

*Załącznik
do Uchwały Senatu nr T.0022.81.2026
z dnia 25 czerwca 2026 roku*

PROGRAM STUDIÓW PODYPLOMOWYCH

Studia realizowane przy Katedrze Bankowości i Globalnego Systemu Finansowego UEK

Nazwa studiów: *Digital banking: ryzyko operacyjne i compliance*

1. Adresaci studiów:

Studia podyplomowe „Digital banking: ryzyko operacyjne i compliance” są skierowane przede wszystkim do osób pracujących lub planujących rozwój zawodowy w sektorze bankowym, finansowym i fintechowym. Program jest adresowany do pracowników banków, instytucji finansowych oraz firm technologicznych współpracujących z branżą finansową, szczególnie tych zajmujących się zarządzaniem ryzykiem operacyjnym, funkcją compliance, audytem, bezpieczeństwem informacji, cyberbezpieczeństwem i kontrolą wewnętrzną.

Kierunek jest również dobrym wyborem dla specjalistów IT związanych z cyfryzacją usług finansowych oraz osób zainteresowanych nowoczesnymi technologiami wykorzystywanymi w bankowości cyfrowej. Program obejmuje zagadnienia związane z ryzykiem operacyjnym, compliance, ochroną danych, cyberzagrożeniami, regulacjami bankowymi oraz transformacją cyfrową sektora finansowego, przygotowując uczestników do pracy na stanowiskach związanych z nadzorem, kontrolą i bezpieczeństwem procesów w dynamicznie rozwijającej się bankowości cyfrowej.

2. Cel studiów:

Celem studiów podyplomowych „Digital banking: ryzyko operacyjne i compliance” jest przygotowanie uczestników do efektywnego funkcjonowania w nowoczesnym sektorze bankowym i finansowym poprzez zdobycie wiedzy oraz praktycznych kompetencji z zakresu zarządzania ryzykiem operacyjnym, compliance oraz cyfrowej transformacji usług finansowych. Studia mają na celu rozwinięcie umiejętności identyfikowania i ograniczania ryzyk związanych z działalnością instytucji finansowych, zapewniania zgodności procesów z obowiązującymi regulacjami prawnymi oraz wdrażania nowoczesnych rozwiązań technologicznych wspierających bezpieczeństwo i efektywność bankowości cyfrowej. Program

kształcenia umożliwia także zdobycie wiedzy dotyczącej cyberbezpieczeństwa, ochrony danych, regulacji sektora finansowego oraz zarządzania procesami w środowisku cyfrowym, przygotowując słuchaczy do pracy w dynamicznie rozwijającym się obszarze bankowości cyfrowej i firmach fintech.

3. Program studiów:

LP.	NAZWA PRZEDMIOTU	LICZBA GODZIN	PUNKTY ECTS
1.	Wprowadzenie do bankowości cyfrowej	20	4
2.	Sieć bezpieczeństwa finansowego	10	2
3.	Ochrona konsumenta na cyfrowym rynku finansowym	10	2
4.	Regulacje dotyczące bankowości cyfrowej	20	4
5.	Ryzyko operacyjne w bankowości	20	4
6.	Cyberbezpieczeństwo w instytucjach finansowych	20	4
7.	Compliance w bankowości cyfrowej	20	4
8.	AML/CFT w środowisku cyfrowym	20	3
9.	Zarządzanie danymi i sztuczna inteligencja w bankowości	20	3
	Razem	160	30

4. Czas trwania studiów i liczba godzin:

Zajęcia na kierunku Digital banking: ryzyko operacyjne i compliance w ramach studiów podyplomowych odbywać się będą w formie stacjonarnej i zdalnej. Zajęcia będą odbywać się tylko w soboty w godzinach 9:00 – 18:00. Wymiar godzin studiów podyplomowych to 160 godzin. Czas trwania studiów podyplomowych to dwa semestry. Język prowadzenia studiów: polski.

5. Warunki oraz sposób zaliczenia studiów:

Zaliczenia semestrów odbywają się w formie pisemnych egzaminów semestralnych. Na zakończenie studiów uczestnicy przystępują do ustnego egzaminu końcowego. Ukończenie studiów wymaga uzyskania pozytywnych ocen ze wszystkich egzaminów oraz udziału w zajęciach.

