Autor*: dr hab. inż. Krzysztof Szczypiorski, prof. PW*

Kryminalistyka cyfrowa (KRYCYF)
Digital Forensics

Poziom kształcenia: I stopień
Forma i tryb prowadzenia przedmiotu: stacjonarna
Kierunek studiów: Cyberbezpieczeństwo
Specjalność:
Grupa przedmiotów:
Poziom przedmiotu: podstawowy
Status przedmiotu: obowiązkowy
Język przedmiotu: polski
Semestr nominalny (tylko dla przedmiotów obowiązkowych): 5
Minimalny numer semestru: 5
Wymagania wstępne, zalecane przedmioty poprzedzające: n/d
Limit liczby studentów: 60

Powód zgłoszenia przedmiotu: program studiów na nowym kierunku Cyberbezpieczeństwo

Cel przedmiotu:

Głównym celem przedmiotu jest wprowadzenie studentów do kryminalistyki cyfrowej jako interdyscyplinarnej dziedziny inżynierii cyberbezpieczeństwa, która wymaga stosowania wielu technik poznawanych w ramach innych przedmiotów fundamentalnych kierunku Cyberbezpieczeństwo.

W ramach przedmiotu omówione zostaną zagadnienia dotyczące kryminalistyki w świecie cyfrowym obejmującym sieci, systemy i użytkowników. Zostanie dokonany przegląd głównych technik i procedur pozyskiwania danych cyfrowych z systemów sprzętowo-programowych oraz sieci. W następnym kroku omówione zostaną techniki analizy tych danych w kierunku ustanowienia wiarygodnych dowodów cyfrowych w postępowaniach sądowych czy sporach prywatnych. Każdy obszar kryminalistyki cyfrowej zostanie scharakteryzowany właściwymi środkami technicznymi i nietechnicznymi. Ponadto przedmiot stanowi interdyscyplinarne połączenie nabytej wiedzy i umiejętności podczas innych przedmiotów na kierunku Cyberbezpieczeństwo.

Założeniem prowadzenia przedmiotu jest ukierunkowanie się na naukę praktyczną. Zajęcia wykładowe będą w większości poświęcone studiowaniu rzeczywistych sytuacji, w których realizują się omawiane zagadnienia. Zajęcia laboratoryjne będą oparte o wykonywanie praktycznych zadań inżynierskich ilustrujących zagadnienia wykładowe. Celem laboratorium jest praktyczne wprowadzenie studentów do systemowej kryminalistyki cyfrowej. Zadania laboratoryjne będą dotyczyły pozyskiwania dowodów cyfrowych z sieci i systemów, analizy dowodów cyfrowych oraz zarządzania incydentami naruszeń bezpieczeństwa komputerowego. W ramach zajęć projektowych studenci będą realizować zadanie typu *studium przypadku na żywo* z zakresu projektowania procesów zarządzania incydentami naruszeń bezpieczeństwa sieci, systemów i użytkowników.

Ponadto przygotują krytyczną analizę materiałów źródłowych z zakresu kryminalistyki cyfrowej.

Treść kształcenia:

WYKŁADY:

1. **Wprowadzenie do kryminalistyki cyfrowej (2 godz.)**
   Pojęcia podstawowe; charakterystyka dziedziny; specjalizacje w ramach kryminalistyki cyfrowej: komputerowa, sieciowa, urządzeń mobilnych, analityczna; Digital Forensics jako element zarządzania cyberbezpieczeństwem; wykorzystanie kryminalistyki cyfrowej: dochodzenia śledcze sądowe, wywiad gospodarczy, compliance, spory prywatne, audyty wewnętrzne organizacji, śledztwa prywatne, fraudy; kryminalistyka cyfrowa jako ogólny proces ustalania tożsamości atakujących bezpieczeństwo w cyberprzestrzeni;

2. **Aspekty prawne i społeczne kryminalistyki cyfrowej (2 godz.)**
   Standardy prowadzenia cyfrowych dochodzeń śledczych w kontekście legalności; standardy prowadzenia cyfrowych dochodzeń śledczych w kontekście sektora prywatnego; aspekty prawne działalności w zakresie cyfrowych dochodzeń śledczych; etyka działań specjalisty od digital forensics; stosowanie technik kryminalistyki cyfrowej w sektorze prywatnym: wywiad gospodarczy, compliance, spory prywatne, audyty wewnętrzne organizacji, śledztwa prywatne, fraudy; studia przypadków realnych projektów kryminalistyki cyfrowej – publiczny proces sądowy, spór prywatny, nadużycia, dziennikarstwo śledcze; inżyniera społeczna w kryminalistyce cyfrowej;

