Załącznik nr 5

KARTA PRZEDMIOTU

Cykl kształcenia od roku akademickiego: 2023/2024

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

Koordynator przedmiotu/osoba odpowiedzialna	mgr Dawid Kowalczyk

Forma zajęć *(katalog zamknięty ze słownika)*	Liczba godzin	semestr	Punkty ECTS
wykład			2
konwersatorium			
ćwiczenia			
laboratorium			
warsztaty	30	4	
seminarium			
proseminarium			
lektorat			
praktyki			
zajęcia terenowe			
pracownia dyplomowa			
translatorium			
wizyta studyjna			

Wymagania wstępne	Znajomość obsługi komputera.

II. Cele kształcenia dla przedmiotu

C1. Przygotowanie studentów do świadomego i bezpiecznego korzystania z sieci internetowej.
C2. Zapoznanie studentów z technikami ataków w sieci oraz wykształcenia podstawowych metod 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 identyfikuje podstawowe pojęcia z obszaru bezpieczeństwa informacyjnego oraz zagrożenia dla systemów informatycznych.	K_W07
UMIEJĘTNOŚCI		
U_01	Student debatuje na tematy wymagań bezpieczeństwa w sieci oraz ewolucji rozwiązań technologicznych.	K_U04
U_02	Student stosuje różnorodne cyfrowe narzędzia szyfrowania i wdraża zasady polityki bezpieczeństwa w sieci.	K_U08
KOMPETENCJE SPOŁECZNE		
K_01	Student stosuje się do zasad higieny cybernetycznej w sytuacjach prywatnych.	K_K05

IV. Opis przedmiotu/ treści programowe

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. Zagrożenia w sieci Wirus, bot, exploit, robak, DDOS-y.

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	Miniwykład konwersatoryjny	Kolokwium	Uzupełnione, sprawdzone i ocenione kolokwium
UMIEJĘTNOŚCI			
U_01	Studium przypadku (case study), dyskusja	Kolokwium, obserwacja	Uzupełnione, sprawdzone i ocenione Kolokwium, zapis w dzienniku ocen (ocena, plus/minus)
U_02	Gra dydaktyczna	Krótkie zadanie (quiz)	Zapis w dzienniku ocen (ocena, plus/minus)

KOMPETENCJE SPOŁECZNE			
K_01	Gra dydaktyczna, dyskusja	Kolokwium, obserwacja, krótkie zadanie (quiz)	Uzupełnione, sprawdzone i ocenione Kolokwium, zapis w dzienniku ocen (ocena, plus/minus)

VI. Kryteria oceny, wagi…

Bezwzględnym warunkiem zaliczenia pracy pisemnej/multimedialnej jest jej samodzielne przygotowanie rozumiane jako opracowanie powstałe w zgodzie z prawem autorskim i prawami pokrewnymi oraz zasadami etyki wykorzystania narzędzi cyfrowych, np. opartych o sztuczną inteligencję.

Zaliczenie na podstawie wyników uzyskanych na kolokwium:
90% - kolokwium zaliczone na pozytywną ocenę
10% - aktywność na zajęciach (nagradzana plusami stawianymi w liście obecności, nie może być ich mniej niż cztery)

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

Dopuszczalne są dwie nieobecności, a pozostałe – muszą być zaliczone w sposób wyznaczony przez prowadzącego.

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. Molski M., Opala S., *Elementarz bezpieczeństwa systemów informatycznych,* Warszawa 2002. Pipkin D. L., *Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa,* przeł. E. Andrukiewicz, Warszawa 2002. Steinberg J., *Cyberbezpieczeństwo dla bystrzaków*, Gliwice 2023.
Literatura uzupełniająca
Liderman K., Analiza ryzyka i ochrona informacji w systemach komputerowych, Warszawa 2009. *RSA Security. A Guide to Security Policy*. Bedford, MA, USA 2000. Mitnick K., Simon W. L., *Sztuka podstępu. Łamałem ludzi nie hasła*, przeł. J. Dobrzański, Gliwice 2016. Schneier B., *Kryptografia dla praktyków***,** przeł. R. Rykaczewski, R. Sobczak, P. Szpryngier, Warszawa 2002. Stallings W., *Kryptografia i bezpieczeństwo sieci komputerowych. Koncepcje i metody bezpiecznej komunikacji*, przeł. Andrzej Grażyński, Gliwice 2012.