

KARTA KURSU

Nazwa	Prawne i społeczne podstawy cyberbezpieczeństwa
Nazwa w j. ang.	Legal and social foundations of cyber security

Kod		Punktacja ECTS*	2
-----	--	-----------------	---

Koordynator	dr Piotr Swoboda	Zespół dydaktyczny
		dr Piotr Swoboda

Opis kursu (cele kształcenia)

Celem kształcenia jest zapoznanie uczestników kursu z podstawowymi pojęciami dotyczącymi cyberbezpieczeństwa, rodzajami problemów, wyzwań, zagrożeń i przestępstw występujących w cyberprzestrzeni oraz ze specyfiką funkcjonowania krajowego systemu cyberbezpieczeństwa, ze szczególnym uwzględnieniem właściwości poszczególnych instytucji w zakresie zgłaszania i obsługi incydentów komputerowych oraz z prawnymi instrumentami międzynarodowymi właściwymi w sprawach cyberbezpieczeństwa.

Warunki wstępne

Wiedza	Student posiada podstawową wiedzę z zakresu bezpieczeństwa państwa, administracji publicznej oraz bezpieczeństwa informacji.
Umiejętności	Student potrafi zidentyfikować podstawowe problemy bezpieczeństwa z punktu widzenia państwa, jak również konkretnej jednostki organizacyjnej oraz potrafi tworzyć logiczne powiązania między różnymi zjawiskami i procesami.
Kursy	Informatyka, cyberbezpieczeństwo.

Efekty kształcenia

	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych
Wiedza	<p>W01, Student dysponuje wiedzą na temat najważniejszych pojęć, zagrożeń i problemów z zakresu bezpieczeństwa informacji i cyberbezpieczeństwa.</p> <p>W02, Student posiada wiedzę na temat organizacji systemu zarządzania cyberbezpieczeństwem oraz bezpieczeństwa informacji.</p> <p>W03, Student zna podstawowe organizacje krajowe i międzynarodowe oraz instrumenty prawne w zakresie cyberbezpieczeństwa..</p>	SC_W04, SC_W06, SC_W07

	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych
Umiejętności	<p>U01, Student potrafi zidentyfikować najważniejsze problemy wyzwania i zagrożenia dla bezpieczeństwa informacji w cyberprzestrzeni oraz ich konsekwencje dla państwa i jednostek organizacyjnych oraz użytkowników systemów przetwarzających.</p> <p>U02, Student jest w stanie zidentyfikować podstawowe instytucje i instrumenty prawne właściwe w zakresie cyberbezpieczeństwa i zwalczania cyberprzestępczości.</p> <p>U03, Student potrafi interpretować i wykorzystywać przepisy poszczególnych aktów prawnych w zakresie cyberbezpieczeństwa i przestępstw popełnianych w cyberprzestrzeni.</p>	SC_U09, SC_U10

	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych
Kompetencje społeczne	<p>K01, Student ma świadomość ryzyka dla bezpieczeństwa informacji przetwarzanych przez podmioty prywatne i publiczne, w szczególności w odniesieniu do zagrożeń występujących w cyberprzestrzeni.</p> <p>K02, Student rozumie złożoność otoczenia wewnętrznego i zewnętrznego współczesnych organizacji w szczególności w kontekście bezpieczeństwa zasobów informacyjnych w cyberprzestrzeni.</p> <p>K03, Student potrafi odpowiednio diagnozować występujące zagrożenia właściwe dla cyberprzestrzeni i zna schematy reagowania na nie w odpowiedni sposób poprzez zgłaszanie incydentów komputerowych właściwym podmiotom.</p>	SC_K01, SC_K02, SC_K03

Studia stacjonarne

Organizacja												
Forma zajęć	Wykład (W)	Ćwiczenia w grupach										
		A		K		L		S		P		E
Liczba godzin	20											

Studia niestacjonarne

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

Opis metod prowadzenia zajęć

Wykłady:

- Prezentacja Power Point;
- Dyskusja.

