Wprowadzenie do informatyki śledczej

Karta opisu przedmiotu

Informacje podstawowe

Kierunek studiów
Nowoczesne Technologie w Kryminalistyce (kierunek wspólny - WIEiT, WH, WIMiC)

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki, Elektroniki i Telekomunikacji

Poziom kształcenia
Studia inżynierskie I stopnia

Forma studiów
Stacjonarne

Profil studiów
Ogólnoakademicki

Cykl dydaktyczny
2026/2027

Kod przedmiotu
INKTS.li2.08531.26

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kierunkowe

Przedmiot powiązany z badaniami naukowymi
Nie

Koordynator przedmiotu	Paweł Oberszt
Prowadzący zajęcia	Paweł Oberszt

Okres	**Forma zaliczenia**	**Liczba punktów ECTS**
Semestr 2	Egzamin **Forma prowadzenia i godziny zajęć** Wykład: 30 Ćwiczenia laboratoryjne: 30	4

Cele kształcenia dla przedmiotu

C1	Zapoznanie studentów z szerokim spektrum zagadnień technicznych dotykanych przez informatykę śledczą.
C2	Przekazanie wiedzy z zakresu podstaw systemów operacyjnych, systemów plików, sieci komputerowych, kryptografii z ukierunkowaniem na informatykę śledczą.

Efekty uczenia się dla przedmiotu

Kod	Efekty w zakresie	Kierunkowe efekty uczenia się	Metody weryfikacji
Wiedzy – Student zna i rozumie:			
W1	Zna konstrukcję systemów plików, pamięci i ruchu sieciowego w stopniu pozwalającym na ich analizę.	NKT1A_W04	Wykonanie ćwiczeń laboratoryjnych
W2	Zna podstawowe artefakty w systemach Windows, Linux, macOS, Android i iOS.	NKT1A_W04	Wykonanie ćwiczeń laboratoryjnych
Umiejętności – Student potrafi:			
U1	Potrafi przeprowadzić analizę dowodową w zakresie systemów plików, pamięci operacyjnej i ruchu sieciowego.	NKT1A_U04	Wykonanie ćwiczeń laboratoryjnych
Kompetencji społecznych – Student jest gotów do:			
K1	Rozumie, jakie konsekwencje mogą mieć dane pozyskane w ramach analizy dowodowej.	NKT1A_K02	Egzamin

Treści programowe zapewniające uzyskanie efektów uczenia się dla modułu zajęć

Przedmiot wprowadza w szerokie zagadnienie informatyki śledczej i analizy dowodowej w zakresie systemów plików, pamięci operacyjnej i ruchu sieciowego.

Nakład pracy studenta

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane aktywności
Wykład	30
Ćwiczenia laboratoryjne	30
Przygotowanie do zajęć	20
Samodzielne studiowanie tematyki zajęć	25
Dodatkowe godziny kontaktowe	5
Łączny nakład pracy studenta	**Liczba godzin** 110
Liczba godzin kontaktowych	**Liczba godzin** 60

* godzina (lekcyjna) oznacza 45 minut

Treści programowe

Lp.	Treści programowe	Efekty uczenia się dla przedmiotu	Formy prowadzenia zajęć
1.	• Podstawy kryptografii. • Podstawy systemów operacyjnych. • Podstawy sieci komputerowych. • Zbieranie cyfrowych danych dowodowych. • Artefakty w systemach Windows, Linux, macOS. • Analiza pamięci operacyjnej. • Analiza systemów plików. • Analiza ruchu sieciowego.	W1, W2, U1, K1	Wykład
2.	• Podstawy kryptografii. • Podstawy systemów operacyjnych. • Podstawy sieci komputerowych. • Zbieranie cyfrowych danych dowodowych. • Artefakty w systemach Windows, Linux, macOS. • Analiza pamięci operacyjnej. • Analiza systemów plików. • Analiza ruchu sieciowego.	W1, W2, U1, K1	Ćwiczenia laboratoryjne

Informacje rozszerzone

Metody i techniki kształcenia :

Mini wykład, Studium przypadku (ang. case study), Odwrócona klasa (ang. flipped classroom), Metoda projektowa (ang. Project Based Learning), Metoda problemowa (ang. Problem Based Learning), Kształcenie zdalne, Grywalizacja, gamifikacja, Design thinking, Praca grupowa, Dyskusja

Rodzaj zajęć	Metody zaliczenia	Warunki zaliczenia przedmiotu
Wykład	Wykonanie ćwiczeń laboratoryjnych, Egzamin	Otrzymanie pozytywnej oceny z egzaminu
Ćwiczenia laboratoryjne	Wykonanie ćwiczeń laboratoryjnych, Egzamin	Otrzymanie ponad 50% punktów z każdego laboratorium i otrzymanie ponad 50% sumy punktów ze wszystkich laboratoriów i otrzymanie ponad 50% punktów z kolokwium (jeżeli w danym roku będzie ono realizowane).

