Załącznik nr 5

KARTA PRZEDMIOTU

I. Dane podstawowe

Nazwa przedmiotu	Zagrożenia w sieci
Nazwa przedmiotu w języku angielskim	Cybersecurity
Kierunek studiów	humanistyka cyfrowa
Poziom studiów (I, II, jednolite magisterskie)	II stopień, magisterskie
Forma studiów (stacjonarne, niestacjonarne)	stacjonarne
Dyscyplina	literaturoznawstwo
Język wykładowy	polski

Koordynator przedmiotu/osoba odpowiedzialna	dr hab. Rafał Lizut, prof. DDUVS

Forma zajęć *(katalog zamknięty ze słownika)*	Liczba godzin	semestr	Punkty ECTS
wykład			
konwersatorium			
ćwiczenia			
laboratorium			
warsztaty	30	III	2
seminarium			
proseminarium			
lektorat			
praktyki			
zajęcia terenowe			
pracownia dyplomowa			
translatorium			
wizyta studyjna			

Wymagania wstępne	Znajomość podstaw sieci i obsługi komputera

II. Cele kształcenia dla przedmiotu

C1. Zapoznanie studentów z podstawowymi pojęciami, koncepcjami i obszarami z obszaru bezpieczeństwa w sieci
C2. Zapoznanie studentów z podstawowymi atakami w sieci i metodami zabezpieczeń przed nimi

III. Efekty uczenia się dla przedmiotu wraz z odniesieniem do efektów kierunkowych

Symbol	Opis efektu przedmiotowego	Odniesienie do efektu kierunkowego
WIEDZA		
W_01	Student rozpoznaje i rozumie podstawowe pojęcia z obszaru bezpieczeństwa informacyjnego. Identyfikuje podstawowe zagrożenia dla bezpieczeństwa informacji oraz systemów informatycznych	K_W07
UMIEJĘTNOŚCI		
U_01	Student identyfikuje potrzebę aktualizacji swojej wiedzy dostosowując ją do wymagań bezpieczeństwa w sieci oraz ewolucji rozwiązań technologicznych.	K_U07
U_02	Student rozumie potrzebę tworzenia i wdrożenia polityki bezpieczeństwa w sieci	K_U05
KOMPETENCJE SPOŁECZNE		
K_01	Student potrafi prawidłowo interpretować kwestie bezpieczeństwa w sieci w kontekście funkcjonowania społeczeństwa.	K_K02
K_02	Student promuje odpowiedzialne postawy w odniesieniu do bezpieczeństwa informatycznego w sytuacjach prywatnych i biznesowych	K_K05

IV. Opis przedmiotu/ treści programowe

Istota i znaczenie bezpieczeństwa w sieci. Podstawowe definicje: polityka bezpieczeństwa, bezpieczeństwo, dostępność, poufność, nienaruszalność, zasady bezpieczeństwa. Atrybuty ochrony informacji: tajność, integralność, dostępność, niezaprzeczalność, autentyczność. Techniki włamań i ataków: inżynieria społeczna, odgadywanie haseł, podsłuchiwanie, podszywanie się, paraliżowanie systemu, wywoływanie błędów, wirusy, podmiana systemu zabezpieczeń.

V. Metody realizacji i weryfikacji efektów uczenia się

Symbol efektu	Metody dydaktyczne *(lista wyboru)*	Metody weryfikacji *(lista wyboru)*	Sposoby dokumentacji *(lista wyboru)*
WIEDZA			
W_01	Wykład problemowy	Kolokwium	Uzupełnione i ocenione kolokwium
UMIEJĘTNOŚCI			
U_01	Studium przypadku (case study)	Kolokwium	Uzupełnione i ocenione kolokwium
U_02	Wykład problemowy	Kolokwium	Uzupełnione i ocenione kolokwium
KOMPETENCJE SPOŁECZNE			
K_01, K_02	Wykład problemowy	Kolokwium	Uzupełnione i ocenione kolokwium

VI. Kryteria oceny, wagi…

Zaliczenie na podstawie kolokwium
100% - kolokwium

Kryteria oceny:
Ocena bardzo dobra 91%-100%
Ocena dobra 71%-90%
Ocena dostateczna 51%-70%
Ocena niedostateczna równe lub mniejsze 50%

VII. Obciążenie pracą studenta

Forma aktywności studenta	Liczba godzin
Liczba godzin kontaktowych z nauczycielem	**30**
Liczba godzin indywidualnej pracy studenta	**30**

VIII. Literatura

Literatura podstawowa
Liderman K., *Bezpieczeństwo informacyjne,* Warszawa 2017. Liderman K., *Bezpieczeństwo teleinformatyczne*, Warszawa 2006. Molski M., Opala S., *Elementarz bezpieczeństwa systemów informatycznych,* Warszawa 2002. Pipkin D. L., *Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa,* Warszawa 2002. Maiwald E., *Bezpieczeństwo w sieci,* Kraków 2002.
Literatura uzupełniająca
RSA Security. A Guide to Security Policy. Bedford, MA, USA 2000. Schneier B. *Kryptografia dla praktyków,* Warszawa 2002.