KARTA PRZEDMIOTU

1. Informacje ogólne

Nazwa przedmiotu i kod (wg planu studiów):	Informatyka śledcza: **D1_8**
Nazwa przedmiotu (j. ang.):	Computer Forensics
Kierunek studiów:	Informatyka
Specjalność/specjalizacja:	Bezpieczeństwo systemów informatycznych
Poziom kształcenia:	studia I stopnia
Profil kształcenia:	praktyczny (P)
Forma studiów:	studia stacjonarne
Obszar kształcenia:	nauki techniczne
Dziedzina:	nauki techniczne
Dyscyplina nauki:	Informatyka
Koordynator przedmiotu:	mgr Radosław Gołąb

2. Ogólna charakterystyka przedmiotu

Przynależność do modułu:	kształcenie specjalnościowe
Status przedmiotu:	obieralny
Język wykładowy:	Polski
Rok studiów, semestr:	III, 5
Forma i wymiar zajęć według planu studiów:	stacjonarne - wykład 30 h, ćw. laboratoryjne 30 h
Interesariusze i instytucje partnerskie (nieobowiązkowe)	
Wymagania wstępne / Przedmioty wprowadzające:	Aspekty prawne ochrony informacji, Systemy operacyjne

3. Bilans punktów ECTS

		stacjonarne
Całkowita liczba punktów ECTS: (A + B)	**6**	
A. Liczba godzin wymagających bezpośredniego udziału nauczyciela z podziałem na typy zajęć oraz całkowita liczba punktów ECTS osiąganych na tych zajęciach:	obecność na wykładach obecność na ćwiczeniach laboratoryjnych udział w konsultacjach **w sumie:** ECTS	30 30 7 67 3
B. Poszczególne typy zadań do samokształcenia studenta (niewymagających bezpośredniego udziału nauczyciela) wraz z planowaną średnią liczbą godzin na każde i sumaryczną liczbą ECTS:	przygotowanie do ćwiczeń laboratoryjnych wykonanie sprawozdań przygotowanie do kolokwium praca w sieci przygotowanie do konsultacji uzupełnienie/studiowanie notatek studiowanie zalecanej literatury **w sumie:** ECTS	10 20 10 5 5 5 5 60 3
C. Liczba godzin praktycznych / laboratoryjnych w ramach przedmiotu oraz związana z tym liczba punktów ECTS:	udział w ćwiczeniach laboratoryjnych praca praktyczna samodzielna **w sumie:** ECTS	30 30 60 2

4. Opis przedmiotu

Cel przedmiotu:

Celem przedmiotu jest zdobycie przez studenta podstawowej wiedzy i umiejętności w zakresie zabezpieczania nośników danych oraz analizy danych pozyskanych z zabezpieczonych nośników danych pod kątem wykorzystania ich jako materiał dowodowy.

Metody dydaktyczne: *wykład, praktyczne ćwiczenia laboratoryjne*

Treści kształcenia:

Wykłady:

1. Wprowadzenie podstawowych koncepcji informatyki śledczej – definicje, potrzeby, wymagania, podstawy prawne, aspekty etyczne; główne fazy śledztwa.
2. Informatyka śledcza a bezpieczeństwo informacji (bezpieczeństwo systemów informatycznych) – reakcja na incydenty z zakresu bezpieczeństwa informacji, aspekty.
3. Identyfikacja elektronicznych dowodów winy, zabezpieczanie dowodów na miejscu przestępstwa i w laboratorium badawczym, katalogowanie i przechowywanie dowodów.
4. Narzędzia pracy informatycznego śledczego.
5. 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.
6. Rozpoznawanie typów, rekonstrukcja i analiza zawartości plików zawierających potencjalne dowody, interpretacja dzienników zdarzeń aplikacji i logów systemowych.

7. Pozyskiwanie i analiza dowodów z urządzeń mobilnych.

Ćwiczenia laboratoryjne:

1. Oprogramowanie informatycznego śledczego, analiza obrazu dysku typu pendrive, odzyskiwanie skasowanych i nadpisanych plików.
2. Zabezpieczanie dowodów - samodzielne wykonywanie obrazów dysków z zapewnieniem ich integralności, poszukiwanie ukrytych dowodów.
3. Tworzenie obrazu systemu plików, analiza i poszukiwanie ukrytych w nim dowodów, odtwarzanie sekwencji zdarzeń.
4. Analizy powłamaniowa systemu (na podstawie dostarczonego obrazu systemu).

5. Efekty kształcenia i sposoby weryfikacji

Efekty kształcenia		
Efekt przedmiotu *(kod przedmiotu + kod efektu kształcenia)*	**Student, który zaliczył przedmiot (spełnił minimum wymagań)**	**Efekt kierunkowy**
	Wiedza:	
D1_8_W01	1. Zna podstawowe metody, techniki, narzędzia i materiały stosowane przy zabezpieczaniu elektronicznego materiału dowodowego.	K_W06
D1_8_W02	2. Ma podstawową wiedzę o trendach rozwojowych w informatyce i ich wpływie na przetwarzanie i magazynowanie danych w komputerach PC.	K_W08
D1_8_W03	3. Zna sposoby analizy nośników danych pod kątem wyszukiwania ukrytych danych.	K_W09
	Umiejętności	
D1_8_U01	1. Student posiada umiejętności zastosowania podstawowych technik pozyskiwania dowodu elektronicznego.	K_U09
D1_8_U02	2. Zna i umie zastosować podstawowe narzędzia do pozyskiwania dowodów elektronicznych.	K_U11
D1_8_U03	3. Potrafi zabezpieczyć dowody elektroniczne w celu ich dalszej analizy.	K_U30
	Kompetencje społeczne	
D1_8_K01	1. Ma świadomość roli i znaczenia bezpieczeństwa przetwarzanych danych w przedsiębiorstwie, gospodarce i społeczeństwie.	K_K01
D1_8_K02	2. Student rozumie potrzebę wykorzystania nabytej wiedzy na niezwykle szybko rozwijającym się rynku aplikacji.	K_K08

