Załącznik Nr 2.3

……

pieczątka Wydziału/Instytutu

Nazwa Wydziału/Instytutu prowadzącego kierunek studiów: ***Wydział Informatyki***
Nazwa kierunku studiów: ***Cyberbezpieczeństwo***
Poziom kształcenia: ***studia II stopnia***
Profil kształcenia: ***ogólnoakademicki***

EFEKTY UCZENIA SIĘ DLA KIERUNKU
określone Uchwałą Senatu Uniwersytetu Kazimierza Wielkiego
Nr 49/2025/2026
z dnia 28 kwietnia 2026 r.

L.p.	symbol kierunkowych efektów uczenia się	kierunkowe efekty uczenia się	odniesienie do charakterystyki drugiego stopnia efektów uczenia się (kod składnika opisu)
		Wiedza	
1.	K_W01	Ma pogłębioną i uporządkowaną wiedzę z zakresu informatyki technicznej i telekomunikacji oraz procesów zachodzących w systemach i sieciach teleinformatycznych, istotnych dla zapewniania bezpieczeństwa ich działania.	P7S_WG
2.	K_W02	Zna metodologiczne podstawy prowadzenia badań naukowych oraz ma wiedzę dotyczącą metodyki prowadzenia prac badawczo-rozwojowych w dziedzinie cyberbezpieczeństwa.	P7S_WG
3.	K_W03	Ma pogłębioną wiedzę o faktach, metodach i narzędziach analizy danych w kryptografii i systemach bezpieczeństwa oraz zna główne trendy, kierunki badań i nowe technologie w cyberbezpieczeństwie wraz z ich wpływem na gospodarkę i społeczeństwo, co umożliwia rozwiązywanie złożonych problemów tego obszaru.	P7S_WG
4.	K_W04	Zna zaawansowane mechanizmy i standardy bezpieczeństwa stosowane w systemach rozproszonych, sieciach i systemach Internetu Rzeczy.	P7S_WG
5.	K_W05	Zna i rozumie, w pogłębionym stopniu, cykl życia systemów informatycznych z uwzględnieniem procesów projektowania, wdrażania, testowania, utrzymania i zapewnienie cyberbezpieczeństwa.	P7S_WG
6.	K_W06	Zna i rozumie uwarunkowania prawne, ekonomiczne, organizacyjne i etyczne działalności zawodowej i naukowej w obszarze cyberbezpieczeństwa, w tym regulacje dotyczące ochrony danych, własności intelektualnej i odpowiedzialności prawnej.	P7S_WK
7.	K_W07	Ma wiedzę o zasadach tworzenia i prowadzenia działalności gospodarczej, w tym startupów technologicznych w obszarze IT i cyberbezpieczeństwa.	P7S_WK
8.	K_W08	Rozumie znaczenie i konsekwencje pozatechnicznych (społecznych, etycznych i środowiskowych) uwarunkowań działalności zawodowej w zakresie technologii informatycznych i zabezpieczeń cyfrowych.	P7S_WK
9.	K_W09	Posiada świadomość problemów współczesnej cywilizacji wynikających z rozwoju nauk technicznych i inżynieryjnych, zwłaszcza informatyki i telekomunikacji, a także z wykorzystania najnowszych osiągnięć nauki i technologii. Rozumie zagrożenia z tym związane, w tym osobiste i społeczne dylematy wynikające z działań mogących naruszać bezpieczeństwo systemów teleinformatycznych.	P7S_WK
10.	K_W10	Ma pogłębioną wiedzę o państwowych i międzynarodowych systemach zarządzania cyberbezpieczeństwem oraz o źródłach i konsekwencjach zagrożeń na poziomie krajowym i globalnym, w tym o roli władz i organizacji międzynarodowych oraz możliwościach przeciwdziałania i łagodzenia skutków tych zagrożeń.	
∑	10		
		Umiejętności	
1.	K_U01	Potrafi samodzielnie pozyskiwać informacje z różnych źródeł, krytycznie je analizować i twórczo interpretować oraz formułować i testować hipotezy, prowadzić eksperymenty i symulacje oraz prezentować ich wyniki, stosując właściwe metody do rozwiązywania złożonych problemów bezpieczeństwa IT.	P7S_UW
2.	K_U02	Potrafi wykorzystywać metody analityczne, symulacyjne i eksperymentalne w analizie i ocenie bezpieczeństwa systemów informatycznych oraz do definiowania i rozwiązywania zadań inżynierskich w tym problemów badawczych.	P7S_UW
3.	K_U03	Potrafi wykrywać podatności i ataki, analizować i oceniać ryzyko w systemach teleinformatycznych oraz opracowywać i wdrażać procedury i strategie ochrony, w tym dla sieci bezprzewodowych i IoT, a także oceniać przydatność nowych rozwiązań technicznych i proponować ich ulepszenia.	P7S_UW
4.	K_U04	Potrafi zaprojektować i zrealizować projekt inżynierski lub badawczy z zakresu cyberbezpieczeństwa, zgodny ze specyfikacją i zapewniający bezpieczeństwo informacji, wykorzystując odpowiednie techniki i narzędzia (potrafi również opracować nowe lub dostosować istniejące), uwzględniając przy tym aspekty etyczne, prawne, organizacyjne, ekonomiczne oraz elementy innowacyjności.	P7S_UW

