Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2019/2020

Wydział Informatyki i Telekomunikacji

Kierunek studiów: Informatyka | Profil: Ogólnoakademicki

Forma sudiów: stacjonarne | Kod kierunku: I

Stopień studiów: II

Specjalności: Cyberbezpieczeństwo dla licencjatów

1 Informacje o przedmiocie

Nazwa przedmiotu	Wstęp do cyberbezpieczeństwa
Nazwa przedmiotu w języku angielskim	Introduction to Cybersecurity
Kod przedmiotu	WIiT I oIIS D2 19/20
Kategoria przedmiotu	Przedmioty specjalnościowe
Liczba punktów ECTS	3.00
Semestry	2

2 Rodzaj zajęć, liczba godzin w planie studiów

Semestr	Wykład	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Seminarium	Projekt
2	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

Wykład		
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

N2 Prezentacje multimedialne

N3 Dyskusja

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	9
Egzaminy i zaliczenia w sesji	1
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	60
Opracowanie wyników	0
Przygotowanie raportu, projektu, prezentacji, dyskusji	5
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 3.0	Student potrafi w sposób nieformalny, lecz zrozumiały zdefiniować pojęcia z zakresu bezpieczeństwa cyberprzestrzeni.
Na ocenę 4.0	Student potrafi w sposób formalny i zrozumiały zdefiniować pojęcia z zakresu bezpieczeństwa cyberprzestrzeni.
Na ocenę 5.0	Student potrafi w sposób formalny, zrozumiały i bezbłędny zdefiniować pojęcia z zakresu bezpieczeństwa cyberprzestrzeni. Student podpiera definicje wieloma przykładami obrazującymi omawiane pojęcia.
Efekt kształcenia 2	
Na ocenę 3.0	Student zna podstawowe pojęcia z części ogólnej prawa polskiego - ustawy o krajowym systemie cyberbezpieczeństwa.
Na ocenę 4.0	Student zna podstawowe pojęcia z części ogólnej prawa europejskiego - ogólnego rozporządzenia o ochronie danych oraz wybranych dyrektyw Parlamentu Europejskiego i Rady (UE).
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.
Efekt kształcenia 3	
Na ocenę 3.0	Student zna podstawowe taksonomie zagrożeń występujących w cyberprzestrzeni.
Na ocenę 4.0	Student poprawnie klasyfikuje w pełni scharakteryzowane zagrożenie cybernetyczne.
Na ocenę 5.0	Student identyfikuje możliwe zagrożenia, dokonuje ich szczegółowej analizy, tworzy charakterystykę oraz poprawnie je klasyfikuje.
Efekt kształcenia 4	
Na ocenę 3.0	Student potrafi zidentyfikować ryzyko wystąpienia podstawowych zagrożeń w cyberprzestrzeni.
Na ocenę 4.0	Student potrafi zidentyfikować ryzyko wystąpienia większości poznanych zagrożeń w cyberprzestrzeni i podjąć działania mające na celu eliminację wystąpienia podstawowych.
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.
Efekt kształcenia 5	
Na ocenę 3.0	Student posiada podstawową świadomość zagrożeń występujących w cyberprzestrzeni i ich wpływu na społeczeństwo.

Na ocenę 4.0	Student posiada ponadpodstawową świadomość zagrożeń występujących w cyberprzestrzeni i ich wpływu na społeczeństwo. Ponadto, jest w stanie częściowo uczestniczyć w dyskusjach poświęconych zagadnieniom cyberbezpieczeństwa.
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.

10 Macierz realizacji przedmiotu

Efekt kształcenia	Odniesienie danego efektu do szczegółowych efektów zdefiniowanych dla programu	Cele przedmiotu	Treści programowe	Narzędzia dydaktyczne	Sposoby oceny
EK1	I2_W08 I2_U09 I2_K04	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 I2_U09 I2_U11 I2_K04	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_W08 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_W08 I2_U09 I2_U11 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 Szmit — *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

(miejscowość, data) (odpowiedzialny za przedmiot) (dziekan)

Przyjmuję do realizacji (data i podpisy osób prowadzących przedmiot)

. . . . . .