**Nazwa przedmiotu:**

Informatyka śledcza

**Koordynator przedmiotu:**

dr inż. Magdalena Szeżyńska

**Status przedmiotu:**

Fakultatywny ograniczonego wyboru

**Poziom kształcenia:**

Studia I stopnia

**Program:**

Informatyka

**Grupa przedmiotów:**

Wspólne

**Kod przedmiotu:**

**Semestr nominalny:**

5 / rok ak. 2011/2012

**Liczba punktów ECTS:**

4

**Liczba godzin pracy studenta związanych z osiągnięciem efektów uczenia się:**

**Liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich:**

**Język prowadzenia zajęć:**

polski

**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym:**

**Formy zajęć i ich wymiar w semestrze:**

|  |  |
| --- | --- |
| Wykład:  | 30h |
| Ćwiczenia:  | 0h |
| Laboratorium:  | 0h |
| Projekt:  | 0h |
| Lekcje komputerowe:  | 0h |

**Wymagania wstępne:**

• Podstawy elektroniki
• Elementy konstrukcji sprzętu cyfrowego
• Systemy operacyjne
• Sieci komputerowe

**Limit liczby studentów:**

**Cel przedmiotu:**

do uzupełnienia

**Treści kształcenia:**

• Wprowadzenie podstawowych koncepcji informatyki śledczej - definicje, potrzeby, wymagania, podstawy prawne, aspekty etyczne; główne fazy śledztwa informatycznego – przygotowanie przypadku, rozpoczęcie śledztwa, przeprowadzenie przykładowego badania, analiza przypadku, sporządzanie dokumentacji.
• Identyfikacja elektronicznych dowodów winy, zabezpieczanie dowodów na miejscu przestępstwa i w laboratorium badawczym, katalogowanie i przechowywanie dowodów, zabezpieczanie dowodów (zapewnienie ich integralności, wiarygodności poufności itp.) oraz prezentacja wniosków z informatycznego śledztwa.
• Narzędzia pracy informatycznego śledczego (TCT, Sleuthkit, Autopsy, specjalizowane dystrybucje Linuxa, rozwiązania przeznaczone na inne platformy i komercyjne, techniki eDiscovery).
• Procesy uruchamiania (booting) systemów, dyski startowe, partycje rozruchowe, sektory i programy ładujące, tworzenie obrazów uruchomieniowych CD/DVD i USB oraz wykorzystywanie płyt CD/DVD i dysków USB w celu nieinwazyjnego dostępu do badanego systemu.
• Systemy plików FAT, NTFS/NTFS5, EXT2/EXT3, USF1/USF2 itp.- specyfikacje, struktury danych, specyficzne techniki badania.
• Rozpoznawanie typów, rekonstrukcja i analiza zawartości plików zawierających potencjalne dowody, interpretacja dzienników zdarzeń aplikacji i logów systemowych, dowodzenie zaistnienia włamania.
• Badanie systemów czynnych (live systems: Windows, Unix/Linux) oraz ruchu sieciowego, poszukiwanie dowodów w Internecie, techniki eDiscovery.

**Metody oceny:**

Wykłady: Dwa testy (bez notatek) w połowie i na koniec semestru (po 25 punktów). 3 ddoatkowe punkty za obecność (lista obecności sprawdzana bez zapowiedzi trzy razy w ciągu semestru).
Laboratoria: Pięć 3-godzinnych laboratoriów rozpoczynających się od 10-minutowego testu, potem indywidualna praca z naciskiem na dokumentację. Do uzyskania 5 x 10 punktów..
Bez poprawek (powtórnych podejść). Nie ma wymagania zaliczenia indywidualnie wykładów i laboratoriów.
Ostateczny wynik: Punkty z testów i laboratoriów sumują się. Do zaliczenia wymagane jest co najmniej 51 punktów. Skala liniowa: (51-60 punktów na 3, 61-70 punktów na 3,5 itd., 91-103 punkty daje 5).

**Egzamin:**

**Literatura:**

• Wewnętrzne materiały dydaktyczne opracowane na potrzeby przedmiotu
• Bogdan Fischer, Przestępstwa komputerowe i ochrona informacji : aspekty prawno kryminalistyczne, ZAKAMYCZE, 2000
Literatura w języku angielskim:
• Harlan Carvey, Windows Forensic Analysis, SYNGRESS 2007
• Keith J. Jones, Richard Bejtlish, Curtis W. Rose, Real Digital Forensics, Computer Security and Incident Response, Addison-Wesley 2006
• Eoghan Casey, Digital Evidence and Computer Crime, Elsevier Academic Press 2004
• Brian Carrier, File System Forensic Analysis, Addison-Wesley 2005
• Barry J. Grundy, The Law Enforcement and Forensic Examiner's Introduction to Linux, LinuxLEO.com
• oraz inne opracowania dostępne w wersji elektronicznej w repozytoriach internetowych

**Witryna www przedmiotu:**

**Uwagi:**

## Efekty przedmiotowe