

KARTA KURSU (realizowanego w module specjalności)**BEZPIECZEŃSTWO INFORMACYJNE***(nazwa specjalności)*

Nazwa	cyberzagrożenia
Nazwa w j. ang.	cyber threats

Koordynator	dr Emilia Musiał	Zespół dydaktyczny
		dr Emilia Musiał
Punktacja ECTS*	2	

Opis kursu (cele kształcenia)

Kurs ma na celu:

- przekazanie studentom specjalistycznej wiedzy na temat zagrożeń stworzonych przez nowoczesne technologie cyfrowe (komputery i pochodne – urządzenia służące do cyfrowego przetwarzania i przesyłania informacji oraz wizualizacji przetwarzania tych informacji), czyli cyberzagrożeń, na które – z racji korzystania z usług dostępnych w Internecie – narażeni są nie tylko przedsiębiorcy, ale także osoby fizyczne;
- przyswojenie przez studentów kompetencji cyfrowych (obejmujących m.in. komfort cyfrowy i kompetencje związane z cyberbezpieczeństwem), które pozwolą im w pełni bezpiecznie funkcjonować i działać w Sieci.

Treści kursu w głównej mierze obejmują problematykę dotyczącą zagrożeń stwarzanych przez media cyfrowe i technologie informacyjno-komunikacyjne, jak również zagrożeń społecznych, wychowawczych, zdrowotnych, moralnych mających miejsce w cyberprzestrzeni (w szczególności krzywdzenia przy użyciu Internetu, interaktywnych lub cyfrowych technologii, uzależnień od komputera, telefonu, gier).

Po ukończeniu kursu student powinien posiadać wiedzę, w jaki sposób rozpoznawać takie problemy jak uzależnienie od środków masowego przekazu, manipulacja w Sieci, podszywanie się pod kogoś w Internecie, przejmowanie prywatnej treści i zawartości komputera czy kradzież i niekontrolowane wydatki, a ponadto umiejętności pozwalające mu w sposób prawidłowy reagować w wypadku pojawienia się symptomów świadczących o tych problemach.

Efekty kształcenia

Wiedza	Efekt kształcenia dla kursu	Odniesienie do efektów dla specjalności (określonych w karcie programu studiów dla modułu specjalnościowego)
--------	-----------------------------	--

	<p>W01: student wyciąga wnioski z daleko idącej cyfrowej cywilizacji (funkcjonowania człowieka w społeczeństwie informacyjnym) – jej szans i zagrożeń.</p> <p>W02: student identyfikuje obszary zagrożeń cyberprzestrzeni i wymienia różnorodne przykłady zagrożeń, patologii i uzależnień.</p> <p>W03: student ocenia przyczyny, przebieg i skutki uzależnień i zagrożeń (m.in. rozpoznaje i dostrzega zależności pomiędzy zagrożeniami a racjonalnym działaniem w zakresie profilaktyki, a także minimalizowania negatywnych skutków).</p> <p>W04: student analizuje zakres i skalę zagrożeń w Polsce i na świecie.</p>	<p>K2_W01 S2_W03 S2_W06</p>
--	---	-------------------------------------

	Efekt kształcenia dla kursu	Odniesienie do efektów dla specjalności (określonych w karcie programu studiów dla modułu specjalność)
Umiejętności	<p>U01: student dostrzega problemy i zjawiska dotyczące cyberzagrożeń oraz analizuje metody przeciwdziałania zagrożeniom i uzależnieniom w cyberprzestrzeni.</p> <p>U02: student rozpoznaje i ocenia przyczyny, przebieg, objawy, skutki uzależnień i zagrożeń w cyberprzestrzeni.</p> <p>U03: student projektuje działania na rzecz profilaktyki zagrożeń i uzależnień w cyberprzestrzeni.</p> <p>U04: student rozwija i testuje swoje kompetencje cyfrowe w zakresie bezpiecznego korzystania z komputera i Sieci.</p>	<p>K2_U01 S2_U04 S2_U05</p>

	Efekt kształcenia dla kursu	Odniesienie do efektów dla specjalności (określonych w karcie programu studiów dla modułu specjalnościowego)
Kompetencje społeczne	<p>K01: student akceptuje konieczność bezpiecznego funkcjonowania w cyberprzestrzeni.</p> <p>K02: student ocenia własne kompetencje cyfrowe i wykazuje zainteresowanie ich rozwijaniem.</p> <p>K03: student przestrzega zasad bezpiecznego korzystania z komputera i Sieci.</p> <p>K04: student efektywnie pracuje zarówno samodzielnie, jak i w grupie podczas zajęć.</p>	<p>K2_K01 K2_K02 K2_K03</p>

Organizacja										
Forma zajęć	Wykład (W)	Ćwiczenia w grupach								
		A		K		L		S		P
Liczba godzin	15	15								

Opis metod prowadzenia zajęć

Wykład: wykład informacyjny, problemowy i konwersatoryjny z prezentacją multimedialną, dyskusja związana z wykładem.

