



## KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Analiza złośliwego oprogramowania

### Przedmiot

Kierunek studiów

Rok/semestr

Informatyka

2/3

Studia w zakresie (specjalność)

Profil studiów

Cyberbezpieczeństwo

ogólnoakademicki

Poziom studiów

Język oferowanego przedmiotu

drugiego stopnia

angielski

Forma studiów

Wymagalność

stacjonarne

obieralny

### Liczba godzin

Wykład

Laboratoria

Inne (np. online)

15

30

Ćwiczenia

Projekty/seminaria

### Liczba punktów ECTS

4

### Wykładowcy

Odpowiedzialny za przedmiot/wykładowca:

dr hab. inż. Piotr Zwierzykowski

Piotr.zwierzykowski@put.poznan.pl

tel: 61 665 39 03

Wydział Informatyki i Telekomunikacji

Instytut Sieci Teleinformatycznych

Odpowiedzialny za przedmiot/wykładowca:

mgr inż. Błażej Nowak

blazej.nowak@put.poznan.pl

tel: 61 665 39 20

Wydział Informatyki i Telekomunikacji

Instytut Sieci Teleinformatycznych

### Wymagania wstępne

Student rozpoczynający ten przedmiot powinien mieć podstawową wiedzę z zakresu sieci komputerowych, algorytmów kryptograficznych i systemów operacyjnych Windows i Linux. Powinien również posiadać umiejętność pozyskiwania informacji ze wskazanych źródeł oraz mieć gotowość do podjęcia współpracy w ramach zespołu.

### Cel przedmiotu

Przekazanie studentom wiedzy z zakresu szeroko rozumianej analizy złośliwego oprogramowania, w tym metod i narzędzi wykorzystywanych analizy statycznej i dynamicznej takiego oprogramowania oraz elementów inżynierii wstecznej.

W ramach realizacji przedmiotu zostaną omówione metody wybrane metody statycznej i dynamicznej analizy złośliwego oprogramowania oraz wykorzystywanej w tym celu inżynierii wstecznej. W ramach



ćwiczeń laboratoryjnych student zapozna się w praktyce z narzędziami umożliwiającymi wykrycie złośliwego oprogramowania

### Przedmiotowe efekty uczenia się

#### Wiedza

Ma uporządkowaną i podbudowaną teoretycznie wiedzę ogólną związaną z kluczowymi zagadnieniami z zakresu analizy złośliwego oprogramowania.

Ma zaawansowaną wiedzę szczegółową dotyczącą wybranych zagadnień z zakresu szeroko rozumianej analizy złośliwego oprogramowania oraz metod i narzędzi wykorzystywanych do analizy statycznej i dynamicznej oraz inżynierii wstecznej.

Ma wiedzę o trendach rozwojowych i najistotniejszych nowych osiągnięciach informatyki i telekomunikacji w zakresie wykrywania, analizy statycznej i dynamicznej złośliwego oprogramowania.

Ma zaawansowaną i szczegółową wiedzę o procesach zachodzących w systemach wykorzystywanych do dynamicznej analizy złośliwego oprogramowania.

#### Umiejętności

Potrafi pozyskiwać informacje na temat metod statycznej i dynamicznej analizy złośliwego oprogramowania. Pozyskane informacje (w języku polskim i angielskim) potrafi integrować i poddawać krytycznej ocenie.

Potrafi wykorzystać metody eksperymentalne do formułowania i rozwiązywania zadań inżynierskich i prostych problemów badawczych w obszarze analizy złośliwego oprogramowania.

Potrafi integrować wiedzę z różnych obszarów informatyki i telekomunikacji przy formułowaniu i rozwiązywaniu zadań inżynierskich związanych z wykrywaniem i analizą złośliwego oprogramowania.

Potrafi ocenić przydatność i możliwość wykorzystania nowych rozwiązań sprzętowych i programowych służących do rozwiązywania zadań inżynierskich, polegających na budowie bezpiecznych systemów przesyłania danych.