6. Efekty uczenia się:

Efekty uczenia się dla studiów podyplomowych		
Jednostka prowadząca:	Katedra Bankowości i Globalnego Systemu Finansowego UEK	
Nazwa studiów podyplomowych:	Digital banking: ryzyko operacyjne i compliance	
Dziedzina nauki:	Nauki społeczne	
Profil studiów:	ogólnoakademicki	
Poziom PRK	7	
Poziom studiów:	podyplomowe	
Liczba semestrów:	2	
Symbol efektu uczenia się dla kierunku	ESM	Odniesienie do charakterystyk efektów uczenia się
P_W (WIEDZA) Uczestnik zna i rozumie:		
DBRC_W1	w pogłębionym stopniu, teorie i koncepcje oraz zależności ekonomiczno-społeczne stanowiące pogłębioną wiedzę z zakresu bankowości cyfrowej	P7S_WG
DBRC_W2	prawne, organizacyjne i etyczne uwarunkowania wykonywania działalności zawodowej w ramach studiowanego kierunku studiów Digital banking: ryzyko operacyjne i compliance	P7S_WK
DBRC_W3	w pogłębionym stopniu funkcjonowanie podmiotów związanych z nowymi technologiami w bankowości	P7S_WG
DBRC_W4	w pogłębionym stopniu proces zmian zachodzący w obszarze ryzyka operacyjnego i compliance w bankowości	P7S_WG
P_U (UMIEJĘTNOŚCI) Uczestnik potrafi:		
DBRC_U1	wykorzystać posiadaną wiedzę do twórczego formułowania i rozwiązywania złożonych oraz niestandardowych problemów związanych z zarządzaniem ryzykiem operacyjnym i compliance w bankowości cyfrowej	P7S_UW
DBRC_U2	dobierać i stosować właściwe metody i narzędzia, w tym zaawansowane techniki informacyjne, do rozwiązywania pojawiających się problemów w zakresie zarządzania ryzykiem operacyjnym i compliance	P7S_UW

DBRC_U3	kierować pracą zespołu, współdziałać z innymi osobami w ramach prac zespołowych przyjmując postawę lidera, motywować i inspirować członków zespołu do aktywności	P7S_UO
DBRC_U4	komunikować się na tematy związane z zarządzaniem ryzykiem operacyjnym i kontrolą z szerokim i zróżnicowanym kręgiem odbiorców i partnerów	P7S_UK
DBRC_U5	samodzielnie planować i realizować własne uczenie się przez całe życie	P7S_UU
P_K (KOMPETENCJE SPOŁECZNE) Uczestnik jest gotów do:		
DBRC_K1	uznawania znaczenia wiedzy w rozwiązywaniu problemów z zakresu zagadnień zarządczych i praktycznych dotyczących ryzyka operacyjnego i compliance	P7S_KK
DBRC_K2	do wypełniania zobowiązań społecznych oraz inspirowania i organizowania działalności na rzecz środowiska społecznego	P7S_KO
DBRC_K3	do odpowiedzialnego pełnienia ról zawodowych z uwzględnieniem zmieniających się potrzeb społecznych, w tym do podtrzymywania odpowiedniego etosu zawodu.	P7S_KR

Objaśnienia oznaczeń w symbolach dotyczących kierunku studiów podyplomowych:

Skrót – kierunek studiów podyplomowych Digital banking: ryzyko operacyjne i compliance (DBRC)

W – kategoria wiedzy

U – kategoria umiejętności

K – kategoria kompetencji społecznych

1, 2, 3 i kolejne – numer efektu uczenia się

Objaśnienia oznaczeń w odniesieniach do charakterystyk efektów uczenia się

P – poziom Polskiej Ramy Kwalifikacji (PRK)

P7S – charakterystyka drugiego stopnia poziomu 7 PRK

P7U_W – charakterystyka uniwersalna (WIEDZA):

P7S_WG – charakterystyka drugiego stopnia (zakres i głębokość)

P7S_WK – charakterystyka drugiego stopnia (kontekst)

P7U_U – charakterystyka uniwersalna (UMIEJĘTNOŚCI):

