

## KARTA KURSU

Nazwa	System cyberbezpieczeństwa		
Kod		Punktacja ECTS*	2
Koordinator	Dr Agnieszka Warchoł	Zespół dydaktyczny	

### Opis kursu (cele kształcenia)

Celem kursu jest zapoznanie studentów z systemem cyberbezpieczeństwa państwa. Na kursie omówiona zostanie współpraca międzynarodowa, ale także kwestie związane z wpływem mediów społecznościowych na kształtowanie środowiska bezpieczeństwa. Dodatkowo, w perspektywie porównawczej zostaną przedstawione polityki cyberbezpieczeństwa wybranych państw oraz bieżące informacje dotyczące cyberbezpieczeństwa w Polsce oraz w skali regionalnej i międzynarodowej.

### Warunki wstępne

Wiedza	-
Umiejętności	-
Kursy	-

### Efekty kształcenia

	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych
Wiedza	<p>W 01 Ma wiedzę o istocie systemu cyberbezpieczeństwa państwa.</p> <p>W 02 Wskazuje główne państwowe, regionalne i międzynarodowe regulacje prawne w zakresie cyberbezpieczeństwa.</p> <p>W 03 Potrafi scharakteryzować i porównać polityki cyberbezpieczeństwa wybranych państw.</p>	BI_W01, BI_W02, BI_W03, BI_W04
Umiejętności	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych

	<p>U 01 Potrafi wykorzystać wiedzę teoretyczną do opisu i analizy zjawisk z zakresu cyberbezpieczeństwa.</p> <p>U 02 Potrafi pozyskiwać informacje, wykorzystywać nowoczesne technologie oraz media dla zapewnienia bezpieczeństwa informacyjnego.</p> <p>U 03 Potrafi zarządzać informacją i przedstawić efekty swojej pracy w sposób zrozumiały i logiczny.</p>	BI_U01, BI_U03	BI_U02,
--	---	-------------------	---------

Kompetencje społeczne	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych	
	<p>K 01 Rozumie potrzebę zdobywania wiedzy i doskonalenia kompetencji w zakresie cyberbezpieczeństwa.</p> <p>K 02 Umie pracować w grupie.</p> <p>K 03 Potrafi samodzielnie i krytycznie oceniać własne kompetencje oraz działać racjonalnie i etycznie.</p>	BI_K01, BI_K03	BI_K02,

Organizacja										
Forma zajęć	Wykład (W)	Ćwiczenia w grupach								
		A		K		L		S		P
Liczba godzin				10						

#### Opis metod prowadzenia zajęć

##### Konwersatorium:

- analiza źródeł, analiza literatury przedmiotu,
- *case study*,
- dyskusja,
- referaty w grupach.

#### Formy sprawdzania efektów kształcenia

	E – learning	Gry dydaktyczne	Ćwiczenia w szkole	Zajęcia terenowe	Praca laboratoryjna	Projekt indywidualny	Projekt grupowy	Udział w dyskusji	Referat	Praca pisemna (esej)	Egzamin ustny	Egzamin pisemny	Inne
W01	X						X	X	X				
W02	X						X	X	X				
W03	X						X	X	X				
U01	X						X	X	X				

U02	X						X	X	X				
U03	X						X	X	X				
K01	X						X	X	X				
K02	X						X	X	X				
K03	X						X	X	X				

Kryteria oceny	<p>Konwersatorium:</p> <ul style="list-style-type: none"> <li>- obecność (dopuszczalna jedna nieobecność nieusprawiedliwiona),</li> <li>- aktywność przejawiająca się w znajomości tekstów rekomendowanych przez prowadzącą oraz znajomość informacji bieżących dotyczących cyberbezpieczeństwa,</li> <li>- referat na wybrany temat.</li> </ul>
----------------	--

Uwagi	Indywidualny program studiów – warunki zaliczenia ustalane indywidualnie z prowadzącą zajęcia po przedstawieniu zgody na indywidualny tok studiów.
-------	--