#### Kompetencje społeczne

Rozumie, że w zakresie bezpieczeństwa teleinformatycznego wiedza i umiejętności bardzo szybko stają się przestarzałe.

Rozumie znaczenie wykorzystywania najnowszej wiedzy z zakresu bezpieczeństwa teleinformatycznego w rozwiązywaniu problemów badawczych i praktycznych.

Ma świadomość konieczności profesjonalnego podejścia do rozwiązywanych problemów bezpieczeństwa teleinformatycznego i podejmowania odpowiedzialności za proponowane przez siebie projekty.

### Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wiedza nabyta w ramach wykładu jest weryfikowana na kolokwium ustnym i/lub pisemnym.



Zagadnienia zaliczeniowe, na podstawie których opracowywane są pytania, przesyłane są studentom drogą mailową z wykorzystaniem systemu uczelnianej poczty elektronicznej, lub umieszczone w kursie przedmiotowym w uczelnianym systemie zdalnego nauczania.

Kolokwium ustne i/lub pisemne obejmuje od 3 do 5 pytań, na które oczekuje się odpowiedzi opisowej. Każda odpowiedź na pytanie jest oceniana w skali od 0 do 5 punktów. Każde pytanie jest równo punktowane. Próg zaliczeniowy: 50% punktów.

W przypadku kolokwium ustnego studenci losują pytania ze zbioru 30 pytań. W przypadku kolokwium pisemnego pytania są zadawane przez prowadzącego.

Umiejętności nabyte w ramach zajęć laboratoryjnych weryfikowane są na bieżąco. Na każdym zajęciach laboratoryjnych oceniana jest poprawność wykonania ćwiczeń w skali od 2 do 5. Ocena końcowa jest średnią ocen uzyskanych z poszczególnych zajęć laboratoryjnych. Ocena końcowa jest średnią ocen uzyskanych z poszczególnych zajęć laboratoryjnych.

### Treści programowe

Tematyka wykładów:

- Introduction to Malware Analysis
- Classification of Malware
- Malware Analysis Methodology
- Malware Analysis Techniques
- Static Analysis of Malware
- Dynamic Analysis of Malware
- Reverse Engineering in Malware Analysis
- Identification and Extraction of Hidden Components
- Static and Dynamic Reversing
- Malware Functionalities and Persistence
- Malware Obfuscation Techniques
- Hunting Malware Using Memory Forensics
- Dependence of Malware from the Platform
- Malware Evasion Techniques

Tematyka laboratoriów:



Zgodna z treściami wykładów

### Metody dydaktyczne

Wykład informacyjny: prezentacja multimedialna, ilustrowana przykładami podawanymi na tablicy.

Ćwiczenia laboratoryjne: ćwiczenia praktyczne w grupach, z wykorzystaniem środowisk i narzędzi testowych.

### Literatura

Podstawowa

D. Barker: Malware Analysis Techniques, Packt>, 2021

Uzupełniająca

1. Alexey Klymenov, Amr Thabet: Mastering Malware Analysis, Packt>, 2019
2. Reginald Wong: Mastering Reverse Engineering, Packet>, 2018
3. K.A. Monnappa: Learning Malware Analysis, Pack>, 2018
4. M. Skikorski, A. Honing: Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, No Starch Press; 1st edition , 2012
5. O. Or-Meir, Nir Nissim, Yuval Elovici, and Lior Rokach: Dynamic Malware Analysis in the Modern Era— A State of the Art Survey, ACM Computing Surveys, Vol. 52 Issue 5, October 2019, Article No.: 88, pp 1–48, 10.1145.3329786

### Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	100	4,0
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	45	2,0
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych, przygotowanie do kolokwium/egzaminu) <sup>1</sup>	55	2,0

<sup>1</sup> niepotrzebne skreślić lub dopisać inne czynności