KARTA KURSU (realizowanego w module specjalności)

BEZPIECZEŃSTWO INFORMACYJNE

(nazwa specjalności)

Nazwa	Przestępstwa przeciwko bezpieczeństwu informacyjnemu
Nazwa w j. ang.	Crimes against Information Security

Koordynator	dr Paulina Motylińska	Zespół dydaktyczny
		dr Paulina Motylińska
Punktacja ECTS*	3	

Opis kursu (cele kształcenia)

Kurs ma na celu przekazanie studentom podstawowej wiedzy w zakresie przestępczości w obszarze bezpieczeństwa informacyjnego. Tematyka zajęć obejmuje głównie zagadnienia związane z przestępczością przeciwko bezpieczeństwu elektronicznie przetwarzanej informacji. Studenci poznają zagadnienia przestępstw przeciwko poufności, integralności i dostępności informacji w systemach komputerowych, przestępstwa związane z naruszaniem praw autorskich i praw pokrewnych, przestępstwa związane z treścią informacji. Przedstawione zostaną także kwestie zapobiegania przestępstwom w cyberprzestrzeni, zwalczania i przyszłości cyberprzestępczości.

Efekty kształcenia

	Efekt kształcenia dla kursu	Odniesienie do efektów dla specjalności (określonych w karcie programu studiów dla modułu specjalnościowego)
Wiedza	W01: Student posiada wiedzę w zakresie uwarunkowań przestępczości przeciwko bezpieczeństwu informacyjnemu. W02: Student zna regulacje prawne w kontekście przestępczości przeciwko bezpieczeństwu informacyjnemu. W03: Student zna typy przestępstw przeciwko bezpieczeństwu informacyjnemu oraz wskazuje możliwości przeciwdziałania im i ich zwalczania.	BI_W02 BI_W03

	Efekt kształcenia dla kursu	Odniesienie do efektów dla specjalności (określonych w karcie programu studiów dla modułu specjalność)
Umiejętności	U01: Student potrafi wykorzystać wiedzę teoretyczną do analizy i charakterystyki wybranych typów przestępstw przeciwko bezpieczeństwu informacyjnemu. U02: Student proponuje rozwiązania w zakresie przeciwdziałania i zwalczania przestępczości przeciwko bezpieczeństwu informacyjnemu.	BI_U01 BI_U02

	Efekt kształcenia dla kursu	Odniesienie do efektów dla specjalności (określonych w karcie programu studiów dla modułu specjalnościowego)
Kompetencje społeczne	K01: Student krytycznie ocenia własne kompetencje w zakresie bezpieczeństwa informacyjnego. K02: Student samodzielnie rozszerza swoją wiedzę w zakresie przestępczości przeciwko bezpieczeństwu informacyjnemu. K03: Student aktywnie pracuje samodzielnie oraz w grupie.	BI_K01 BI_K03 BI_K02

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

Opis metod prowadzenia zajęć

Wykład z wykorzystaniem prezentacji multimedialnych, filmów i analizy zawartości stron internetowych. Ćwiczenia zostaną poprowadzone w sposób aktywizujący studentów (dyskusja na podstawie przeczytanej lektury, zadania praktyczne indywidualne i grupowe).

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 (zadania w trakcie zajęć)
W01								x				x	x
W02								x				x	x

W03								x				x	x
U01							x	x					x
U02							x	x					x
K01								x					x
K02							x	x					x
K03							x						x

Kryteria oceny	Wykład: – obecność na zajęciach (minimum 80% obecności) Ćwiczenia: – aktywność i wykonywanie zadań w trakcie zajęć – obecność na zajęciach (minimum 80% obecności) Egzamin (forma testowa): - uzyskanie min. 60% punktów

Uwagi	Wszystkie zadania z ćwiczeń muszą zostać wykonane. Nieobecność na zajęciach nie zwalnia z konieczności wykonania zadania.

