

POLITECHNIKA KRAKOWSKA IM. TADEUSZA KOŚCIUSZKI

KARTA PRZEDMIOTU

obowiązuje studentów rozpoczynających studia w roku akademickim 2021/2022

Wydział Informatyki i Telekomunikacji

Kierunek studiów: Informatyka

Profil: Ogólnoakademicki

Forma studiów: stacjonarne

Kod kierunku: I

Stopień studiów: II

Specjalności: Cyberbezpieczeństwo

1 INFORMACJE O PRZEDMIOCIE

NAZWA PRZEDMIOTU	Wstęp do cyberbezpieczeństwa
NAZWA PRZEDMIOTU W JĘZYKU ANGIELSKIM	Introduction to Cybersecurity
KOD PRZEDMIOTU	WiIT I oIIS D2 21/22
KATEGORIA PRZEDMIOTU	Przedmioty specjalnościowe
LICZBA PUNKTÓW ECTS	3.00
SEMESTRY	1

2 RODZAJ ZAJĘĆ, LICZBA GODZIN W PLANIE STUDIÓW

SEMESTR	WYKŁAD	ĆWICZENIA	LABORATORIUM	LABORATORIUM KOMPUTERO- WE	SEMINARIUM	PROJEKT
1	15	0	0	0	0	0

3 CELE PRZEDMIOTU

Cel 1 Wprowadzenie podstawowych pojęć związanych z cyberbezpieczeństwem.

Cel 2 Zapoznanie z zagrożeniami płynącymi z użytkowania sieci lokalnej oraz Internet, a także aplikacji i systemów operacyjnych, w tym usług bankowych.

Cel 3 Zapoznanie z polskimi i europejskimi regulacjami prawnymi w zakresie ochrony cyberprzestrzeni oraz bezpieczeństwa przechowywania i przetwarzania danych osobowych.

Cel 4 Zapoznanie z podstawowymi metodami i pojęciami z zakresu kryptografii.

Cel 5 Wprowadzenie w temat bezpieczeństwa infrastruktury krytycznej.

4 WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

5 EFEKTY KSZTAŁCENIA

EK1 Wiedza Student objaśnia podstawowe pojęcia z zakresu cyberbezpieczeństwa.

EK2 Wiedza Student posiada elementarną znajomość przepisów prawa polskiego i europejskiego w dziedzinie ochrony cyberprzestrzeni oraz bezpieczeństwa przechowywania i przetwarzania danych osobowych.

EK3 Umiejętności Student potrafi analizować i wykorzystywać uzyskaną wiedzę do identyfikacji i klasyfikacji napotkanych zagrożeń w cyberprzestrzeni.

EK4 Umiejętności Student potrafi podejmować działania mające na celu eliminację lub zmniejszenie ryzyka wystąpienia zagrożeń w cyberprzestrzeni.

EK5 Kompetencje społeczne Student ma świadomość wpływu cyfryzacji na społeczeństwo oraz zagrożeń jakie nowe technologie generują. Ponadto Student potrafi aktywnie uczestniczyć w dyskusji poświęconej zagadnieniom cyberbezpieczeństwa.

6 TREŚCI PROGRAMOWE

WYKLAD		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
W1	Podstawowe pojęcia z zakresu cyberbezpieczeństwa	1
W2	Wybrane zagrożenia sieciowe	3
W3	Krajowy i europejski system cyberbezpieczeństwa	1
W4	Przepisy prawa polskiego i europejskiego w dziedzinie ochrony cyberprzestrzeni	1
W5	Prawna ochrona dzieci i młodzieży	1
W6	Bezpieczeństwo przechowywania i przetwarzania danych	2
W7	Bezpieczeństwo usług bankowych	1
W8	Bezpieczeństwo infrastruktury krytycznej	1
W9	Podstawy kryptografii i podpisów cyfrowych	1
W10	Deep web i dark web	1
W11	Bezpieczeństwo aplikacji i systemów operacyjnych	2

7 NARZĘDZIA DYDAKTYCZNE

N1 Wykłady (w przypadku realizacji zajęć w trybie zdalnym z wykorzystaniem stosownych narzędzi teleinformatycznych)

N2 Prezentacje multimedialne

N3 Dyskusja

N4 MS Teams

8 OBCIĄŻENIE PRACĄ STUDENTA

FORMA AKTYWNOŚCI	ŚREDNIA LICZBA GODZIN NA ZREALIZOWANIE AKTYWNOŚCI
Godziny kontaktowe z nauczycielem akademickim, w tym:	
Godziny wynikające z planu studiów	15
Konsultacje przedmiotowe	35
Egzaminy i zaliczenia w sesji	0
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	40
Opracowanie wyników	0
Przygotowanie raportu, projektu, prezentacji, dyskusji	0
SUMARYCZNA LICZBA GODZIN DLA PRZEDMIOTU WYNIKAJĄCA Z CAŁEGO NAKŁADU PRACY STUDENTA	90
SUMARYCZNA LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU	3.00

9 SPOSOBY OCENY

OCENA PODSUMOWUJĄCA

P1 Zaliczenie pisemne

WARUNKI ZALICZENIA PRZEDMIOTU

W1 Uzyskanie pozytywnej oceny z zaliczenia pisemnego.