P7S_UW – charakterystyka drugiego stopnia (wykorzystanie wiedzy)

P7S_UK – charakterystyka drugiego stopnia (komunikowanie się)

P7S_UO – charakterystyka drugiego stopnia (organizacja pracy)

P7S_UU – charakterystyka drugiego stopnia (uczenie się)

P7U_K – charakterystyka uniwersalna (KOMPETENCJE SPOŁECZNE):

P7S_KK – charakterystyka drugiego stopnia (oceny/krytyczne podejście)

P7S_KO – charakterystyka drugiego stopnia (odpowiedzialność)

P7S_KR – charakterystyka drugiego stopnia (rola zawodowa)

Skrócone karty przedmiotów:

Nazwa przedmiotu
Wprowadzenie do bankowości cyfrowej
Język prowadzenia zajęć
Język polski
Realizowane efekty uczenia się
Wiedza: Uczestnik zna i rozumie w pogłębionym stopniu teorie, koncepcje oraz zależności ekonomiczno-społeczne związane z funkcjonowaniem bankowości cyfrowej oraz podmiotów wykorzystujących nowe technologie w sektorze finansowym. (DBRC_W1, DBRC_W3; P7S_WG) Umiejętności: Uczestnik potrafi wykorzystywać wiedzę oraz nowoczesne narzędzia informacyjne do analizowania procesów transformacji cyfrowej i rozwiązywania problemów związanych z funkcjonowaniem bankowości cyfrowej. (DBRC_U1, DBRC_U2; P7S_UW) Kompetencje społeczne: Uczestnik jest gotów do uznawania znaczenia wiedzy i nowych technologii w rozwiązywaniu problemów praktycznych sektora finansowego oraz odpowiedzialnego pełnienia ról zawodowych. (DBRC_K1, DBRC_K3; P7S_KK, P7S_KR)
Treści programowe przedmiotu
1. Istota i rozwój bankowości cyfrowej. 2. Modele bankowości elektronicznej i mobilnej. 3. Fintech i innowacje finansowe. 4. Open banking i PSD2. 5. Transformacja cyfrowa sektora finansowego. 6. Wpływ nowych technologii na relacje z klientem.

Nazwa przedmiotu
Sieć bezpieczeństwa finansowego
Język prowadzenia zajęć
Język polski
Realizowane efekty uczenia się
Wiedza: Uczestnik zna i rozumie w pogłębionym stopniu zasady funkcjonowania instytucji odpowiedzialnych za stabilność systemu finansowego oraz regulacyjne i organizacyjne uwarunkowania bezpieczeństwa rynku finansowego. (DBRC_W2, DBRC_W4; P7S_WG, P7S_WK) Umiejętności: Uczestnik potrafi analizować mechanizmy ograniczania ryzyka systemowego oraz dobierać właściwe rozwiązania wspierające bezpieczeństwo instytucji finansowych. (DBRC_U1, DBRC_U2; P7S_UW) Kompetencje społeczne: Uczestnik jest gotów do odpowiedzialnego działania na rzecz stabilności systemu finansowego oraz współpracy z otoczeniem instytucjonalnym. (DBRC_K2, DBRC_K3; P7S_KO, P7S_KR)
Treści programowe przedmiotu
1. Pojęcie i znaczenie sieci bezpieczeństwa finansowego. 2. Rola banku centralnego. 3. System gwarantowania depozytów. 4. Nadzór nad rynkiem finansowym. 5. Zarządzanie kryzysowe w sektorze bankowym. 6. Stabilność systemu finansowego w środowisku cyfrowym.