Treści merytoryczne (wykaz tematów)

1. Definicje, pojęcia, tematy:

Bezpieczeństwo informacyjne, bezpieczeństwo informacji, zagrożenia dla bezpieczeństwa informacji (podział, przykłady), atrybuty bezpieczeństwa informacji, cyberbezpieczeństwo, cyberzagrożenia, cyberprzestępczość, pasywne i aktywne ataki na systemy komputerowe, spam, phishing, carding, prawo autorskie (podstawowe pojęcia, np. utwór, prawa majątkowe i osobiste, przedmiot i podmiot prawa autorskiego, dozwolony użytek prywatny, plagiat), piractwo, pornografia dziecięca, krajowy system cyberbezpieczeństwa, Zespół Reagowania na Incydenty Bezpieczeństwa, zarządzanie bezpieczeństwem informacyjnym, audyt bezpieczeństwa informacji, Polityka bezpieczeństwa informacji (w tym zabezpieczenia), kompetencje informacyjne i cyfrowe.

2. Podział cyberprzestępstw według Konwencji Rady Europy o cyberprzestępczości z 2001 r. + analiza przykładów cyberprzestępstw

3. Kodeks Karny – typy przestępstw przeciwko bezpieczeństwu informacyjnemu, sposoby definiowania

- przestępstwa przeciw poufności, integralności i dostępności danych i systemów

- przestępstwa: komputer jako narzędzie

- przestępstwa związane z treścią informacji

4. Naruszenia prawa autorskiego – typy naruszeń/przestępstw wymienione w KK, Ustawie z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, Ustawie z dnia 30 czerwca 2000 r. Prawo własności przemysłowej, Ustawie z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji.

5. Organy działające w intencji przeciwdziałania cyberprzestępczości – główne obszary działań.

6. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024.

Wykaz literatury podstawowej:

1. Liderman K. (2017). *Bezpieczeństwo informacyjne. Nowe wyzwania*. Warszawa: PWN. (lub wydanie z 2012)
2. Kowalewski, Jakub; Kowalewski, Marian (2017). *Zagrożenia informacji w cyberprzestrzeni, cyberterroryzm*. Warszawa: Oficyna Wydawnicza Politechniki Warszawskiej.
3. Białkowski, Marek (2016). *Ocena prawna i kryminalistyczna przestępczości komputerowej*. Warszawa: CeDeWu.
4. Kosiński, Jerzy (2015). *Paradygmaty cyberprzestępczości*. Warszawa: Difin.
5. Banasiński, Cezary red. (2018). *Cyberbezpieczeństwo*. Warszawa: Wolters Kluwers.
6. Kodeks Karny Dz.U. 1997 nr 88 poz. 553

Wykaz literatury uzupełniającej:

1. Wasiuta O., Klepka R., red. (2019). *Vademecum Bezpieczeństwa Informacyjnego*. Kraków: AT Wydawnictwo, LIBRON.
2. Janczak J., Nowak A. (2013). *Bezpieczeństwo informacyjne: wybrane problemy*. Warszawa: AON.
3. Lisiak-Felicka, Dominika; Szmit, Maciej (2016). *Cyberbezpieczeństwo administracji publicznej w Polsce*. Kraków: European Association for Security.
4. Bączek P. (2006). *Zagrożenia informacyjne a bezpieczeństwo Państwa Polskiego*. Toruń: Wydaw. Adam Marszałek.
5. Wiśniewski, Piotr; Boehlke, Jerzy (2016). *Cyberprzestępczość w gospodarce*. Toruń: Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika.
6. Wodecka-Hyjek A. (2012). *Wybrane aspekty bezpieczeństwa zasobów informacyjnych*. W: Borowiecki R., Czekaj J. (red.). *Zarządzanie informacją i komunikacją w organizacjach gospodarczych i instytucjach sektora publicznego*. Toruń: Wydawnictwo Dom Organizatora, s. 49-68.
7. Jabłoński M., Mielus M. (2010). *Zagrożenia bezpieczeństwa informacji w organizacji gospodarczej*. W: Kwieciński M. (red.). *Bezpieczeństwo informacji – zagadnienia wybrane*. Kraków: Krakowskie Towarzystwo Edukacyjne, s. 23-38.

Dodatkowa literatura będzie także prezentowana na zajęciach.

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	10
	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	25
Ogółem bilans czasu pracy		75
Ilość punktów ECTS w zależności od przyjętego przelicznika		3