3. **Metodyki pracy w kryminalistyce cyfrowej (2 godz.)**
   Procedury śledcze; kolekcjonowanie i pozyskiwanie danych; egzaminowanie cyfrowych dowodów śledczych w kontekście wiarygodności; raportowanie śledztwa cyfrowego; przegląd narzędzi specjalisty kryminalistyki cyfrowej;

4. **Kryminalistyka cyfrowa w kontekście systemów sprzętowo-programowych (4 godz.)**
   Pozyskiwanie danych śledczych z pamięci urządzeń cyfrowych – komputery, urządzenia mobilne: metody, zabezpieczanie materiału dowodowego, praca z materiałem dowodowym, akwizycja danych; pozyskiwanie danych śledczych z systemów plików: metody, zabezpieczanie materiału dowodowego, praca z materiałem dowodowym, akwizycja danych;

5. **Kryminalistyka cyfrowa w kontekście sieci (4 godz.)**
   Pozyskiwanie danych śledczych jako strumieni komunikacji: kontekst sieci, systemów i użytkowników; przechwytywanie sieciowych strumieni komunikacji – sieci przewodowe LAN i bezprzewodowe (WiFi, GSM/3G/4G/5G, NFC, ZigBee); Czyszczenie danych, parsowanie i właściwa interpretacja strumieni komunikacji; analiza pakietów – techniki i narzędzia;

6. **Analiza złośliwego oprogramowania (6 godz.)**
   Podstawowe techniki przełamywania zabezpieczeń systemów operacyjnych i systemów komputerowych; przejmowanie kontroli i wykonywanie arbitralnego oprogramowania; złośliwe oprogramowanie (malware): rodzaje, podstawowe pojęcia, architektura; warsztat analityka malware; wprowadzenie do klasycznych technik detekcji i analizy malware – metody statyczne i dynamiczne; nowe techniki detekcji i analizy malware; techniki unikania detekcji i utrudniania analizy malware; sieci malware, czyli botnety: podstawowe pojęcia, elementy, architektura; analiza i detekcja botnetów (w kontekście analizy malware); ukrywanie kanałów C&C; trendy i case study: ransomware, IoT botnets, cryptojacking, steganografia, botnet-as-a-service;

7. **Analityczna kryminalistyka cyfrowa (6 godz.)**
   Techniki i metody analizy pozyskanych materiałów ze źródeł cyfrowych (sprzęt, oprogramowanie, sieci); metodyki analitycznego ustanawiania dowodów cyfrowych; Przełamywanie technik utrudniających cyfrową analizę śledczą (anti-forensics); Big Data w kontekście kryminalistyki cyfrowej: odkrywanie głównych aktorów zagrożeń w dużych zbiorach danych; Techniki poszukiwań i prowokacji atakujących: biały wywiad, Dark Web, honeypots/honeynets;

8. **Zarządzanie incydentami naruszeń bezpieczeństwa komputerowego (4 godz.)**
   Incydent naruszenia bezpieczeństwa komputerowego; metodyki i architektury zarządzania incydentami naruszeń bezpieczeństwa komputerowego; Zarządzanie cyberbezpieczeństwem: Threat Intelligence, SOC/CERT/CSIRT, zarządzanie incydentami, metodyki modelowania ryzyka i oceny zagrożeń w cyberprzestrzeni; Digital Forensics w kontekście Intrustion Kill Chain;

ĆWICZENIA:

–

LABORATORIA:

W ramach projektu studenci w zespołach 2-osobowych będą mieli do wykonania 4 zadania praktyczne posiłkując się instruktażem Prowadzącego w zakresie:

1) Metod cyfrowej kryminalistyki śledczej w zakresie systemów sprzętowo-programowych: pozyskiwanie danych cyfrowych z urządzeń, pamięci i systemów plików na potrzeby ustanowienia dowodów cyfrowych;
2) Metod cyfrowej kryminalistyki śledczej w zakresie strumieni komunikacji: pozyskiwania danych z sieci przewodowych i bezprzewodowych, analizy i interpretacji danych sieciowych;
3) Metod analizy złośliwego oprogramowania statycznej i dynamicznej: analiza próbek, odkrywanie wektorów ataku i zastosowanych technik wykorzystania dziur w systemach;
4) Zarządzania incydentami naruszenia bezpieczeństwa komputerowego

Na każde ćwiczenie przewiduje 4 godziny pracy studenta.

PROJEKT:

W ramach projektu zespoły 2-osobowe będą miały do wykonania projekt z zakresu zastosowania technik analitycznych w kryminalistyki cyfrowej. W ramach zadania zespół

opracuje rozwiązanie analityczne postawionego problemu ora implementuje *proof-of-concept* swojego pomysłu. Podsumowaniem prac będzie raport przygotowany zgodnie ze standardami dla cyfrowych dochodzeń. Ponadto każdy zespół przeprowadzi prezentację ustną ze swoich prac.