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	
W02	x							x				x	
W03	x							x				x	
U01	x							x				x	
U02	x							x				x	
U03	x							x				x	
K01	x							x				x	
K02	x							x				x	
K03	x							x				x	

Kryteria oceny	Obecność i aktywność na zajęciach. Kolokwium zaliczeniowe - 10 pytań. Test jednokrotnego wyboru (kryterium zaliczenia: min. 6 poprawnych odpowiedzi).
----------------	--

Uwagi	Indywidualny program studiów – warunki zaliczenia ustalane indywidualnie z prowadzącym zajęcia po przedstawieniu zgody na indywidualny tok studiów. Przepisanie oceny z kursu o tej samej nazwie (lub zbliżonej) realizowanego na tym samym stopniu kształcenia warunkowane jest ekwiwalentną liczbą godzin, punktów ECTS oraz co najmniej oceną dobrą. Odrobienie nieobecności na zajęciach – wykonanie dodatkowej pracy po indywidualnym ustaleniu z prowadzącym.
-------	---

Treści merytoryczne (wykaz tematów)

- 1) Podstawowe pojęcia. Cyberprzestrzeń. Cyberbezpieczeństwo. Cyberprzestępczość. Bezpieczeństwo informacji i bezpieczeństwo informacyjne. Infrastruktura krytyczna państwa. Zagrożenia i podatności.
- 2) Podstawowe pojęcia i problemy bezpieczeństwa w cyberprzestrzeni. Przestępczość pospolita. Przestępczość zorganizowana. Terroryzm. Walka informacyjna. Szpiegostwo. Działania hybrydowe. Cele cyberprzestępców.
- 3) Zagrożenia w cyberprzestrzeni i rodzaje cyberprzestępstw.
- 4) Międzynarodowe regulacje prawne w zakresie ochrony cyberprzestrzeni.
- 5) Ochrona cyberprzestrzeni w prawodawstwie krajowym.
- 6) System przeciwdziałania i zwalczania cyberprzestępczości. Wymiar międzynarodowy i wymiar krajowy.
- 7) Ochrona cyberprzestrzeni z punktu widzenia jednostki (osoby fizycznej).
- 8) Ochrona cyberprzestrzeni z punktu widzenia przedsiębiorstwa (firmy prywatnej).
- 9) Ochrona cyberprzestrzeni z punktu widzenia instytucji publicznej.
- 10) Ochrona cyberprzestrzeni na poziomie państwa (sfera cywilna i militarna).

Wykaz literatury podstawowej

- 1) Banasiński C. (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Wolters Kluwer, Warszawa 2018 (wyd. I), 2023 (wyd. 2).
- 2) Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, t. j. Dz. U. 2024, poz. 1077 (z późn. zm.).
- 3) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148, Dz.U. L 333 z 27.12.2022, p. 80–152 (dyrektywa NIS 2).
- 4) Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa wraz z naniesionymi zmianami z projektu nowelizacji ustawy z dnia 2 grudnia 2024 roku, KancelariaTrapele Konarski Podrecki i Wspólnicy, <https://www.traple.pl/wp-content/uploads/2025/01/250110-tkp-uksc-wersja-scalona-projekt-z-2-grudnia-2024-r.pdf> [25.02.2025].
- 5) Konwencja Rady Europy o cyberprzestępczości z dnia 23 listopada 2001 r., Dz. U. 2015, poz. 728.
- 6) Protokół dodatkowy do Konwencji Rady Europy o cyberprzestępczości dotyczący penalizacji czynów o charakterze rasistowskim lub ksenofobicznym popełnionych przy użyciu systemów komputerowych z dnia 28 stycznia 2003 r., Dz. U. 2015, poz. 730.