Sposoby weryfikacji efektów kształcenia*:*
(np. dyskusja, gra dydaktyczna, zadanie e-learningowe, ćwiczenie laboratoryjne, projekt indywidualny/ grupowy, zajęcia terenowe, referat studenta, praca pisemna, kolokwium, test zaliczeniowy, egzamin, opinia eksperta zewnętrznego, etc. Dodać do każdego wybranego sposobu symbol zakładanego efektu, jeśli jest ich więcej)

Lp.	**Efekt przedmiotu**	**Sposób weryfikacji**	**Ocena formująca**	**Ocena końcowa**
1	D1_8_W01 D1_8_W02 D1_8_W03	kolokwium zaliczeniowe	ocena z kolokwium - sprawdzian wiedzy i umiejętności	Ocena końcowa z laboratorium - średnia z ocen

	D1_8_U01 D1_8_U02 D1_8_U03			formujących
2	D1_8_U01 D1_8_U02 D1_8_U03 D1_8_K01 D1_8_K02	ćwiczenia laboratoryjne	ocena sprawozdania z prac laboratoryjnych, ocena zaangażowania na zajęciach	

Kryteria oceny (*oceny 3,0 powinny być równoważne z efektami kształcenia, choć mogą być bardziej szczegółowo opisane*)**:**

w zakresie wiedzy		**Efekt kształcenia**
Na ocenę 3,0	Student uzyskał min. 50% wymaganej wiedzy w zakresie obowiązującego materiału. Student: - Zna podstawowe metody, techniki, narzędzia i materiały stosowane przy zabezpieczaniu elektronicznego materiału dowodowego. - Ma podstawową wiedzę o trendach rozwojowych w informatyce i ich wpływie na przetwarzanie i magazynowanie danych w komputerach PC. - Zna sposoby analizy nośników danych pod kątem wyszukiwania ukrytych danych.	D1_8_W01 D1_8_W02 D1_8_W03
Na ocenę 5,0	Student zdobył powyżej 95% wymaganej wiedzy w zakresie obowiązującego materiału. Student: - Wie jak dobrać odpowiednia narzędzia do analizy konkretnego przypadku. - Rozumie znaczenie szybkich zmian w przetwarzaniu i magazynowaniu danych w systemach komputerowych. - Zna zaawansowane techniki pozyskiwania dowodów elektronicznych.	D1_8_W01 D1_8_W02 D1_8_W03
w zakresie umiejętności		**Efekt kształcenia**
Na ocenę 3,0	Student uzyskał min. 50% wymaganych umiejętności w zakresie obowiązującego materiału. Student potrafi: - Student posiada umiejętności zastosowania podstawowych technik pozyskiwania dowodu elektronicznego. - Zna i umie zastosować podstawowe narzędzia do pozyskiwania dowodów elektronicznych. - Potrafi zabezpieczyć dowody elektroniczne w celu ich dalszej analizy.	D1_8_U01 D1_8_U02 D1_8_U03
Na ocenę 5,0	Student uzyskał min. 50% wymaganych umiejętności w zakresie obowiązującego materiału. Student potrafi: - Student potrafi zaplanować, oraz przeprowadzić proces pozyskiwania dowodów elektronicznych. - Student potrafi zastosować zaawansowane narzędzia do pozyskiwania dowodów elektronicznych. - Umie analizować wcześniej zabezpieczone dowody elektroniczne.	D1_8_U01 D1_8_U02 D1_8_U03
w zakresie kompetencji społecznych		**Efekt kształcenia**
Na ocenę 3,0	Student osiągną wymagane kompetencje społeczne na poziomie min. 50%.	D1_8_K01 D1_8_K02
Na ocenę 5,0	Student osiągną wymagane kompetencje społeczne na poziomie wyższym niż 90%.	D1_8_K01 D1_8_K02

Student, który nie osiągnął zakładanych efektów kształcenia, nie zalicza przedmiotu.

Kryteria oceny końcowej:
ocena z laboratorium: ocena z kolokwium: 30 % ocena ze sprawozdania: 50% samodzielne wykonanie ćwiczeń laboratoryjnych: 15% aktywność na zajęciach: 5%
Zalecana literatura :
Literatura podstawowa: 1. Kalinowski A., Metody Inwigilacji i Elementy Informatyki Śledczej., CSH, 2011 2. Mueller S.,Rozbudowa i naprawa komputerów PC. Wydanie XVIII., Helion, 2009 3. Metzger P.,GIMP. Anatomia PC. Wydanie XI., Helion, 2007 **Literatura uzupełniająca:** Źródła internetowe: Serwisy internetowe poświęcone informatyce śledczej

Informacje dodatkowe:

Dodatkowe obowiązki prowadzącego wraz z szacowaną całkowitą liczbą godzin:
Konsultacje – 15 godzin
Poprawa prac projektowych – 10 godzin
Przygotowanie ćwiczeń laboratoryjnych - 5 godzin
W sumie: 30 godzin