AKADEMIA WSB					
Kierunek studiów: Bezpieczeństwo narodowe					
Przedmiot: Informatyka śledcza					
Profil kształcenia: praktyczny					
Poziom kształcenia: studia II stopnia					
Liczba godzin w semestrze	1		2		
	I	II	III	**IV**	
Studia stacjonarne (w/ćw/lab/pr/e)				**22ćw**	
Studia niestacjonarne (w/ćw/lab/pr/e)					
WYKŁADOWCA	dr inż. Krystian Mączka				
FORMA ZAJĘĆ	Ćwiczenia				
CELE PRZEDMIOTU	Celem przedmiotu jest wprowadzenie w szerokie zagadnienie informatyki śledczej i analizy dowodowej w zakresie systemów plików, pamięci operacyjnej i ruchu w internecie.				
Odniesienie do efektów uczenia się		**Opis efektów uczenia się**		**Sposób weryfikacji efektu uczenia się**	
Efekt kierunkowy	**PRK**				
WIEDZA					
BN2_W07	P7S_WG	Student zna konstrukcję systemów plików, pamięci i ruchu sieciowego w stopniu pozwalającym na ich analizę;		Test wiedzy;	
UMIEJĘTNOŚCI					
BN2_U01	P7S_UW	Student właściwie dokonuje oceny i krytycznej analizy konieczności podejmowania badań z zakresu informatyki śledczej, wykorzystuje odpowiednie metody i narzędzia do przeprowadzenia podstawowej oceny dowodu cyfrowego, potrafi analizować wyniki pracy specjalistów z tego zakresu		Ocena umiejętności studenta w ramach analizowanego na ćwiczeniach problemu;	
BN2_U02	P7S_UW	Student potrafi przeprowadzić analizę dowodową w zakresie systemów plików, pamięci operacyjnej i ruchu sieciowego;		Ocena umiejętności studenta w ramach analizowanego na ćwiczeniach problemu;	
KOMPETENCJE SPOŁECZNE					
BN2_K01	P7S_KK	Student jest gotów do odpowiedzialnego pełnienia roli zawodowej uwzględniając znaczenie i zastosowanie jakie mogą mieć dane pozyskane w ramach analizy dowodowej;		Ocena postaw studenta w ramach analizowanego na ćwiczeniach problemu;	
Nakład pracy studenta (w godzinach dydaktycznych 1h dyd.=45 minut)**					

Stacjonarne	**Niestacjonarne**
udział w wykładach =	udział w wykładach =
udział w ćwiczeniach = 22	udział w ćwiczeniach =
przygotowanie do ćwiczeń = 12	przygotowanie do ćwiczeń =
przygotowanie do wykładu/ konwersatorium =	przygotowanie do wykładu/ konwersatorium =
przygotowanie do zaliczenia/egzaminu =12	przygotowanie do zaliczenia/egzaminu =
realizacja zadań projektowych =	realizacja zadań projektowych =
e-learning =	e-learning =
zaliczenie/egzamin =2	zaliczenie/egzamin =
inne (konsultacje) = 4	inne (konsultacje) =
RAZEM:52	**RAZEM:**
Liczba punktów ECTS: 2	**Liczba punktów ECTS:**
w tym w ramach zajęć kształtujących umiejętności praktyczne:2	**w tym w ramach zajęć kształtujących umiejętności praktyczne:**

WARUNKI WSTĘPNE	Nie wymaga się
TREŚCI PRZEDMIOTU	Treści realizowane w formie bezpośredniej: 1. Informatyka śledcza – definicje, potrzeby, wymagania, podstawy prawne, aspekty etyczne; główne fazy śledztwa informatycznego 2. Informatyka śledcza a bezpieczeństwo informacji 3. Identyfikacja elektronicznych dowodów winy, zabezpieczanie dowodów na miejscu przestępstwa i w laboratorium badawczym, katalogowanie i przechowywanie dowodów, zabezpieczanie dowodów. 4. Narzędzia pracy informatycznego śledczego 5. Wirtualizacja w służbie informatyki śledczej. 6. Systemy plików – specyfikacje, struktury danych, specyficzne techniki badania. 7. Rozpoznawanie typów, rekonstrukcja i analiza zawartości plików zawierających potencjalne dowody, interpretacja dzienników zdarzeń aplikacji i logów systemowych, dowodzenie zaistnienia włamania. 8. Pozyskiwanie i analiza dowodów z urządzeń mobilnych. 9. Poszukiwanie dowodów w Internecie. Treści realizowane w formie e-learning: nie dotyczy
LITERATURA OBOWIĄZKOWA	1. H. Carvey, Analiza śledcza i powłamaniowa. Zaawansowane techniki prowadzenia analizy w systemie Windows 7. Wydanie III, Helion 2013. 2. C. Altheide, H. Carvey, Informatyka śledcza. Przewodnik po narzędziach open source, Helion 2014. 3. A. Chojnowski, Informatyka sądowa w praktyce (ebook), Helion 2019
LITERATURA UZUPEŁNIAJĄCA	1. G. Johansen, Digital Forensics and Incident Response. 2017, Packt Publishing. 2. B. Nikkel, Practical Forensic Imaging, 2016, No Starch Press. 3. A. Cory, C. Harlan, Informatyka śledcza. Przewodnik po narzędziach open source, Helion 2021. 4. L. Jason, P. Matthew, M. Kevin, Incydenty bezpieczeństwa. Metody reagowania w informatyce śledczej, Wydawnictwo Helion, 2021
METODY NAUCZANIA	W formie bezpośredniej: • metody laboratoryjne W formie e-learning: nie dotyczy
POMOCE NAUKOWE	• prezentacja multimedialna, • teksty źródłowe,
PROJEKT	Nie dotyczy
FORMA I WARUNKI ZALICZENIA	Ćwiczenia – test zaliczeniowy – zaliczenie na ocenę