Elementem projektu będzie także wykonanie przez każdego studenta przedmiotu krytycznego przeglądu literatury naukowej, technicznej i biznesowej z zakresu zagadnień cyfrowej kryminalistyki śledczej, zwieńczonej raportem.

ZAJĘCIA ZINTEGROWANE:

Treść kształcenia - streszczenie w jęz. angielskim:

The course discusses issues related to forensic science in the digital world including networks, systems and users. A review of the main techniques and procedures for obtaining digital data from hardware and software systems and networks is presented. In the next step, techniques for analyzing this data are discussed in the direction of establishing reliable digital evidence in court proceedings or private disputes. Each area of digital forensics is characterized by appropriate technical and non-technical means. In addition, the subject is an interdisciplinary combination of acquired knowledge and skills in other subjects in the field of Cybersecurity.

Egzamin: NIE

Literatura i oprogramowanie:
Materiały do zajęć – slajdy, opracowania, artykuły

Książki:

1. A. Harper et al.: Gray Hat Hacking: The Ethical Hacker's Handbook, 5th Ed.; 2018; McGraw-Hill Education; ISBN 978-1260108415
2. J. Luttgens, M. Pepe, K. Mandia: Incident Response & Computer Forensics, 3rd Ed.; 2014; McGraw-Hill Education; ISBN 978-0071798686
3. SP 800-61: Computer Security Incident Handling Guide; Rev.2; 2012; US NIST
4. A. J. White, B. Clark: Blue Team Field Manual; 2017; CreateSpace Independent Publishing Platform; ISBN 978-1541016361
5. B. Clark: Red Team Field Manual; 2014; CreateSpace Independent Publishing Platform; ISBN 978-1494295509
6. M. Sikorski, A. Honig: Practical Malware Analisys: A Hands-on guide to dissecting malicious software; 2012; No Starch Press; ISBN 978-1593272906
7. A. Ziaja: Praktyczna analiza powłamaniowa. Aplikacja webowa w środowisku Linux; 2017; PWN; ISBN 978-8301193478

Oprogramowanie:

- Systemy operacyjne Windows, Linux, MacOS – wersje klienckie i serwerowe;

- Oprogramowanie open source i komercyjne do realizacji zadań praktycznych z zakresu przedmiotu:
    - profesjonalne oprogramowanie do kryminalistyki cyfrowej – EnCase
    - oprogramowanie do kryminalistyki cyfrowej w zakresie systemów sprzętowo-programowych
    - oprogramowanie do krymininalistyki cyfrowej w zakresie sieci i komunikacji
    - oprogramowanie do analizy danych i Big Data

Wymiar godzinowy zajęć:	W	C	L	P
	30	–	15	15

Przewidywane formy kształcenia i organizacja przedmiotu

Realizacja przedmiotu obejmuje następujące formy zajęć:

- wykład prowadzony w wymiarze 2 godz. tygodniowo,
- zajęcia laboratoryjne; w ramach tych zajęć student, korzystając z oprogramowania i sprzętu będzie realizował wskazane zadania związane z cyfrową kryminalistyką cyfrową w kontekście sprzętowo-programowym oraz sieciowym, analizą złośliwego oprogramowania oraz zarządzania incydentami naruszeń bezpieczeństwa komputerowego;
- zajęcia projektowe; w ramach tych zajęć zespoły studentów będą wykonywały zadanie praktyczne związane z metodami analitycznymi w cyfrowej kryminalistyce śledczej. Studenci przygotują rozwiązania, raporty oraz podsumowują prezentację ustną. Ponadto każdy student będzie miał za zadanie wykonanie krytycznego przeglądu literatury naukowej, technicznej i biznesowej z zakresu cyberbezpieczeństwa;

Sprawdzanie założonych efektów kształcenia realizowane jest przez:

- ocenę wiedzy i umiejętności związanych z realizacją zadań laboratoryjnych – ocenę sprawozdań z realizacji zadań;
- ocenę wiedzy i umiejętności związanych z realizacją zadań projektowych – ocena raportu i prezentacji z realizacji zadania praktycznego oraz raportu z przeglądu literatury;
- ocenę wiedzy i umiejętności wykazanych na egzaminie pisemnym o charakterze problemowym oraz – w przypadkach wątpliwości co do oceny – na egzaminie ustnym,

Wymiar w jednostkach ECTS: 5 pkt.

