POLSKO-JAPOŃSKA AKADEMIA TECHNIK KOMPUTEROWYCH

SYLABUS PRZEDMIOTU

Nazwa przedmiotu:	**Kryminalistyka Cyfrowa**
Kod przedmiotu:	KC
Kierunek / Profil:	Informatyka / praktyczny
Tryb studiów:	stacjonarny
Rok / Semestr:	/ 5
Charakter:	obowiązkowy
Odpowiedzialny:	
Wersja z dnia:	19.02.2026

1. Godziny zajęć i punkty ECTS

Wykłady	Ćwiczenia	Laboratori	Z prowa-dzącym	Praca własna	Łącznie	ECTS
30 h	—	30 h	60 h	65 h	125 h	**5**

2. Forma zajęć

Forma zajęć	Sposób zaliczenia
Wykład	Egzamin

3. Cel dydaktyczny

Kryminalistyka cyfrowa to dziedzina zajmująca się śledztwem i badaniem dowodów związanych z przestępstwami cyfrowymi. Jest to rodzaj kryminalistyki, która koncentruje się na zdolności do wykorzystywania technologii i nauki do zgromadzenia dowodów, które mogą być przedstawione w sądzie. Kryminalistyka Cyfrowa odgrywa kluczową rolę w walce z cyberprzestępczością, pomagając organom ścigania zrozumieć, jak doszło do przestępstwa, kto może za nie odpowiadać i jakie kroki mogą być podjęte, aby zapobiec przyszłym incydentom. Główne cele dydaktyczne to badanie sieci, czyli umiejętność analizy ruchu

sieciowego w celu wykrycia nieprawidłowości lub dowodów na działania przestępcze.Inny cel to analiza logów systemowych, czyli zebranie informacji o tym, co się działo na danym systemie w określonym czasie. Analiza tych logów może pomóc w ustaleniu, co się stało podczas incydentu.

4. Treści programowe

1. Wykład:
2. Wprowadzenie do Kryminalistyki Cyfrowej
3. Bezpieczeństwo protokołów i urządzeń warstwy 1-2 modelu OSI
4. Bezpieczeństwo protokołów i urządzeń warstwy 3-4 modelu OSI
5. Bezpieczeństwo protokołów i urządzeń warstwy 5-7 modelu OSI
6. Metody analizy ruchu sieciowego (Network analysis)
7. Metody analizy oprogramowania (Software analysis)
8. Metody analizy mediów (Media analysis)
9. Metody analizy sprzętu (Hardware analysis)
10. Ćwiczenia:

Linux 1 Operacje na plikach
Linux 1 Operacje identyfikacji oraz kodowania danych
Linux 1 Analiza logów
Linux 2 Mechanizmy systemowe i skrypty Bash
Linux 2 Analiza danych z pliku
Linux 2 Administracja systemem GNU/Linux
Linux 2 Zarządzanie procesami
Sieci 2 Protokół http
Sieci 2 Protokół DNS
Sieci 2 Protokoły poczty
Sieci 2 Inne protokoły
Sieci 2 Bezpieczna komunikacja
Sieci 2 Bezpieczeństwo sieci WiFi

5. Efekty kształcenia

Wiedza

- Student zna i rozumie anatomię kluczowych zagrożeń Cyber
- Student zna i rozumie podstawowe środki ochrony i reakcji na kluczowe zagrożenia Cyber

Umiejętności

- Student potrafi przygotować zestaw środków ochrony informacji odpowiednich dla różnych typów zagrożeń
- Student potrafi wskazać mocne i słabe strony systemów ochrony informacji

Kompetencje społeczne

- Student jest gotów do pracy zespołowej w dziale SOC

6. Kryteria oceny

- Zadania CTF
- Laboratoria
- Kryteria oceny
- Laboratorium/Projekt
- raport z wykonanych zadań laboratoryjnych, kolokwia
- Kryteria oceny:niedostateczny: < 50% możliwych do zdobycia punktów dostateczny : 50%-60% możliwych do zdobycia punktów dostateczny+ : 61%- 70% możliwych do zdobycia punktówdobry : 71%-80% możliwych do zdobycia punktówdobry +: 81%-90% możliwych do zdobycia punktów bardzo dobry : >90% możliwych do zdobycia punktów
- Kryteria oceny:niedostateczny: < 50% poprawnie rozwiązanych zadań egz.dostateczny : 50%-60% poprawnie rozwiązanych zadań egz.dostateczny+ : 61%- 70% poprawnie rozwiązanych zadań egz.dobry : 71%-80% poprawnie rozwiązanych zadań egz.dobry +: 81%-90% poprawnie rozwiązanych zadań egz.bardzo dobry : >90% poprawnie rozwiązanych zadań zaliczeniowych egz.

7. Metody dydaktyczne

Wykład, laboratoria, praca własna studenta.

8. Literatura

Podstawowa:

- William Stallings, Lawrie Brown - Bezpieczeństwo systemów informatycznych. Zasady i praktyka. (ang. Computer Security: Principles and Practice), Wydanie IV. Tom 1 i 2, Helion 2019

Uzupełniająca:

- Brak danych.