wiedzę ogólną dotyczącą kluczowych zagadnień z zakresu informatyki, w tym analizy systemów operacyjnych. [k2st_w2]
student ma zaawansowaną wiedzę szczegółową dotyczącą wybranych zagadnień informatycznych i ich zastosowań w kryminalistyce cyfrowej. [k2st_w3]
student zna trendy i najważniejsze osiągnięcia w informatyce, w szczególności w obszarze kryminalistyki cyfrowej. [k2st_w4]
student zna podstawowe programy i aplikacje służące do gromadzenia danych i ich analizy w procesie śledztwa kryminalistycznego. [k2st_w6]

Umiejętności:
student potrafi ocenić przydatność i możliwość wykorzystania informacji uzyskanych w analizie literatury i dostępnych w internecie w obszarze kryminalistyki cyfrowej. [k2st_u1]
student potrafi ocenić przydatność i możliwość wykorzystania nowych osiągnięć (metod i narzędzi) oraz nowych produktów informatycznych z zakresu kryminalistyki cyfrowej. [k2st_u6]
student potrafi ocenić przydatność oraz możliwość wykorzystania i rozwijania podstawowych narzędzi stosowanych w kryminalistyce cyfrowej. [k2st_u8]
student zna podstawowe pojęcia z zakresu kryminalistyki cyfrowej i potrafi je wykorzystać do opisu procesu postępowania kryminalistycznego. [k2_u12]
student potrafi definiować etapy dalszego zdobywania wiedzy z zakresu kryminalistyki cyfrowej, a także pozyskiwać informacje na ten temat oraz realizować proces samokształcenia, w tym innych osób w tym zakresie. [k2_u16]

Kompetencje społeczne:
student rozumie, że w zakresie it, cyberbezpieczeństwa i kryminalistyki cyfrowej wiedza i umiejętności szybko się dezaktualizują. [k2st_k1]
student rozumie znaczenie wykorzystania najnowszej wiedzy z zakresu informatyki, cyberbezpieczeństwa i kryminalistyki cyfrowej w rozwiązywaniu problemów badawczych i praktycznych. [k2st_k2]
student rozumie znaczenie działań popularyzatorskich dotyczących najnowszych osiągnięć w dziedzinie kryminalistyki cyfrowej. [k2st_k3]
student ma świadomość konieczności rozwijania dorobku zawodowego i przestrzegania zasad etyki zawodowej. [k2st_k4]

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wykład: wiedza jest weryfikowana poprzez test pisemny i/lub ustny. Ocena zaliczeniowa wynosi 51% punktów, a podczas testu nie wolno używać żadnych materiałów pomocniczych.

Treści programowe

Wykład:
1. Wstęp – pojęcia, definicje i czynności z zakresu kryminalistyki.
2. Cyfrowa kryminalistyka - prezentacja czym jest kryminalistyka cyfrowa i artefakty cyfrowe.
3. Cyberprzestępczość i dowody – podstawowa wiedza o cyberprzestępczości, reagowaniu na incydenty, zbieraniu dowodów i analizie danych.
4. Zbieranie danych - najważniejsze informacje o indeksowaniu, wyszukiwaniu, łamaniu i znajdowaniu artefaktów.
5. Narzędzia - opisujące narzędzia wolnego dostępu.
6. Analiza pamięci i analiza złośliwego oprogramowania.
7. Cyfrowe dowody dotyczące różnych systemów operacyjnych.
8. Kryminalistyka sieciowa.

Tematyka zajęć

Wykład:
1. Wstęp – pojęcia, definicje i czynności z zakresu kryminalistyki.
2. Cyfrowa kryminalistyka - prezentacja czym jest kryminalistyka cyfrowa i artefakty cyfrowe.
3. Cyberprzestępczość i dowody – podstawowa wiedza o cyberprzestępczości, reagowaniu na incydenty,

zbieraniu dowodów i analizie danych.
4. Zbieranie danych - najważniejsze informacje o indeksowaniu, wyszukiwaniu, łamaniu i znajdowaniu artefaktów.
5. Narzędzia - opisujące narzędzia wolnego dostępu.
6. Analiza pamięci i analiza złośliwego oprogramowania.
7. Cyfrowe dowody dotyczące różnych systemów operacyjnych.
8. Kryminalistyka sieciowa.

Metody dydaktyczne

1. Wykłady: prezentacje multimedialne ilustrowane przykładami.

Literatura

Podstawowa
J. Kavrestad, "Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications", Springer, 2nd Edition, 2020
A. Arnes, "Digital Forensics", Willey, 2018
E. Casey, "Digital Evidence and Computer Crime", Academic Press, 3rd Edition, 2011
T. J. Holt, A. M. Bossler, K. C Seigfried-Spellar, "Cybercrime and Digital Forensics," Routledge, 2018.
Dz. U. 2018 poz. 1560, Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa
Uzupełniająca
N. A. Hassan, "Digital Forensics Basics. A practical guide using Windows OS", Apress, 2019
W. Oettinger, "Learn Computer Forensics: a beginner"s guide to searching, analyzing, and securing digital evidence", Packt Publishing, 2020

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	25	1,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	15	0,50
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	10	0,50