KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Informatyka śledcza [S1Cybez1>INFŚ]

Przedmiot

Kierunek studiów
Cyberbezpieczeństwo

Rok/Semestr
2/4

Studia w zakresie (specjalność)
–

Profil studiów
ogólnoakademicki

Poziom studiów
pierwszego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obligatoryjny

Liczba godzin

Wykład
8

Laboratorium
16

Inne
0

Ćwiczenia
0

Projekty/seminaria
0

Liczba punktów ECTS

2,00

Koordynatorzy

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

Wykładowcy

Wymagania wstępne

• Podstawowa wiedza z zakresu bezpieczeństwa systemów informatycznych. • Znajomość systemów operacyjnych (Windows, Linux) na poziomie użytkownika zaawansowanego. • Zrozumienie podstaw sieci komputerowych.

Cel przedmiotu

Celem przedmiotu jest zapoznanie studentów z metodami i technikami wykorzystywanymi w informatyce śledczej, w tym gromadzeniem, analizą i interpretacją dowodów cyfrowych. Studenci nauczą się stosować narzędzia informatyki śledczej w sposób zgodny z przepisami prawa oraz poznają procesy wykorzystywane w dochodzeniach cyberprzestępczych.

Przedmiotowe efekty uczenia się

Wiedza:
• Zna podstawowe pojęcia i zasady informatyki śledczej.[K1_W22]
• Rozumie procesy gromadzenia, zabezpieczania i analizy dowodów cyfrowych. [K1_W05]
• Rozumie wymagania prawne dotyczące prowadzenia działań śledczych w środowisku cyfrowym. [K1_W17]

Umiejętności:
• Potrafi zidentyfikować i zabezpieczyć dowody cyfrowe w sposób zgodny z obowiązującymi standardami. [K1_U03]
• Umie diagnozować problemy i analizować je przy pomocy narzędzi informatycznych. [K1_U09]
• Potrafi rozwiązywać problemy kryminalistyczne z wykorzystaniem wybranych narzędzi informatycznych. [K1_U02]
• Potrafi przygotować raporty ze śledztwa cyfrowego, które mogą być wykorzystywane w postępowaniach prawnych. [K1_U04]

Kompetencje społeczne:
• Rozumie znaczenie etycznego podejścia w informatyce śledczej i przestrzega zasad poufności oraz integralności danych. [K1_K05]
• Potrafi pracować w grupie, przedstawiając wnioski w sposób jasny i zrozumiały. [K1_K05]
• Rozumie znaczenie kryminalistyki cyfrowej i zagrożenia płynące z cyberprzestępczości w ujęciu społecznym. [K1_K03]

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:
Wykład:
Wiedza zdobyta w ramach wykładu weryfikowana jest przez test w formie (1) pisemnej lub (2) ustnej. W formie pisemnej studenci muszą udzielić odpowiedzi na 3 - 5 pytań (testowych i otwartych) różnie punktowanych.
W formie ustnej student najpierw losuje 2 grupy tematyczne z pośród 3 głównych tematów podejmowanych w części wykładowej, a następnie w każdej grupie losuej 1 pytanie. Do każdego wylosowanego pytania, student może otrzymać dodatkowe pytanie (związane z wylosowanym pytaniem). Ocena pytania (obejmuje odpowiedź zarówno na pytanie wylosowane jak i pytanie dodatkowe) obejmuje zakres odpowiedzi oraz głębię zrozumienia zagadnienia.
Laboratorium:
Umiejętności nabyte w ramach laboratorium będą weryfikowane każdorazowo podczas zajęć na podstawie przydzielonych zadań lub projektów obejmujących wykorzystanie narzędzi w ramach studium przypadków.
Skala ocen dla częsci wykładowej i laboraoryjnej:
W obu formach dydaktycznych przyjmuje się próg zaliczeniowy wynoszący 50% możliwych do zdobycia punktów. Stosuje się następującą skalę ocen: < 50% 2.0; 50%-59% 3.0; 60%-69% 3.5; 70%-79% 4.0; 80%-
89% 4.5; 90%-100% 5.0.
Zasady zaliczania przedmiotu i dokładne progi zaliczeniowe zostaną przekazane studentom na początku semestru z wykorzystaniem uczelnianych systemów elektronicznych oraz na pierwszych zajęciach (w każdej formie zajęć).

Treści programowe

W trakcie semestru studenci poznają podstawowe pojęcia, definicje i czynności z zakresu informatyki śledczej, ze szczególną uwagą kryminalistyki cyfrowej. Pozyskają teoretyczną i praktyczną wiedzę z zakresu cyberprzestępczości oraz pozyskiwania i analizy artefaktów cyfrowych w procesie dochodzenia kryminalistycznego. Przedstawione zostaną narzędzia wspierające proces identyfikacji, indeksowania, kopiowania a także tworzenia cyfrowych odcisków palców dla dowodów cyfrowych, a także narzędzia umożliwiające automatyzację procesu analizy dowodów cyfrowych. Studenci zdobędą wiedzę z zakresu realizacji wywiadu kryminalistycznego z wykorzystaniem narzędzi kryminalistyki cyfrowej oraz zapoznają się z praktycznym obszarem zawodu kryminalistyka.

Tematyka zajęć

1. Wprowadzenie do informatyki śledczej
- podstawowe pojęcia i definicje
- proces informatyki śledczej
- rola informatyki śledczej, kwestie etyczne i prawne

2. Cyberbprzestępczość
- definicje i charakterystyka cyberprzestępczości
- specyfika środowiska i mechanizmów ataków
- regulacje prawne i dane statystyczne
3. Narzędzia informatyki śledczej
- przegląd narzędzi
- analiza podstawowych narzędzi: zabezpieczania, analizy oraz prezentacji
4. Studium przypadków
- analiza konkretnych incydentów i spraw kryminalnych
- rekonstrukcja zdarzeń
- praktyki postępowania
Zajęcia laboratoryjne będą obejmowały praktyczne aspekty podejmowane podczas wykładów, w tym: metody zabezpieczania dowodów, analizy danych, odtwarzania zdarzeń na podstawie pozyskanych informacji, analiza artefaktów oraz przygotowywanie raportów, z wykorzystaniem narzędzi informatycznych.

Metody dydaktyczne

• Wykłady z prezentacją multimedialną oraz dodatkowymi elementami praktycznymi w celu omówienia zastosowania narzędzi informatycznych w postaci studiów przypadków.
• Laboratoria obejmujące ćwiczenia z zastosowania narzędzi informatyki śledczej na podstawie dostarczonych przez prowadzącego instrukcji i/lub projekt obejmujący studium przypadku.

Literatura

Podstawowa:
• Daren Hayes, “A Practical Guide to Digital Forensics Investigations”
• Joakim Karvestad, “Fundamentals of Digital Forensics. Theory, Methods, and Real-Life Applications”
• Gerard Johansen “Digital Forensics and Incident Response - Second Edition”

Uzupełniająca:

• Casey, E. "Digital Evidence and Computer Crime", Academic Press, 2011.
• Sammons, J. "The Basics of Digital Forensics", Syngress, 2015.
• Raporty branżowe, organizacji społecznych

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	54	2,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	24	1,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	30	1,00