#### Treści merytoryczne (wykaz tematów)

<p>Konwersatorium:</p> <p>Zajęcia rozpoczynają się od przedstawienia informacji bieżących, tego co obecnie dzieje się na rynku nowoczesnych technologii w zakresie bezpieczeństwa oraz kwestii dotyczących cyberbezpieczeństwa.</p> <p>Następnie, studenci przedstawiają referaty, w których przybliżają określoną problematykę badawczą, będącą sferą zainteresowań danej osoby, związaną z tematem cyberbezpieczeństwa. Wystąpienia mają na celu samodzielne rozpoznanie, przygotowanie i zaprezentowanie tematu i mogą być przyczynkiem do dyskusji przez resztę odbiorców. Na końcu wystąpienia studenci prezentują źródła.</p> <p>Wystąpienia mogą dotyczyć np.: podmiotów – kreatorów zagrożeń, poszczególnych wyzwań, szans lub zagrożeń związanych z cyberbezpieczeństwem, instytucji odpowiedzialnych za zapewnienie cyberbezpieczeństwa, rynku nowoczesnych technologii w zakresie bezpieczeństwa, informacji bieżących dotyczących Polski lub innego, wybranego państwa, organizacji międzynarodowych lub regionalnych, kwestii prawnych, organizacyjnych, trendów w zakresie cyberbezpieczeństwa.</p>
---

#### Wykaz literatury podstawowej

<p>Obowiązujące akty prawne i strategie.</p> <p><i>Ustawa z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa</i>, (Dz. U. 2018 poz. 1560).</p> <p>Dela P.T., <i>Założenia działań w cyberprzestrzeni</i>, PWN, Warszawa 2022.</p> <p>Rydlowski G., <i>Rządzenie w epoce informacji, cyfryzacji i sztucznej inteligencji</i>, Elipsa, Warszawa 2021.</p> <p>Banasiński C. (red.), <i>Cyberbezpieczeństwo. Zarys wykładu</i>, Wolters Kluwers, Warszawa 2023.</p> <p><i>Routledge Companion to Global Cyber-Security Strategy</i>, Scott N. Romaniuk, Mary Manijikian (ed.), Routledge NY, 2020</p>
---

Wykaz literatury uzupełniającej

Siudak R., *Cyberbezpieczeństwo w Polsce. Od dyskursów do polityk publicznych*, Wydawnictwo Księgarnia Akademicka, Kraków 2022.

Choucri N., Clark David D., *International Relations in the Cyber Age. The Co-Evolution Dilemma*, MIT 2018.

Hoffmann T., *Wybrane aspekty cyberbezpieczeństwa w Polsce*, Poznań 2018.

Klimburg A., *The Darkening Web. The War for Cyberspace*, NY 2017.

Lakomy, M., *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2015.

Liderman K., *Bezpieczeństwo informacyjne. Nowe wyzwania*, PWN, Warszawa 2017.

Warchoła A., *Wpływ cyberprzestrzeni na bezpieczeństwo państwa na początku XXI wieku (praca doktorska)*, Kraków 2017(wybrane fragmenty).

Ball M., *Metawersum. Jak internet przyszłości zrewolucjonizuje świat i biznes*, Warszawa 2022.

Kitler W., Taczowska-Olszewska J., Radoniewicz F. (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, C.H.Beck, Warszawa 2019.

Kreft J., *Władza platform. Za fasadą Google, Facebooka i Spotify*, Kraków 2021.

Libicki M.C., *Cyberdeterrence and Cyberwar*, RAND Corporation, Santa Monica, CA 2009.

Marczewska-Rytko M. (red.), *Haktywizm (cyberterroryzm, haking, protest obywatelski, cyberaktywizm, e-mobilizacja*, Lublin 2014.

Olejnik Ł., Kurasiński A., *Filozofia cyberbezpieczeństwa. Jak zmienia się świat? Od złośliwego oprogramowania do cyberwojny*, PWN, Warszawa 2022.

Rid T., *Wojna informacyjna*, Warszawa 2020.

*The Tallinn Manual 2.0*

*Vademecum bezpieczeństwa informacyjnego (wybór haseł)*.

Zuboff S., *Wiek kapitalizmu inwigilacji. Walka o przyszłość ludzkości na nowej granicy władzy*, Wydawnictwo Zysk i S-ka, Poznań 2020.

Warchoła A., *Ochrona praw i wolności w dobie Internetu*, [w:] *Cyberprzestrzeń jako pole zmagania o bezpieczeństwo informacyjne*, (red.) W. Fehler, Siedlce 2022.

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta)

liczba godzin w kontakcie z prowadzącymi	Wykład	
	Konwersatorium (ćwiczenia, laboratorium itd.)	10
	Pozostałe godziny kontaktu studenta z prowadzącym	
liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	20
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	10
	Przygotowanie do egzaminu/zaliczenia	10
Ogółem bilans czasu pracy		50

Liczba punktów ECTS w zależności od przyjętego przelicznika
---

2
---