Wykaz literatury uzupełniającej

- 1) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013, Dz.U. L 151 z 7.6.2019, p. 15–69 (akt o cyberbezpieczeństwie).
- 2) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń (UE) nr 168/2013 i (UE) 2019/1020 i dyrektywy (UE) 2020/1828, Dz.U. L, 2024/2847, 20.11.2024, ELI (akt o cyberodporności).
- 3) Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, t. j. Dz. U. 2023, poz. 122 (z późn. zm.).
- 4) Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, t. j. Dz. U. 2022, poz. 1648 (z późn. zm.).
- 5) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) dnia 27 kwietnia 2016 r., (Dz.Ur.UE.L nr 119, str. 1 z późn. zm.).
- 6) Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, t.j. Dz.U. 2023 poz. 756 (z późn. zm.).
- 7) Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, t.j. Dz. U. 2022, poz. 2509.
- 8) Ustawa z dnia 6 czerwca 1997 r. Kodeks karny, t. j. Dz. U. 2022, poz. 1138 (z późn. zm.).
- 9) Biuro Bezpieczeństwa Narodowego, *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Warszawa 2015.
- 10) *Strategia Cyberbezpieczeństwa RP na lata 2019 – 2024*, Ministerstwo Cyfryzacji, Warszawa 2019.
- 11) Kosiński J., *Paradygmaty cyberprzestępczości*, Difin, Warszawa 2015.
- 12) Adamski A., *Prawo karne komputerowe*, Wydawnictwo C. H. BECK, Warszawa 2000.
- 13) Adamski A., *Cyberprzestępczość – aspekty prawne i kryminologiczne*, „*Studia Prawnicze*” 2005 nr 4 (166).
- 14) Wiśniewski A., *Przestępstwa w Internecie związane z prawem autorskim i prawami pokrewnymi*, „*Studia Prawnicze*” 2005 nr 4 (166).
- 15) Denning D. E., *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002.
- 16) Wiśniewski P., Boehlke J., *Cyberprzestępczość w gospodarce*, Wydawnictwo Naukowe UMK, Toruń 2016.
- 17) Hadnagy C., Fincher M., *Mroczne odmęty phishingu. Nie daj się złowić!*, Helion, Gliwice 2015.
- 18) Ciborski T., *Ukryta tożsamość. Jak się obronić przed utratą prywatności*, Helion, Gliwice 2015.
- 19) Opitek P., *Skimming – aspekty kryminalistyczne. Cyberprzestępczość w bankowości elektronicznej*, C. H. Beck, Warszawa 2017.
- 20) Wasilewski J., *Przestępczość w cyberprzestrzeni*, „*Przegląd Bezpieczeństwa Wewnętrznego*” 2016 nr 15 (8).
- 21) Lebedowicz A., *Wybrane aspekty prawnokarne, kryminalistyczne i kryminologiczne cyberprzestępczości*, „*Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury*” 2022 Nr 45 (1).
- 22) Kępa L., *Zagrożenia komputerowe a ochrona danych osobowych*, Legalis C. H. Beck.
- 23) Warchoła A., *Przestępstwa komputerowe i problemy wojny w cyberprzestrzeni*, [w:] Swoboda P., Żebrowski A. (red.), *Elementy bezpieczeństwa narodowego Rzeczypospolitej Polskiej: analiza*

wybranych systemów, Kraków 2020.

24) Wasiuta O., Klepka R., Vademecum bezpieczeństwa informacyjnego, t. 1 i 2, AT Wydawnictwo, Wydawnictwo LIBRON – Filip Lohner, Kraków 2019.

25) Wasiuta O., Wasiuta S., Encyklopedia bezpieczeństwa, t. 1-6, Wydawnictwo LIBRON – Filip Lohner, Kraków 2021-2022.

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) – studia stacjonarne

Ilość godzin w kontakcie z prowadzącymi	Wykład	20
	Konwersatorium (ćwiczenia, laboratorium itd.)	-
	Pozostałe godziny kontaktu studenta z prowadzącym	5
Ilość godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	15
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	-
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	-
	Przygotowanie do egzaminu	10
Ogółem bilans czasu pracy		50
Ilość punktów ECTS w zależności od przyjętego przelicznika		2

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) – studia niestacjonarne

Ilość godzin w kontakcie z prowadzącymi	Wykład	10
	Konwersatorium (ćwiczenia, laboratorium itd.)	-
	Pozostałe godziny kontaktu studenta z prowadzącym	10
Ilość 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)	-
	Przygotowanie do egzaminu	10
Ogółem bilans czasu pracy		50
Ilość punktów ECTS w zależności od przyjętego przelicznika		2