# KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Analiza złośliwego oprogramowania [S1Cybez1>AZO]

## Przedmiot

Kierunek studiów
Cyberbezpieczeństwo

Rok/Semestr
3/5

Studia w zakresie (specjalność)
–

Profil studiów
ogólnoakademicki

Poziom studiów
pierwszego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obligatoryjny

## Liczba godzin

Wykład
16

Laboratorium
30

Inne
0

Ćwiczenia
0

Projekty/seminaria
30

## Liczba punktów ECTS

5,00

## Koordynatorzy

dr inż. Marek Michalski
marek.michalski@put.poznan.pl

dr hab. inż. Mariusz Żal
mariusz.zal@put.poznan.pl

## Wykładowcy

## Wymagania wstępne

• Znajomość podstaw programowania w językach niskopoziomowych (np. C, Assembly). • Umiejętność korzystania z systemów operacyjnych Linux i Windows na poziomie administracyjnym. • Podstawowa wiedza z zakresu sieci komputerowych oraz protokołów komunikacyjnych. • Zrozumienie podstaw kryptografii i bezpieczeństwa informacji.

## Cel przedmiotu

Celem przedmiotu jest zapoznanie studentów z metodami analizy złośliwego oprogramowania, w tym identyfikacją, dekompilacją oraz analizą funkcjonalną i behawioralną. Studenci nabędą umiejętność rozpoznawania zagrożeń, ich charakterystyki i przeciwdziałania ich skutkom.

## Przedmiotowe efekty uczenia się

Wiedza:
• Zna podstawowe typy złośliwego oprogramowania i ich charakterystykę. [K1_W06]

• Rozumie proces analizy statycznej i dynamicznej. [K1_W06]
• Zna narzędzia stosowane w analizie złośliwego oprogramowania. [K1_W09]

Umiejętności:
• Potrafi przeprowadzić analizę statyczną i dynamiczną próbek złośliwego oprogramowania. [K1_U03]
•Umie korzystać z narzędzi do analizy statycznej i dynamicznej w celu identyfikacji funkcjonalności złośliwego oprogramowania. [K1_U02]

Kompetencje społeczne:
• Docenia rolę prewencji w bezpieczeństwie IT. [K1_K05]
• Jest gotowy do samodzielnego poszerzania wiedzy o nowe zagrożenia w dynamicznie zmieniającym się świecie cyberbezpieczeństwa. [K1_K01]

## Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:
• Test zaliczeniowy w formie pisemnej lub ustnej. Pytania zamknięte i otwarte (wymagające opisu).
• Projekt laboratoryjny i ocena ćwiczeń laboratoryjnych, wykonywana w trakcie realizacji ćwiczeń.
W każdej formie zaliczenia przedmiotu ocena zależy od liczby zdobytych przez studenta punktów w stosunku do maksymalnej liczby punktów obowiązkowych. Warunkiem pozytywnego zaliczenia jest otrzymanie co najmniej 50% punktów możliwych do zdobycia. Zależność oceny od liczby punktów definiuje Regulamin Studiów. Dodatkowo zasady zaliczania przedmiotu i dokładne progi zaliczeniowe zostaną przekazane studentom na początku semestru z wykorzystaniem uczelnianych systemów elektronicznych oraz na pierwszych zajęciach (w każdej formie zajęć).

## Treści programowe

Przedmiot wprowadza studentów w zagadnienia związane z analizą złośliwego oprogramowania (malware). Omawia podstawowe techniki analizy statycznej i dynamicznej oraz narzędzia wykorzystywane w celu identyfikacji, badania i przeciwdziałania zagrożeniom wynikającym z działalności malware.

## Tematyka zajęć

1. Wprowadzenie do analizy malware: Podstawowe pojęcia, typy złośliwego oprogramowania.
2. Analiza statyczna: Badanie plików binarnych, odczytanie metadanych, analiza kodu.
3. Analiza dynamiczna: Uruchamianie malware w kontrolowanym środowisku, monitorowanie zachowania.
4. Inżynieria wsteczna: Narzędzia do dekompilacji i analizy kodu (np. IDA Pro, Ghidra).
5. Środowiska analizy: Tworzenie sandboxów i bezpiecznych środowisk testowych.
6. Przeciwdziałanie malware: Techniki ochrony i usuwania złośliwego oprogramowania.
7. Studium przypadków: analiza historycznych i aktualnych zagrożeń.
Zajęcia laboratoryjne będą obejmowały praktyczne aspekty tematów podejmowanych podczas wykładu, w tym deasemblację, analizę statyczną i dynamiczną, analiza pamięci, wykorzystanie narzędzi do analizy złośliwego oprogramowania wraz z budową bezpiecznego środowiska.

## Metody dydaktyczne

• Wykłady teoretyczne ilustrowane studiami przypadków.
• Zajęcia laboratoryjne z wykorzystaniem narzędzi analizy złośliwego oprogramowania.

## Literatura

Podstawowa:
• Michael Sikorski, Andrew Honig, Practical Malware Analysis, No Starch Press, 2012.
• Monnappa K A, Learning Malware Analysis, Packt Publishing, 2018.
• Skoudis, E., Zeltser, L. "Malware: Fighting Malicious Code", Pearson, 2003.

Uzupełniająca:

• Dokumentacje narzędzi analitycznych, np. Ghidra, Cuckoo Sandbox, Wireshark.
• National Institute of Standards and Technology (NIST)

## Bilans nakładu pracy przeciętnego studenta

| | Godzin | ECTS |
|---|---|---|
| Łączny nakład pracy | 136 | 5,00 |
| Zajęcia wymagające bezpośredniego kontaktu z nauczycielem | 76 | 3,00 |
| Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu) | 60 | 2,00 |