Nazwa przedmiotu
Ochrona konsumenta na rynku cyfrowym rynku finansowym
Język prowadzenia zajęć
Język polski
Realizowane efekty uczenia się
Wiedza: Uczestnik zna i rozumie w pogłębionym stopniu prawne, organizacyjne i etyczne aspekty ochrony konsumenta korzystającego z usług finansowych w środowisku cyfrowym. (DBRC_W2; P7S_WG) Umiejętności: Uczestnik potrafi identyfikować problemy związane z ochroną klienta rynku finansowego oraz stosować odpowiednie regulacje i narzędzia wspierające bezpieczeństwo konsumentów. (DBRC_U1, DBRC_U4; P7S_UW, P7S_UO) Kompetencje społeczne: Uczestnik jest gotów do odpowiedzialnego pełnienia ról zawodowych z uwzględnieniem ochrony interesów klientów oraz standardów etycznych. (DBRC_K2, DBRC_K3; P7S_KO, P7S_KR)
Treści programowe przedmiotu
1. Prawa konsumenta na rynku finansowym. 2. Ochrona danych osobowych klientów. 3. Bezpieczeństwo usług cyfrowych. 4. Reklamacje i odpowiedzialność instytucji finansowych. 5. Nadużycia i cyberzagrożenia wobec klientów. 6. Edukacja finansowa konsumentów.

Nazwa przedmiotu
Regulacje w bankowości cyfrowej
Język prowadzenia zajęć
Język polski
Realizowane efekty uczenia się
Wiedza: Uczestnik zna i rozumie w pogłębionym stopniu regulacje prawne oraz organizacyjne uwarunkowania funkcjonowania bankowości cyfrowej i nowych technologii finansowych. (DBRC_W2, DBRC_W3; P7S_WG) Umiejętności: Uczestnik potrafi interpretować przepisy prawa oraz stosować odpowiednie rozwiązania compliance w działalności instytucji finansowych. (DBRC_U1, DBRC_U2; P7S_UW) Kompetencje społeczne: Uczestnik jest gotów do odpowiedzialnego wykonywania obowiązków zawodowych zgodnie z regulacjami i standardami rynku finansowego. (DBRC_K1, DBRC_K3; P7S_KK, P7S_KR)
Treści programowe przedmiotu
1. System regulacji rynku finansowego. 2. PSD2/3 i open banking. 3. DORA i cyberodporność sektora finansowego. 4. RODO w bankowości cyfrowej. 5. Regulacje dotyczące usług płatniczych. 6. Rozporządzenie o sztucznej inteligencji (AI Act 2026)

Nazwa przedmiotu
Ryzyko operacyjne w bankowości
Język prowadzenia zajęć
Język polski
Realizowane efekty uczenia się
Wiedza: Uczestnik zna i rozumie w pogłębionym stopniu procesy oraz zmiany zachodzące w obszarze zarządzania ryzykiem operacyjnym w instytucjach finansowych. (DBRC_W4; P7S_WK) Umiejętności: Uczestnik potrafi identyfikować, analizować i ograniczać ryzyko operacyjne przy wykorzystaniu odpowiednich metod i narzędzi zarządczych. (DBRC_U1, DBRC_U2; P7S_UW) Kompetencje społeczne: Uczestnik jest gotów do uznawania znaczenia zarządzania ryzykiem operacyjnym w zapewnianiu bezpieczeństwa organizacji i interesariuszy. (DBRC_K1; P7S_KK)
Treści programowe przedmiotu
1. Istota ryzyka operacyjnego. 2. Źródła i klasyfikacja ryzyka operacyjnego. 3. Metody identyfikacji i pomiaru ryzyka. 4. System kontroli wewnętrznej. 5. Zarządzanie incydentami i ciągłość działania. 6. Raportowanie ryzyka operacyjnego.

Nazwa przedmiotu
Cyberbezpieczeństwo w instytucjach finansowych
Język prowadzenia zajęć
Język polski
Realizowane efekty uczenia się
Wiedza: Uczestnik zna i rozumie w pogłębionym stopniu zagadnienia związane z cyberbezpieczeństwem oraz funkcjonowaniem systemów ochrony informacji w sektorze finansowym. (DBRC_W2, DBRC_W3; P7S_WG) Umiejętności: Uczestnik potrafi dobierać i stosować narzędzia wspierające ochronę systemów informatycznych oraz reagowanie na incydenty bezpieczeństwa. (DBRC_U2, DBRC_U3; P7S_UW, P7S_UK) Kompetencje społeczne: Uczestnik jest gotów do odpowiedzialnego działania na rzecz bezpieczeństwa informacji oraz współpracy w zespołach odpowiedzialnych za cyberbezpieczeństwo. (DBRC_K2, DBRC_K3; P7S_KO, P7S_KR)
Treści programowe przedmiotu
1. Podstawy cyberbezpieczeństwa. 2. Zagrożenia cybernetyczne w sektorze finansowym. 3. Ochrona danych i systemów IT. 4. Zarządzanie incydentami bezpieczeństwa. 5. Cyberodporność organizacji finansowych. 6. Standardy i regulacje bezpieczeństwa IT.