W2 Uzyskanie pozytywnej oceny z każdego efektu kształcenia.

KRYTERIA OCENY

EFEKT KSZTAŁCENIA 1	
NA OCENĘ 2.0	Student nie spełnia warunków określonych dla oceny 3.0.
NA OCENĘ 3.0	Student uzyskuje co najmniej 51% z testu zaliczeniowego - pełne kryterium opisano na ocenę 5.0.
NA OCENĘ 3.5	Student uzyskuje co najmniej 61% z testu zaliczeniowego - pełne kryterium opisano na ocenę 5.0.
NA OCENĘ 4.0	Student uzyskuje co najmniej 71% z testu zaliczeniowego - pełne kryterium opisano na ocenę 5.0.
NA OCENĘ 4.5	Student uzyskuje co najmniej 81% z testu zaliczeniowego - pełne kryterium opisano na ocenę 5.0.
NA OCENĘ 5.0	Student potrafi w sposób formalny, zrozumiały i bezbłędny zdefiniować pojęcia z zakresu bezpieczeństwa cyberprzestrzeni. Student podpira definicje wieloma przykładami obrazującymi omawiane pojęcia. Student uzyskuje co najmniej 91% z testu zaliczeniowego.
EFEKT KSZTAŁCENIA 2	
NA OCENĘ 2.0	Student nie spełnia warunków określonych dla oceny 3.0.
NA OCENĘ 3.0	Student uzyskuje co najmniej 51% z testu zaliczeniowego - pełne kryterium opisano na ocenę 5.0.
NA OCENĘ 3.5	Student uzyskuje co najmniej 61% z testu zaliczeniowego - pełne kryterium opisano na ocenę 5.0.
NA OCENĘ 4.0	Student uzyskuje co najmniej 71% z testu zaliczeniowego - pełne kryterium opisano na ocenę 5.0.
NA OCENĘ 4.5	Student uzyskuje co najmniej 81% z testu zaliczeniowego - pełne kryterium opisano na ocenę 5.0.
NA OCENĘ 5.0	Student posiada szczegółową wiedzę z zakresu podstawowych pojęć prawa polskiego i europejskiego - w tym rozporządzenie Parlamentu Europejskiego i Rady (UE) w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych. Student uzyskuje co najmniej 91% z testu zaliczeniowego.
EFEKT KSZTAŁCENIA 3	
NA OCENĘ 2.0	Student nie spełnia warunków określonych dla oceny 3.0.
NA OCENĘ 3.0	Student uzyskuje co najmniej 51% z testu zaliczeniowego - pełne kryterium opisano na ocenę 5.0.
NA OCENĘ 3.5	Student uzyskuje co najmniej 61% z testu zaliczeniowego - pełne kryterium opisano na ocenę 5.0.
NA OCENĘ 4.0	Student uzyskuje co najmniej 71% z testu zaliczeniowego - pełne kryterium opisano na ocenę 5.0.

NA OCENĘ 4.5	Student uzyskuje co najmniej 81% z testu zaliczeniowego - pełne kryterium opisano na ocenę 5.0.
NA OCENĘ 5.0	Student identyfikuje możliwe zagrożenia, dokonuje ich szczegółowej analizy, tworzy charakterystykę oraz poprawnie je klasyfikuje. Student uzyskuje co najmniej 91% z testu zaliczeniowego.
EFEKT KSZTAŁCENIA 4	
NA OCENĘ 2.0	Student nie spełnia warunków określonych dla oceny 3.0.
NA OCENĘ 3.0	Student uzyskuje co najmniej 51% z testu zaliczeniowego - pełne kryterium opisano na ocenę 5.0.
NA OCENĘ 3.5	Student uzyskuje co najmniej 61% z testu zaliczeniowego - pełne kryterium opisano na ocenę 5.0.
NA OCENĘ 4.0	Student uzyskuje co najmniej 71% z testu zaliczeniowego - pełne kryterium opisano na ocenę 5.0.
NA OCENĘ 4.5	Student uzyskuje co najmniej 81% z testu zaliczeniowego - pełne kryterium opisano na ocenę 5.0.
NA OCENĘ 5.0	Student potrafi zidentyfikować ryzyko wystąpienia wszystkich poznanych zagrożeń w cyberprzestrzeni i podjąć działania mające na celu eliminację wystąpienia zdecydowanej większości z nich. Student uzyskuje co najmniej 91% z testu zaliczeniowego.
EFEKT KSZTAŁCENIA 5	
NA OCENĘ 2.0	Student nie spełnia warunków określonych dla oceny 3.0.
NA OCENĘ 3.0	Student uzyskuje co najmniej 51% z testu zaliczeniowego - pełne kryterium opisano na ocenę 5.0.
NA OCENĘ 3.5	Student uzyskuje co najmniej 61% z testu zaliczeniowego - pełne kryterium opisano na ocenę 5.0.
NA OCENĘ 4.0	Student uzyskuje co najmniej 71% z testu zaliczeniowego - pełne kryterium opisano na ocenę 5.0.
NA OCENĘ 4.5	Student uzyskuje co najmniej 81% z testu zaliczeniowego - pełne kryterium opisano na ocenę 5.0.
NA OCENĘ 5.0	Student posiada wysoka świadomość zagrożeń występujących w cyberprzestrzeni, dostrzega prawdopodobne zagrożenia mogące pojawić się wraz z wprowadzeniem nowych technologii. Ponadto, student potrafi aktywnie uczestniczyć w dyskusjach poświęconych zagadnieniom cyberbezpieczeństwa dokładnie argumentując swoje racje. Student uzyskuje co najmniej 91% z testu zaliczeniowego.