Audytorium: praca indywidualna i grupowa studentów (m.in. burza mózgów, metoda sytuacyjna) połączona z wcześniejszą prezentacją przeprowadzoną przez prowadzącego zajęcia. Dyskusja problemowa w grupie na zadany temat. Rozwiązywanie zadań problemowych. Wykonanie projektów grupowych na zajęciach i poza nimi.

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					
W02								X					
W03							X	X					
W04								X					
U01					X		X						
U02					X		X	X					
U03							X						
U04							X		X				
K01								X					
K02					X		X						
K03					X		X						
K04							X	X					

Kryteria oceny	Wykład:
	<ul style="list-style-type: none"> – obecność na wykładach – aktywność w trakcie wykładu (uczestnictwo w dyskusji, rozwiązywanie quizów) – kolokwium podsumowujące materiał z wykładów
Kryteria oceny	Audytorium:
	<ul style="list-style-type: none"> – projekty grupowe (realizowane na 1-2 zajęciach) zw. z oceną przyczyn, przebiegu, objawów, skutków uzależnień i zagrożeń w cyberprzestrzeni oraz działaniami na rzecz profilaktyki cyberzagrożeń – obecność na zajęciach – aktywność i wykonywanie zadań w trakcie zajęć – quizy wiedzy

Uwagi	Nieobecność na zajęciach powinna zostać odrobiona (np. poprzez wykonanie dodatkowych zadań lub pracę na platformie zdalnej po wcześniejszej konsultacji z prowadzącym).
-------	---

Treści merytoryczne (wykaz tematów)

Wykład – problematyka:

1. Ogólne zagadnienia związane z cyberprzestrzenią (definicje, funkcje, cechy, zalety, obszary specyficznych ograniczeń)
2. Klasyfikacja obszarów zagrożeń cyberprzestrzeni, podstawowe rodzaje cyberzagrożeń: cyberprzemoc, cyberprzestępstwo, cyberinwigilacja, cyberterrorizm, cyberautorytaryzm, cyberwojna
3. Zagrożenia cyberprzestrzeni i świata wirtualnego: zagrożenia zdrowia fizycznego i psychicznego, zagrożenia społeczno-wychowawcze, zagrożenia moralne, zespół uzależnienia od Internetu, zagrożenia poznawczo-intelektualne, zagrożenia (choroby) informacyjne, zagrożenia substancjami chemicznymi z inspiracji sieci
4. Przystępność, ryzykowne zachowania i bezpieczeństwo teleinformatyczne: przestępstwa przeciwko ochronie informacji
5. Krajobraz zagrożeń w cyberprzestrzeni w Polsce i na świecie. Służby specjalne i społeczne wobec zagrożeń cyberprzestrzeni

6. Społeczeństwo nadzorowane – nowe technologie w służbie inwigilacji

Audytarium:

1. Analiza podstawowych zagrożeń zdrowotnych związanych z użytkowaniem komputera i Internetu (w szczególności cyberprzemocy) – m.in. uwarunkowania, prawidłowości oraz mechanizmy dotyczące zagrożeń zdrowia psychicznego i fizycznego oraz cyberprzemocy; orientacja stanu i zasięgu zagrożeń zdrowia psychicznego i fizycznego oraz cyberprzemocy; diagnozowanie przyczyn, przebiegu, objawów, skutków zagrożeń zdrowia psychicznego i fizycznego oraz cyberprzemocy; przeciwdziałanie i realizowanie profilaktyki w zakresie dotyczącym zagrożeń zdrowia psychicznego i fizycznego oraz cyberprzemocy
2. Analiza wybranych zagrożeń społeczno-wychowawczych (pedofilia w sieci, pornografia, seksting, sekty) – m.in. diagnoza zagrożeń związanych z korzystaniem z portali poświęconych sektom, pornografii, pedofilii, sekstingowi; umiejętność udzielania wsparcia osobom korzystającym z portali poświęconych: sektom, pornografii, pedofilii, sekstingowi; analiza podstawowych objawów zjawisk; charakterystyka sprawców i ofiar; znajomość podstawowych zapisów prawnych
3. Zagrożenia związane z uzależnieniami (infoholizm, uzależnienie od gier, Internet źródłem informacji o substancjach odurzających i dopingujących) – m.in. uwarunkowania, prawidłowości oraz mechanizmy uzależnień i grania w gry komputerowe; diagnozowanie przyczyn, przebiegu, objawów, skutków uzależnień; przeciwdziałanie i realizacja profilaktyki w zakresie uzależnień
4. Cyberprzestępstwa i nadużycia (portfel, komputer, prywatność, treści) – m.in. znajomość zagadnień odnoszących się do bezpieczeństwa w Sieci; zasady bezpiecznych zakupów oraz korzystania z serwisów społecznościowych; zasady bezpiecznego korzystania ze sprzętu komputerowego; przechowywanie w sposób bezpieczny danych komputerowych
5. Kompetencje cyfrowe – akcje i programy edukacyjne nakierowane na podnoszenie kompetencji cyfrowych wśród dzieci i młodzieży, a także wśród nauczycieli, rodziców i opiekunów (m.in. podnoszenie poziomu świadomości na temat potencjalnych zagrożeń w cyberprzestrzeni)

Wykaz literatury podstawowej:

1. Bednarek J., Andrzejewska A. (red.), *Zagrożenia cyberprzestrzeni i świata wirtualnego*, Wydaw. Difin, Warszawa 2014
2. Kozak S., *Patologia cyfrowego dzieciństwa i młodości. Przyczyny, skutki, zapobieganie w rodzinie i w szkołach*, Wydaw. Difin, Warszawa 2014
3. Bednarek J. (red.), *Człowiek w obliczu szans cyberprzestrzeni i świata wirtualnego*, Wyda. Difin, Warszawa 2014
4. Kosiński J., *Paradygmaty cyberprzestępczości*, Wydaw. Difin, Warszawa 2015
5. Derlatka K., *Cyberzagrożenia w edukacji dla bezpieczeństwa i świadomość uczniów w obszarze bezpieczeństwa Internetu*, „Interdyscyplinarne Studia Społeczne” 2017, nr 1 (3)
6. *Zagrożenia cyberprzestrzeni*, https://akademia.nask.pl/pliki/4-zagrozenia_cyberprzestrzeni_produk_t_finalny.pdf
7. Pyżalski J., *Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży*, Oficyna Wydawnicza „Impuls”, Kraków 2012

Wykaz literatury uzupełniającej:

1. Morańska D. (red.), *Patologie w cyberprzestrzeni. Profilaktyka zagrożeń medialnych*, Wydawnictwo: WSB Dąbrowa Górnicza, Dąbrowa Górnicza 2015
2. Angwin J., *Społeczeństwo nadzorowane. W poszukiwaniu prywatności, bezpieczeństwa i wolności w świecie permanentnej inwigilacji*, Kurhaus Publishing Kurhaus Media sp. z o.o. sp.k., Warszawa 2017
3. Kupczyk P., *Współczesne cyberzagrożenia – jak z nimi walczyć*, https://www.bcc.org.pl/uploads/media/klp_bcc_wspolczesne_zagrozenia_it.pdf
4. *Cyberbezpieczeństwo w Polsce: ochrona urzędów końcowych przed cyberatakami. Analiza sytuacji i rekomendacje działań*, https://cyfrowapolska.org/wp-content/uploads/2019/01/Raport_cyberbezpiecze%C5%84stwo_2019.pdf
5. *Jak reagować na cyberprzemoc. Poradnik dla szkół*, https://www.edukacja.fdds.pl/cb0428e3-c0d8-47cb-8508-1b865100a1f9/Extras/ksiazka-jak_reagowac_na_cyberprzemoc-FDDS-12042017.pdf

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta)

Ilość godzin w kontakcie z prowadzącymi	Wykład	15
	Konwersatorium (ćwiczenia, laboratorium itd.)	15

	Pozostałe godziny kontaktu studenta z prowadzącym	--
Ilość godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	5
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu (zadanie - ewaluacja otwartych źródeł informacji)	5
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	10
	Przygotowanie do egzaminu	--
Ogółem bilans czasu pracy		50
Ilość punktów ECTS w zależności od przyjętego przelicznika		2