



113-17-5

## BEZPIECZEŃSTWO TELEINFORMATYCZNE

ECTS: 8

## TELE-INFORMATION SECURITY

### TREŚCI WYKŁADÓW

1. Podstawowe pojęcia 2. Modele bezpieczeństwa informacji 3. Analiza zagrożeń i zabezpieczeń systemów teleinformatycznych i komputerowych 4. Planowanie odtwarzania systemów 5. Kryptograficzna ochrona informacji 6. Typy ataków na systemy teleinformatyczne i komputerowe

### TREŚCI ĆWICZEŃ

1. Metody szyfrowania, funkcje skrótu, itp. 2. Bezpieczeństwo sieci przewodowych i bezprzewodowych 3. Tworzenie i przywracanie kopii bezpieczeństwa 4. Systemy kontroli dostępu 5. Systemy kontroli ruchu sieciowego 6. Zaawansowane rozwiązania antywirusowe 7. Wykonywanie ataków na systemy teleinformatyczne i komputerowe 8. Wirtualne sieci prywatne VPN 9. Stosowanie mechanizmów redundancji

### CEL KSZTAŁCENIA

Celem przedmiotu jest zapoznanie studenta z podstawami modeli bezpieczeństwa informacji w systemach komputerowych, analizą ryzyka i zabezpieczaniu informacji oraz sposobów odtwarzania informacji i systemów informatycznych.

### OPIS EFEKTÓW KSZTAŁCENIA PRZEDMIOTU W ODNIESIENIU DO OBSZAROWYCH I KIERUNKOWYCH EFEKTÓW KSZTAŁCENIA

**Symbole efektów obszarowych** T1A\_W02, T1A\_W03, T1A\_W04, T1A\_W05, T1A\_U01, T1A\_U03, T1A\_U05, T1A\_U07, T1A\_U10, T1A\_U12, T1A\_U15, T1A\_U16, T1A\_U18, T1A\_K01, T1A\_K04

**Symbole efektów kierunkowych** K\_W12, K\_W13, K\_U01, K\_U03, K\_U05, K\_U18, K\_K01, K\_K04.

### EFEKTY KSZTAŁCENIA

#### Wiedza

Student posiada wiedzę nt. modeli bezpieczeństwa informacji, zna potencjalne zagrożenia dla bezpieczeństwa informacji oraz metody zabezpieczenia informacji w systemach komputerowych (K2\_W12, K2\_W13)

#### Umiejętności

Student jest w stanie zidentyfikować najpoważniejsze zagrożenia dla bezpieczeństwa informacji w systemach komputerowych oraz zastosować mechanizmy przeciwdziałające. Student potrafi wykorzystać rozwiązania zwiększające bezpieczeństwo przechowywanych informacji np. metody szyfrowania czy systemy kontroli dostępu do informacji. Student jest w stanie opracować optymalną metodę archiwizacji danych firmowych oraz szybkiego przywracania systemu informacyjnego do sprawności w sytuacji awarii (K\_U01, K\_U03, K\_U05, K\_U18)

#### Kompetencje społeczne

Student docenia ważność bezpieczeństwa informacji w ciągłości procesów biznesowych firmy. Student zachowuje otwartość na nowoczesne rozwiązania zwiększające bezpieczeństwo. Student utrzymuje sprawność powierzonych systemów informacyjnych i jest w stanie szybko i sprawnie przywrócić je do działania w przypadku wystąpienia awarii (K\_K01, K\_K04)

### LITERATURA PODSTAWOWA

1) Krzysztof Liderman, 2012r., "Bezpieczeństwo Informatyczne", wyd. Wydawnictwo Naukowe PWN, 2) N. Ferguson, 2004r., "Kryptografia w praktyce", wyd. Helion, 3) Kancelaria Sejmu, "USTAWA z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych, Dz.U.1999 nr 11 poz. 95", 4) Kancelaria Sejmu, "ROZPORZĄDZENIE PREZESA RADY MINISTRÓW z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. z dnia 8 września 2005 r.)", 5) Liderman Krzysztof, 2009r., "Podręcznik Administratora Bezpieczeństwa Teleinformatycznego", wyd. Wydawnictwo Naukowe PWN.

**Przedmiot/moduł:**  
BEZPIECZEŃSTWO TELEINFORMATYCZNE

**Obszar kształcenia:** nauki techniczne

**Status przedmiotu:** Obligatoryjny

**Kod ECTS:** 113-17-5

**Nazwa studiów podyplomowych/kursu:**  
Zaawansowane technologie informatyczne

**Forma studiów:** Niestacjonarne

**Poziom studiów/Forma kształcenia:** Studia podyplomowe/kurs dokształcający

**Rok/semestr:** 1/1

**Rodzaje zajęć:** wykłady/ćwiczenia

**Liczba godzin w semestrze**

wykłady: 10/2

ćwiczenia: 30/6

**Formy i metody dydaktyczne**

**wykłady:** wykład z prezentacją multimedialną

**ćwiczenia:** pisanie skryptów wspomagających prace administratora systemu

**Forma i warunki zaliczenia:** Zaliczenie na ocenę/

Obecność na zajęciach, aktywność, wykonanie wszystkich zadań laboratoryjnych, zaliczenie końcowe na ocenę.

**Liczba punktów ECTS:** 8

**Język wykładowy:** polski

**Wymagania wstępne:**

**Nazwa jednostki organizacyjnej realizującej**

**przedmiot:**

Wydział Matematyki i Informatyki

**adres:** , ,

**Osoba odpowiedzialna za realizację przedmiotu:**

mgr inż. Łukasz Dylewski

## Szczegółowy opis przyznanej punktacji ECTS - część B

### BEZPIECZEŃSTWO TELEINFORMATYCZNE TELE-INFORMATION SECURITY

ECTS: 8

Na przyznaną liczbę punktów ECTS składają się :

1. Godziny kontaktowe z nauczycielem akademickim:

- udział w wykładach	10,0 godz.
- udział w ćwiczeniach	30,0 godz.
- udział w konsultacjach	20,0 godz.
- omówienie wyników zaliczenia przedmiotu	5,0 godz.
	65,0 godz.

2. Samodzielna praca studenta:

- przygotowanie się do ćwiczeń	50,0 godz.
- samodzielne rozwiązywanie zadań domowych	45,0 godz.
- przygotowanie się do kolokwium	40,0 godz.
	135,0 godz.

godziny kontaktowe + samodzielna praca studenta OGÓŁEM: 200,0 godz.

1 punkt ECTS = 25,00 godz. pracy przeciętnego studenta,

liczba punktów ECTS = 200,00 godz.: 25,00 godz./ECTS = **8,00 ECTS**

w zaokrągleniu: **8 ECTS**

- w tym liczba punktów ECTS za godziny kontaktowe z bezpośrednim udziałem nauczyciela akademickiego - **2,60** punktów ECTS,

- w tym liczba punktów ECTS za godziny realizowane w formie samodzielnej pracy studenta - **5,40** punktów ECTS.