

KARTA PRZEDMIOTU

Cykl kształcenia od roku akademickiego: 2022/2023

I. Dane podstawowe

Nazwa przedmiotu	Bezpieczeństwo 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

Koordinator przedmiotu/osoba odpowiedzialna	mgr Dawid Kowalczyk
---	---------------------

Forma zajęć (<i>katalog zamknięty ze słownika</i>)	Liczba godzin	semestr	Punkty ECTS
wykład			1
konwersatorium			
ćwiczenia			
laboratorium			
warsztaty	15	3	
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. Student nabywa podstawową wiedzę z zakresu bezpieczeństwa w sieci.
C2. Student zapoznaje się z technikami ataków w sieci oraz poznaje praktyczne metody zabezpieczenia się 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, w skomplikowanych przypadkach korzystając z pomocy specjalistów.	K_U04
U_02	Student stosując różnorodne nowoczesne narzędzia rozumie potrzebę tworzenia i wdrożenia polityki bezpieczeństwa w sieci.	K_U08
KOMPETENCJE SPOŁECZNE		
K_01	Student promuje odpowiedzialne postawy w odniesieniu do bezpieczeństwa informatycznego w sytuacjach prywatnych i biznesowych	K_K05

IV. Opis przedmiotu/ treści programowe

<ol style="list-style-type: none"> 1. Znaczenie i istota bezpieczeństwa w sieci: polityka bezpieczeństwa, dostępność, poufność, nienaruszalność, zasady bezpieczeństwa, analiza ryzyka. 2. Rodzaje informacji chronionych. 3. Atrybuty ochrony informacji: tajność, integralność, dostępność, niezaprzeczalność, autentyczność. 4. Techniki włamań i ataków: inżynieria społeczna, odgadywanie haseł, wirtualne śledzenie, podsłuchiwanie, celowe wywoływanie błędów, paraliż systemu. 5. Fizyczne zagrożenia dotyczące dostępu do usług. 6. Metody wykrywania i zapobiegania ataków. 7. Kryptografia. 8. Podpis elektroniczny. 9. Sieci otwarte i zamknięte. 10. Wirus, bot, exploit, robak, DDOS-y.

V. Metody realizacji i weryfikacji efektów uczenia się

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

VI. Kryteria oceny, wagi...

Zaliczenie na podstawie wyników uzyskanych na kolokwium:

90% - kolokwium

10% - obecność na zajęciach (dopuszczalne są dwie nieobecności)

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	15
Liczba godzin indywidualnej pracy studenta	15

VIII. Literatura

Literatura podstawowa
Liderman K., <i>Bezpieczeństwo informacyjne</i> , Warszawa 2017.
Liderman K., <i>Bezpieczeństwo teleinformatyczne</i> , Warszawa 2006.
Molski M., Opala S., <i>Elementarz bezpieczeństwa systemów informatycznych</i> , Warszawa 2002.
Pipkin D. L., <i>Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa</i> , przeł. E. Andrukiewicz, Warszawa 2002.
Maiwald E., <i>Bezpieczeństwo w sieci</i> , przeł. K. Stankiewicz, Kraków 2002.
Literatura uzupełniająca
Liderman K., <i>Analiza ryzyka i ochrona informacji w systemach komputerowych</i> , Warszawa 2009.
<i>RSA Security. A Guide to Security Policy</i> . Bedford, MA, USA 2000.
Schneier B. <i>Kryptografia dla praktyków</i> , przeł. R. Rykaczewski, R. Sobczak, P. Szpryngier, Warszawa 2002.
Stallings W., <i>Kryptografia i bezpieczeństwo sieci komputerowych. Konceptcje i metody bezpiecznej komunikacji</i> , przeł. Andrzej Grażyński, Gliwice 2012.