Liczba godzin pracy studenta związanych z osiągnięciem efektów kształcenia (opis):

1. liczba godzin kontaktowych – **60 godz.**, w tym
    - obecność na wykładach: **30 godz.**,
    - obecność na zajęciach laboratoryjnych: **16 godz.**,
    - obecność na zajęciach projektowych: **4 godz.**,
    - udział w konsultacjach związanych z realizacją przedmiotu: **12 godz.**

2. praca własna studenta – **77 godz.**, w tym
    - analiza literatury i materiałów wykładowych związana z przygotowaniem do kolejnych wykładów: **10 godz.**

- analiza literatury i materiałów wykładowych związana z przygotowaniem do laboratorium: **20 godz.**
- realizacja projektu: **25 godz.** (studium na żywo) + **12 godz.** (analiza literatury i przygotowanie raportu) = **37 godz.**.
- przygotowanie do kolokwium: **10 godz.**

Łączny nakład pracy studenta wynosi 137 godz., **co odpowiada** 5 pkt. **ECTS.**

Liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich: 2 pkt. ECTS, co odpowiada 60 godz. kontaktowym.

Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym: 3 pkt. ECTS (co odpowiada 26+57 = 83 godz. realizacji projektu i laboratorium)

EFEKTY KSZTAŁCENIA/UCZENIA SIĘ

efekty kształcenia/uczenia się student, który zaliczył przedmiot:	**forma zajęć/ technika kształcenia**	**sposób weryfikacji (oceny)***	**odniesienie do efektów uczenia się dla programu**
WIEDZA			
W1: ma wiedzę dotyczącą podstawowych pojęć z zakresu kryminalistyki cyfrowej	wykład + projekt + laboratorium	projekt, laboratorium, kololwium	W07 W09 W12
W2: ma podstawową wiedzę z zakresu uwarunkowań społeczno-ekonomiczno-prawnych przestępstw w cyberprzestrzeni	wykład + projekt + laboratorium	laboratorium, kololwium	W07 W09 W12
W3: ma podstawową wiedzę z zakresu pozyskiwania i zabezpieczenia cyfrowego materiału dowodowego z różnych źródeł (systemy sprzętowo-programowe, sieci)	wykład + laboratorium	laboratorium kololwium	W07
W4: ma wiedzę z zakresu analizowania cyfrowego materiału dowodowego	wykład + laboratorium	laboratorium, kololwium	W07
W5: ma wiedzę z zakresu analizowania złośliwego oprogramowania: pozyskiwania materiału, narzędzi, technik analizy i technik przełamywania mechanizmów anti-forensics	wykład + laboratorium	laboratorium, kololwium	W07
W6: ma wiedzę z zakresu metod analitycznych stosowanych w kryminalistyce śledczej	wykład + projekt	projekt, kololwium	W07
W7: ma wiedzę metodyki procesu zarządzania incydentami	wykład + laboratorium + projekt	projekt, laboratorium, kololwium	W07
W8: ma podstawową wiedzę z zakresu modelowania zagrożeń	wykład + laboratorium + projekt	projekt, laboratorium, kololwium	W07 W12
UMIEJĘTNOŚCI			
U1: potrafi przygotować środowisko pracy analityka kryminalistyki śledczej	wykład + laboratorium	laboratorium	U03
U2: potrafi zabezpieczyć cyfrowy materiał dowodowy z oprogramowania, systemów operacyjnych, serwerów, dysków i sieci	wykład + laboratorium	laboratorium	U08
U3: potrafi przygotować środowisko pracy analityka złośliwego oprogramowania	wykład + laboratorium	laboratorium	U03
U4: potrafi zabezpieczyć materiał złośliwego oprogramowania i wykonać podstawową analizę jego działania	wykład + laboratorium	laboratorium	U08
U5: potrafi modelować zagrożenia z wykorzystaniem standardowych metodyk	wykład + projekt	projekt	U04 U07

U6: potrafi stosować metody analityczne do pozyskanego cyfrowego materiału dowodowego	wykład + laboratorium + projekt	Laboratorium projekt	U04 U07 U08
U7: potrafi w podstawowym zakresie definiować procesy zarządzania incydentami naruszeń bezpieczeństwa sieci, systemów i użytkowników	wykład + laboratorium	laboratorium	U05 U07
U8: potrafi rozwiązywać zadania formułowane na bieżąco, komunikować wnioski i opinie, prowadzić na ich temat dyskusję i przekonywać innych	projekt	projekt	U09 U11
U9: potrafi przygotować i przeprowadzić prezentację dotyczącą zagadnień technicznych związanych z problemem rozwiązywanym na bieżąco	projekt	projekt	U10
U10: potrafi krytycznie analizować dostępną literaturę z zakresu domeny wiedzy	projekt	projekt	U01
KOMPETENCJE SPOŁECZNE			
KS1: ma świadomość konieczności komunikowania się z otoczeniem, także pozazawodowym, w sposób zrozumiały dla odbiorcy	wykład + projekt + laboratorium	projekt + laboratorium	KS05
KS2: ma orientację zawodową w obszarze inżynierii cyberbepieczeństwa i jest świadomy procesu uczenia się w kierunku zwiększania kompetencji w tym obszarze	wykład + projekt	n/d	KS01

Uwagi:

Data i podpis autora (kierownika zespołu autorskiego):