5.	K_U05	Potrafi oszacować przydatność, aspekt ekonomiczny i posługiwać się zaawansowanymi metodami i narzędziami informatycznymi, analitycznymi i diagnostycznymi w zadaniach inżynierskich i naukowych, dotyczących cyberbezpieczeństwa, łącząc wiedzę z różnych obszarów informatyki i innych dyscyplin.	P7S_UW
6.	K_U06	Potrafi skutecznie komunikować się na tematy specjalistyczne w środowisku zawodowym i naukowym, w języku polskim i angielskim, właściwie dobierając i stosując techniki informacyjno-komunikacyjne, w tym przygotować opracowanie naukowe lub raport techniczny z zakresu cyberbezpieczeństwa oraz zaprezentować jego wyniki.	P7S_UK
7.	K_U07	Potrafi pracować indywidualnie i w zespole (także kierując jego pracą), biorąc odpowiedzialność za jej wyniki, oraz samodzielnie określać kierunki rozwoju zawodowego i naukowego, planować i realizować samokształcenie, a także ukierunkowywać w nim innych.	P7S_UO, P7S_UU
8.	K_U08	Potrafi stosować zasady etyki zawodowej, ochrony informacji i odpowiedzialnego wykorzystania technologii informatycznych.	P7S_UW
9.	K_U09	Posiada praktyczne umiejętności posługiwania się językiem angielskim na poziomie B2+ Europejskiego Systemu Opisu Kształcenia Językowego.	P7S_UK
10.	K_U10	Potrafi analizować, odpowiednio dobierać i stosować a także przystosowywać i opracowywać metody oraz narzędzia działania w celu prognozowania, wyjaśniania i rozwiązywania problemów w obszarze cyberbezpieczeństwa.	
11.	K_U11	Potrafi odpowiednio dobierać źródła i selekcjonować informacje, dokonywać ich krytycznej analizy, syntezy i oceny w celu prognozowania, wyjaśnienia i rozwiązania problemów w obszarze cyberbezpieczeństwa.	
12.	K_U12	Potrafi wykonać typowe dla cyberbezpieczeństwa proste systemy, narzędzia lub konfiguracje zabezpieczeń zgodnie z określoną specyfikacją, dobierając właściwe metody, techniki i środowiska, a także poprawnie realizując proces implementacji i testowania.	
∑	12		
Kompetencje społeczne			
1.	K_K01	Rozumie dynamikę zmian, w zakresie wiedzy i umiejętności charakterystyczną dla cyberbezpieczeństwa, jest gotów do krytycznej oceny posiadanej wiedzy i odbieranych treści, uznaje znaczenie wiedzy w rozwiązywaniu problemów poznawczych i praktycznych oraz zasięganie opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu.	P7S_KK
2.	K_K02	Jest gotów do przestrzegania zasad etyki zawodowej, działania na rzecz przestrzegania tych zasad oraz jest świadomy potrzeby i znaczenia rozwoju dorobku zawodowego.	P7S_KR
3.	K_K03	Jest gotów do pełnienia ról zawodowych i społecznych wymagających odpowiedzialności, przywództwa i współpracy w zespołach interdyscyplinarnych.	P7S_KR, P7S_KO
4.	K_K04	Jest gotów do inicjowania działań na rzecz bezpieczeństwa w cyberprzestrzeni oraz popularyzowania wiedzy o zagrożeniach i dobrych praktykach wśród społeczeństwa.	P7S_KO
5.	K_K05	Jest gotów do podejmowania inicjatyw przedsiębiorczych oraz działalności innowacyjnej w obszarze technologii informatycznych i bezpieczeństwa cyfrowego.	P7S_KO
∑	5		