Nazwa przedmiotu
Compliance w bankowości cyfrowej
Język prowadzenia zajęć
Język polski
Realizowane efekty uczenia się
Wiedza: Uczestnik zna i rozumie w pogłębionym stopniu organizacyjne, prawne i etyczne aspekty compliance w instytucjach finansowych działających w środowisku cyfrowym. (DBRC_W2, DBRC_W4; P7S_WG, P7S_WK) Umiejętności: Uczestnik potrafi stosować procedury compliance oraz rozwiązywać problemy związane z zapewnieniem zgodności działalności bankowej z regulacjami. (DBRC_U1, DBRC_U2; P7S_UW) Kompetencje społeczne: Uczestnik jest gotów do odpowiedzialnego pełnienia funkcji związanych z nadzorem zgodności i promowania etycznych standardów działania. (DBRC_K1, DBRC_K3; P7S_KK, P7S_KR)
Treści programowe przedmiotu
1. Istota i funkcje compliance. 2. System zarządzania zgodnością w instytucjach finansowych. 3. Zasady etyczne i standardy profesjonalnego zachowania w bankowości. 4. Monitoring i raportowanie compliance. 5. Konsekwencje braku zgodności. 6. Compliance w środowisku cyfrowym: prywatność danych i AI

Nazwa przedmiotu
AML/CFT w środowisku cyfrowym
Język prowadzenia zajęć
Język polski
Realizowane efekty uczenia się
Wiedza: Uczestnik zna i rozumie w pogłębionym stopniu regulacje i mechanizmy przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu w środowisku cyfrowym. (DBRC_W2, DBRC_W4; P7S_WG, P7S_WK) Umiejętności: Uczestnik potrafi wykorzystywać metody analizy ryzyka AML/CFT oraz stosować narzędzia wspierające monitorowanie transakcji i identyfikację nadużyć. (DBRC_U1, DBRC_U2; P7S_UW) Kompetencje społeczne: Uczestnik jest gotów do odpowiedzialnego działania na rzecz bezpieczeństwa obrotu finansowego oraz przeciwdziałania przestępczości finansowej. (DBRC_K1, DBRC_K3; P7S_KK, P7S_KR)
Treści programowe przedmiotu
1. Podstawy AML/CFT. 2. Identyfikacja i weryfikacja klienta (KYC). 3. Monitorowanie transakcji finansowych. 4. Analiza ryzyka AML/CFT. 5. Technologie wspierające wykrywanie nadużyć. 6. Obowiązki instytucji obowiązanych.

Nazwa przedmiotu
Zarządzanie danymi i sztuczna inteligencja w bankowości
Język prowadzenia zajęć
Język polski
Realizowane efekty uczenia się
Wiedza: Uczestnik zna i rozumie w pogłębionym stopniu znaczenie danych oraz nowych technologii, w tym sztucznej inteligencji, w funkcjonowaniu nowoczesnej bankowości. (DBRC_W1, DBRC_W3; P7S_WG) Umiejętności: Uczestnik potrafi wykorzystywać zaawansowane techniki informacyjne i narzędzia analityczne do rozwiązywania problemów związanych z przetwarzaniem danych w sektorze finansowym. (DBRC_U1, DBRC_U2; P7S_UW) Kompetencje społeczne: Uczestnik jest gotów do odpowiedzialnego wykorzystywania danych i technologii AI z uwzględnieniem aspektów etycznych i społecznych. (DBRC_K2, DBRC_K3; P7S_KO, P7S_KR)
Treści programowe przedmiotu
1. Zarządzanie danymi w instytucjach finansowych. 2. Big Data i analityka danych. 3. Sztuczna inteligencja w bankowości. 4. Automatyzacja procesów finansowych. 5. Etyka i bezpieczeństwo AI. 6. Wykorzystanie machine learning w analizie ryzyka.