Dodatkowy opis

Zajęcia prowadzone z wykorzystaniem innowacyjnych metod dydaktycznych opracowanych w projekcie POWR.03.04.00-00-D002/16 realizowanym w latach 2017-2019 na Wydziale Informatyki, Elektroniki i Telekomunikacji w ramach POWER 2014-2020.

Warunki i sposób zaliczenia poszczególnych form zajęć, w tym zasady zaliczeń poprawkowych, a także warunki dopuszczenia do egzaminu

- Laboratorium: otrzymanie ponad 50% punktów z każdego laboratorium i otrzymanie ponad 50% sumy punktów ze wszystkich laboratoriów i otrzymanie ponad 50% punktów z kolokwium (jeżeli w danym roku będzie ono realizowane). Ze względu na charakter przedmiotu, brak jest możliwości uzyskania zaliczenia w terminie poprawkowym.
- Egzamin: brak warunków dopuszczenia, trzy terminy zaliczenia.

Sposób obliczania oceny końcowej

Średnia ważona ocen z laboratorium i egzaminu.

Sposób i tryb wyrównywania zaległości powstałych wskutek nieobecności studenta na zajęciach

Laboratoria muszą być realizowane przez studenta na bieżąco. Brak przystąpienia do realizacji laboratorium musi być usprawiedliwiony. Nieprzystąpienie do więcej niż dwóch laboratoriów bez usprawiedliwienia skutkuje otrzymaniem wpisu „nb" na koniec semestru. W przypadku usprawiedliwienia nieobecności możliwe jest jej odrobienie (max dwie nieobecności).

Wymagania wstępne i dodatkowe

Studenci powinni:

- znać system Linux w stopniu przynajmniej pozwalającym na płynne poruszanie się w terminalu i korzystaniu z zaawansowanych komend,
- umieć pisać skrypty w języku Python.

Zasady udziału w poszczególnych zajęciach, ze wskazaniem, czy obecność studenta na zajęciach jest obowiązkowa

1. Wykład: Studenci uczestniczą w zajęciach poznając kolejne treści nauczania zgodnie z syllabusem przedmiotu. Studenci winni na bieżąco zadawać pytania i wyjaśniać wątpliwości. Rejestracja audiowizualna wykładu wymaga zgody prowadzącego.
2. Ćwiczenia laboratoryjne: Studenci wykonują ćwiczenia laboratoryjne zgodnie z materiałami udostępnionymi przez prowadzącego. Student jest zobowiązany do przygotowania się w przedmiocie wykonywanego ćwiczenia, co może zostać zweryfikowane kolokwium w formie ustnej lub pisemnej. Zaliczenie zajęć odbywa się na podstawie zaprezentowania rozwiązania postawionych problemów.

Literatura

Obowiązkowa

1. Eoghan Casey, „Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet." Academic Press, 2011.
2. Eoghan Casey, „Handbook of digital forensics and investigation." Elsevier Academic Press, 2010.
3. * Michael Hale Ligh & Andrew Case & Jamie Levy & Aaron Walters, „The Art of Memory Forensics." John Wiley and Sons, 214
4. Brian Carrier, „File System Forensic Analysis." Pearson Education, 2005.
5. Andrew S. Tanenbaum & Herbert Bos, „Modern Operating Systems: Fourth Edition." Pearson Education, 2015.
6. Charles M. Kozierok, „THE TCP/IP GUIDE. A Comprehensive, Illustrated Internet Protocols Reference." No Starch Press, 2005.

Kierunkowe efekty uczenia się

Kod	Treść
NKT1A_K02	Ma świadomość roli społecznej oraz zawodowej absolwenta uczelni technicznej i ważności zachowania w sposób profesjonalny, przestrzegania zasad etyki zawodowej i dbałości o dorobek i tradycje zawodu oraz poszanowania różnorodności kultur. Ma także świadomość ważności i rozumie pozatechniczne aspekty i skutki działalności inżyniera, w tym jej wpływ na środowisko, i związaną z tym odpowiedzialność za podejmowane decyzje;
NKT1A_U04	Potrafi planować i przeprowadzać testy, eksperymenty i badania z dziedziny elektroniki, telekomunikacji i informatyki, w szczególności związane z analizą kryminlistyczną oraz analizą bezpieczeństwa, oparte na obliczeniach, symulacjach komputerowych i pomiarach.
NKT1A_W04	Ma uporządkowaną wiedzę na temat sieci teleinformatycznych, zasad adresacji, mechanizmów doboru tras; zna podstawowe pojęcia z zakresu przesyłania danych, zna rolę kodowania, modulacji i kryptografii, zna metody kodowania dźwięków, obrazów i tekstu w multimediach; w zakresie architektury komputerów, systemów i sieci komputerowych, baz danych oraz systemów operacyjnych, niezbędną do instalacji, obsługi i utrzymania narzędzi informatycznych służących do przetwarzania informacji; ma wiedzę na temat bezpieczeństwa komunikacji oraz bezpieczeństwa systemów operacyjnych