Efekty kształcenia dla kierunku opracowano na podstawie *Rozporządzenia Ministra Nauki i Szkolnictwa Wyższego w sprawie charakterystyk drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-8 Polskiej Ramy Kwalifikacji z dnia 14 listopada 2018 r. (Dz.U. Z 2018 r., poz. 2218*

.....

data i podpis

Zastępca ds. Kształcenia

.....

data i podpis

Dyrektor Kolegium

Symbol efektu tworzą:

- litera K - dla wyróżnienia, że chodzi o efekty kierunkowe,
- znak _ (podkreślnik),
- jedna z liter W, U lub K - dla oznaczenia kategorii efektów (W - wiedza, U - umiejętności, K - kompetencje społeczne),
- numer efektu w obrębie danej kategorii, zapisany w postaci dwóch cyfr (numery od 1 do 9 należy poprzedzić cyfrą 0).

W kolumnie odniesienia do charakterystyki drugiego stopnia efektów uczenia się należy wskazać kody składników opisu efektów uczenia się zaczerpnięte z opisu efektów uczenia się , zgodnie z Ustawą o Zintegrowanym Systemie Kwalifikacji oraz Rozporządzenia Ministra Nauki i Szkolnictwa Wyższego w sprawie charakterystyk drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-8 Polskiej Ramy Kwalifikacji z dnia 14 listopada 2018 r. (Dz.U. z 2018 r., poz. 2218). Występujące w charakterystykach kody składnika opisu są złożone z następujących elementów:

- jedna litera P – dla oznaczenia słowa poziom;
- jedna z cyfr 6, 7, 8 – dla oznaczenia numeru poziomu (6 – szósty, 7 – siódmy, 8 – ósmy);
- jedna litera S – dla oznaczenia słowa studia;
- znak _ (podkreślnik),
- jedna z liter W, U lub K - dla oznaczenia kategorii efektów (W - wiedza, U - umiejętności, K - kompetencje społeczne),
- jedna z liter:
  - G – występującą w kategorii wiedza, która określa zakres i głębię/kompletność perspektywy poznawczej i zależności,
  - K – występującą w kategorii wiedza, która określa kontekst/uwarunkowania, skutki,
  - W – występującą w kategorii umiejętności, która określa wykorzystanie wiedzy/rozwiązywane problemy i wykonywane zadania,
  - K – występującą w kategorii umiejętności, która określa komunikowanie się/ odbieranie i tworzenie wypowiedzi, upowszechnianie wiedzy w środowisku naukowym i posługiwanie się językiem obcym,
  - O – występującą w kategorii umiejętności, która określa organizację pracy/planowanie i pracę zespołową,
  - U – występującą w kategorii umiejętności, która określa uczenie się/ planowanie własnego rozwoju i rozwoju innych osób,
  - K – występującą w kategorii kompetencje społeczne, która określa oceny/krytyczne podejście,
  - O – występującą w kategorii kompetencje społeczne, która określa odpowiedzialność/wypełnianie zobowiązań społecznych i działanie na rzecz interesu społecznego,
  - R – występującą w kategorii kompetencje społeczne, która określa rolę zawodową/niezależność i rozwój etosu.