**Nazwa przedmiotu:**

Metody formalne i weryfikacja protokołów kryptograficznych

**Koordynator przedmiotu:**

Dr inż. Tomasz Brengos

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Matematyka

**Grupa przedmiotów:**

Wspólne

**Kod przedmiotu:**

.

**Semestr nominalny:**

2 / rok ak. 2022/2023

**Liczba punktów ECTS:**

4

**Liczba godzin pracy studenta związanych z osiągnięciem efektów uczenia się:**

1. godziny kontaktowe – 65 h; w tym
a) obecność na wykładach – 30 h
b) obecność na laboratoriach – 30 h
c) konsultacje – 5 h
2. praca własna studenta – 60 h; w tym
a) przygotowanie do laboratoriów i do kolokwum – 30 h
b) przygotowanie projektu – 30 h
Razem 125 h, co odpowiada 4 pkt. ECTS

**Liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich:**

a) obecność na wykładach – 30 h
b) obecność na laboratoriach – 30 h
c) konsultacje – 5 h
Razem 65 h, co odpowiada 3 pkt. ECTS

**Język prowadzenia zajęć:**

polski

**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym:**

.

**Formy zajęć i ich wymiar w semestrze:**

|  |  |
| --- | --- |
| Wykład: | 30h |
| Ćwiczenia: | 0h |
| Laboratorium: | 30h |
| Projekt: | 0h |
| Lekcje komputerowe: | 0h |

**Wymagania wstępne:**

Algebra i Jej Zastosowania, Elementy Logiki i Teorii Mnogości

**Limit liczby studentów:**

Bez limitu

**Cel przedmiotu:**

Zapoznanie studentów z podstawowymi pojęciami teorii informacji oraz ich zastosowaniami

**Treści kształcenia:**

1. Logika intuicjonistyczna, logika rachunku zdań, logika pierwszego rzędu: dedukcja naturalna, rachunek sekwentów, eliminacja reguły „cut”.
2. (Typowany) rachunek lambda: definicje, własności. Izomorfizm Curriego-Howarda.
3. Wprowadzenie do teorii typów: definicje, własności.
4. Wprowadzenie do programowanie w Agda.
5. Dowodzenie programów w Agda w praktyce, terminacja.
6. Systemy komunikujące się: rachunek CCS, rachunek Pi i ich zastosowania w weryfikacji protokołów kryptograficznych.
7. Wstęp do systemu ProVerif.

**Metody oceny:**

Metody oceniania:
Jedno kolokwium sprawdzające. Ocena aktywności na zajęciach (rozwiązywania zadań przy tablicy i przygotowywanych referatów). Projekt.
Regulamin zaliczenia:
Student może zdobyć od 0 do 100 punktów z ćwiczeń
(60 punków za kolokwium i aktywność, 40 pkt z projektu).
Aby zaliczyć ćwiczenia należy uzyskać z nich co najmniej 50 punktów.
Ocena końcowa wystawiana jest w następujący sposób:
Suma zdobytych punktów 0 – 50 51 – 60 61 – 70 71 – 80 81 – 90 91 – 100
Ocena końcowa 2 3 3,5 4 4,5 5

**Egzamin:**

nie

**Literatura:**

1. “Program = Proof”, Samuel Mimram, Independently Published 2020
2. “ProVerif 2.02pl1: Automatic Cryptographic Protocol Verifier, User Manual and Tutorial”, B. Blanchet, B. Smyth, V. Cheval, M. Sylverstre, Independently Published 2020

**Witryna www przedmiotu:**

brak

**Uwagi:**

## Charakterystyki przedmiotowe

### Profil ogólnoakademicki - wiedza

**Charakterystyka MF\_W01:**

Ma pogłębioną wiedzę dotyczącą modeli analitycznych, probabilistycznych, algebraicznych. Ma pogłębioną wiedzę w zakresie wybranych struktur algebraicznych występujących w matematyce i w zastosowaniach w cyberbezpieczeństwie.

Weryfikacja:

Kolokwium, projekt

**Powiązane charakterystyki kierunkowe:** M2\_W01, M2MCB\_W01

**Powiązane charakterystyki obszarowe:**

**Charakterystyka MF\_W02:**

Ma podstawową wiedzę dotyczącą uwarunkowań badawczych w zakresie modelowania matematycznego i posiada ogólną wiedzę o aktualnych kierunkach rozwoju i najnowszych odkryciach w zakresie matematyki.

Weryfikacja:

Kolokwium, projekt

**Powiązane charakterystyki kierunkowe:** M2\_W02, M2\_W03

**Powiązane charakterystyki obszarowe:**

**Charakterystyka MF\_W03:**

Zna podstawowe zagadnienia zastosowań metod formalnych w cyberbezpieczeństwie.

Weryfikacja:

Kolokwium, projekt

**Powiązane charakterystyki kierunkowe:** M2MCB\_W13

**Powiązane charakterystyki obszarowe:**

### Profil ogólnoakademicki - umiejętności

**Charakterystyka MF\_U01:**

Potrafi za pomocą narzędzi metod formalnych zweryfikować poziom bezpieczeństwa systemów cyfrowych.

Weryfikacja:

Kolokwium, projekt

**Powiązane charakterystyki kierunkowe:**

**Powiązane charakterystyki obszarowe:**

### Profil ogólnoakademicki - kompetencje społeczne

**Charakterystyka MF\_K01:**

Rozumie przydatność nabytej wiedzy i umiejętności obliczeniowych do stawiania hipotez oraz ich weryfikacji w możliwych zastosowaniach.

Weryfikacja:

Projekt

**Powiązane charakterystyki kierunkowe:** M2MCB\_K02

**Powiązane charakterystyki obszarowe:**