

KARTA PRZEDMIOTU

1. Informacje wstępne

Nazwa przedmiotu	Warsztat cyberbezpieczeństwa
Wydział	Wydział Zarządzania i Komunikacji Społecznej
Kierunek	Dziennikarstwo i komunikacja społeczna
Specjalność/Ścieżka specjalizacyjna	—
Poziom PRK	6 PRK
Poziom kształcenia	studia pierwszego stopnia
Forma studiów	studia stacjonarne
Grupa zajęć	—
Liczba punktów ECTS	2
Rodzaj przedmiotu	obowiązkowy
Liczba godzin ogółem	20 godz.
Cykl dydaktyczny	2023/2024 zimowy
Semestr studiów	4
Rok studiów	2
Profil kształcenia	praktyczny
Rok realizacji	2024/2025
Język wykładowy	polski
Osoba odpowiedzialna za przedmiot	mgr Lech Mikulski (e-mail: lmikulski@uafm.edu.pl)

Semestr, liczba punktów ECTS, rodzaj zajęć, liczba godzin w planie studiów

Semestr	Ćwiczenia
4	20 godz. 2 ECTS

2. Cele przedmiotu

C1	Zaznajomienie z podstawami cyberbezpieczeństwa. Poznanie terminologii oraz nabycie podstawowych umiejętności z zakresu cyberbezpieczeństwa.
----	---

3. Wymagania wstępne

Brak.

4. Opis efektów uczenia się

W1	Wiedza: Student wie jak rozpoznać potencjalne zagrożenia z zakresu cyberbezpieczeństwa.	EUK6_W5, EUK6_W6
U1	Umiejętności: Student umie korzystać ze współczesnych narzędzi komunikacji zachowując dbałość o jej bezpieczeństwo.	EUK6_U3
K1	Kompetencje społeczne: Student potrafi samodzielnie rozwijać swoje umiejętności z zakresu cyberbezpieczeństwa, rozumie potrzebę zdobywania wiedzy z jej zakresu.	EUK6_KS1

5. Treści programowe

Ćwiczenia (20 godz.)

Kod	Tematyka zajęć (nr semestru: 4)
Cw1	Wstęp do cyberbezpieczeństwa – 2 h
Cw2	Rodzaje cyberataków oraz metody zapobiegania – 2 h
Cw3	Bezpieczeństwo urządzeń mobilnych – 2 h
Cw4	Komunikatory i ich bezpieczeństwo – 2 h
Cw5	E-mail – struktura maila i protokoły, szyfrowanie korespondencji, możliwe zagrożenia i zabezpieczenia – 4 h
Cw6	Socjotechnika – studia przypadku – 2 h
Cw7	Wojna informacyjna - propaganda, boty i trolle – 2 h
Cw8	Przeglądarki i wyszukiwarki oraz ich specyfika działania – 2 h
Cw9	Prywatność i anonimowość w Internecie – 2 h

6. Metody dydaktyczne

Ćwiczenia	
M1	Analiza przypadków
M4	Ćwiczenia komputerowe

7. Nakład pracy studenta

Forma aktywności studenta	Obciążenie studenta
Ćwiczenia	20 godz.
W tym metodą e-learning:	0 godz.

Praca własna studenta	
Praca własna studenta, zapoznanie się z literaturą	30 godz.

Całkowite obciążenia	
Sumaryczna liczba godzin dla przedmiotu wynikająca z całego nakładu pracy studenta	50 godz.
Sumaryczna liczba punktów ECTS dla przedmiotu	2 ECTS

8. Kryteria oceny

Warunki zaliczenia przedmiotu:

Aktywne uczestnictwo w zajęciach oraz wykonanie ćwiczeń w ich trakcie, a następnie udokumentowanie swoich osiągnięć, w zależności od tematu, w sposób wskazany przez prowadzącego.

Ćwiczenia	
Na ocenę 5:	Student przejawia wysokie zainteresowanie tematyką cyberbezpieczeństwa. W stopniu bardzo dobrym jest w stanie rozpoznać możliwe zagrożenia i podjąć właściwe środki zaradcze zapewniające mu bezpieczeństwo.
Na ocenę 4,5:	Student przejawia ponad przeciętne zainteresowanie tematyką cyberbezpieczeństwa. W stopniu dobrym jest w stanie rozpoznać możliwe zagrożenia i podjąć właściwe środki zaradcze zapewniające mu bezpieczeństwo.
Na ocenę 4:	Student przejawia przeciętne zainteresowanie tematyką cyberbezpieczeństwa. W stopniu dobrym jest w stanie rozpoznać możliwe zagrożenia i podjąć właściwe środki zaradcze zapewniające mu bezpieczeństwo.
Na ocenę 3,5:	Student przejawia umiarkowane zainteresowanie tematyką cyberbezpieczeństwa. W stopniu dostatecznym jest w stanie rozpoznać możliwe zagrożenia, ale może mieć kłopot z samodzielnym podjęciem właściwych środków zaradczych by zadbać o swoje bezpieczeństwo.
Na ocenę 3:	Student przejawia znikome zainteresowanie tematyką cyberbezpieczeństwa. W stopniu podstawowym jest w stanie rozpoznać możliwe zagrożenia, ale może mieć kłopot z podjęciem właściwych środków zaradczych by zadbać o swoje bezpieczeństwo.

9. Literatura

Literatura podstawowa

1. Steinberg, Joseph – Cyberbezpieczeństwo dla bystrzaków, Gliwice, 2023, Helion
2. Mierzyńska, Anna – Efekt niszczący. Jak dezinformacja wpływa na nasze życie, Warszawa, 2022, Wydawnictwo Agora
3. Aro, Jessikka – Trolle Putina, Kraków, 2020, Wydawnictwo SQN

Literatura uzupełniająca

1. Mitnick, Kevin; Wozniak, Steve (Foreword); Simon, William L. (Contributor) – Duch w sieci. Moje przygody jako najbardziej poszukiwanego hakera wszech czasów, Gliwice, 2022, Helion
2. Mitnick, Kevin; Simon, William L. – Sztuka podstęp. Łamałem ludzi, nie hasła., Gliwice, 2024, Helion

Publikacje prowadzącego

1. Mikulski, Lech – Cyberbezpieczeństwo i Cyberobrona. Instrukcja dla osób w sytuacji zagrożenia, Kraków, 2023, wyd. własne [e-book dostępny na stronie autora: lechmikulski.com -> w zakładce Cyberbezpieczeństwo, dostęp: 21.11.2024]

10. Informacje dodatkowe dla studentów

Szanowni Państwo,

w razie pytań można się ze mną skontaktować pod służbowym adresem e-mail lmikulski@afm.edu.pl lub spotkać się ze mną na dyżurze.

Z poważaniem

Lech Mikulski

11. Informacja o osobach prowadzących zajęcia

Osoby prowadzące zajęcia

mgr Lech Mikulski (e-mail: lmikulski@uafm.edu.pl)