10 MACIERZ REALIZACJI PRZEDMIOTU

EFEKT KSZTAŁCENIA	ODNIESIENIE DANEGO EFEKTU DO SZCZEGÓLOWYCH EFEKTÓW ZDEFINIOWANYCH DLA PROGRAMU	CELE PRZEDMIOTU	TREŚCI PROGRAMOWE	NARZĘDZIA DYDAKTYCZNE	SPOSOBY OCENY
EK1	I2_W08	Cel 1 Cel 2 Cel 3 Cel 4	W1 W2 W3 W4 W5 W6 W7 W8 W9 W10 W11	N1 N2	P1
EK2	I2_W08	Cel 1 Cel 2 Cel 3 Cel 5	W1 W3 W4 W5 W6 W7 W8 W9 W11	N1 N2	P1
EK3	I2_U09 I2_U11	Cel 1 Cel 2 Cel 3 Cel 4 Cel 5	W1 W2 W3 W4 W5 W6 W7 W8 W9 W10 W11	N1 N2 N3	P1
EK4	I2_U09 I2_U11	Cel 1 Cel 2 Cel 3 Cel 4 Cel 5	W1 W2 W3 W4 W5 W6 W7 W8 W9 W11	N1 N2 N3	P1
EK5	I2_K04	Cel 1 Cel 2 Cel 3	W1 W2 W3 W4 W5 W6 W7 W8 W9 W10 W11	N1 N2 N3	P1

11 WYKAZ LITERATURY

LITERATURA PODSTAWOWA

- [1] **Tomasz Hoffmann** — *Wybrane aspekty cyberbezpieczeństwa w Polsce*, Poznań, 2018, FNCE sp. z o.o.
- [2] **red. W. Kitler, K. Chałubińska-Jentkiewicz, K. Badźmirowska-Masłowska** — *System bezpieczeństwa w cyberprzestrzeni RP*, Warszawa, 2018, Towarzystwo Wiedzy Obronnej
- [3] **Dominika Lisiak-Felicka, Maciej Szmít** — *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*, Kraków, 2016, European Association for Security
- [4] **Michał Nosowski** — *Prawne aspekty cyberbezpieczeństwa. Praktyczne wskazówki dla przedsiębiorców*, Warszawa, 2019, Weronika Wota

LITERATURA UZUPEŁNIAJĄCA

- [1] **red. Kinga Flaga-Gieruszyńska, Jacek Gołaczyński, Dariusz Szostek** — *Sztuczna inteligencja, blockchain, cyberbezpieczeństwo oraz dane osobowe. Zagadnienia wybrane*, Warszawa, 2019, C.H.Beck
- [2] **red. Robert Maciejewski** — *Cyberbezpieczeństwo i bezpieczeństwo fizyczne obiektów w energetyce*, Poznań, 2018, Fundacja na rzecz Czystej Energii
- [3] **red. Marek Górka** — *Cyberbezpieczeństwo dzieci i młodzieży Realny i wirtualny problem polityki bezpieczeństwa*, Warszawa, 2017, Difin SA

12 INFORMACJE O NAUCZYCIELACH AKADEMICKICH

OSOBA ODPOWIEDZIALNA ZA KARTĘ

dr inż. Daniel Grzonka (kontakt: daniel.grzonka@pk.edu.pl)

OSOBY PROWADZĄCE PRZEDMIOT

1 dr inż. Daniel Grzonka (kontakt: dgrzonka@pk.edu.pl)

13 ZATWIERDZENIE KARTY PRZEDMIOTU DO REALIZACJI

(miejsowość, data)

(odpowiedzialny za przedmiot)

(dziekan)

PRZYJMUJĘ DO REALIZACJI (data i podpisy osób prowadzących przedmiot)

.....