



BR.0211.125.2025

**Uchwała nr 3599**  
**Senatu Uniwersytetu w Białymstoku**  
**z dnia 17 grudnia 2025 r.**

**w sprawie ustalenia, obowiązującego od roku akademickiego 2026/2027,**  
**programu studiów na kierunku**  
**prawo nowych technologii i cyberbezpieczeństwa,**  
**na poziomie studiów drugiego stopnia**  
**o profilu ogólnoakademickim**

Na podstawie § 33 ust. 1 pkt 12 Statutu Uniwersytetu w Białymstoku (t.j. Obwieszczenie nr 4/2025 Rektora Uniwersytetu w Białymstoku z dnia 1 października 2025 r.) Senat Uniwersytetu w Białymstoku uchwala, co następuje:

**§ 1**

1. Senat Uniwersytetu w Białymstoku ustala, obowiązujący od roku akademickiego 2026/2027, program studiów na kierunku prawo nowych technologii i cyberbezpieczeństwa, na poziomie studiów drugiego stopnia o profilu ogólnoakademickim.
2. Program studiów stanowi Załącznik do niniejszej Uchwały.

**§ 2**

Uchwała wchodzi w życie z dniem podjęcia.

**Przewodniczący**  
**Senatu Uniwersytetu w Białymstoku**  
**prof. dr hab. Mariusz Popławski**

**PROGRAM STUDIÓW**  
**Kierunek studiów:**  
**Prawo nowych technologii i cyberbezpieczeństwa**  
obowiązuje od roku akademickiego: 2026/2027

**Część I. Informacje ogólne.**

1. Nazwa jednostki prowadzącej kształcenie: Wydział Prawa
2. Poziom kształcenia: studia drugiego stopnia (studia stacjonarne)
3. Profil kształcenia: ogólnoakademicki
4. Liczba semestrów: 4
5. Łączna liczba punktów ECTS konieczna do ukończenia studiów: 105
6. Łączna liczba godzin zajęć konieczna do ukończenia studiów: 984
7. Zaopiniowano na radzie wydziału w dniu: 21 listopada 2025 r.
8. Kod Międzynarodowej Standardowej Klasyfikacji Edukacji (ISCED): 0499
9. Wskazanie dyscypliny wiodącej, w której będzie uzyskiwana ponad połowa efektów uczenia się oraz procentowy udział poszczególnych dyscyplin, w ramach których będą uzyskiwane efekty uczenia się określone w programie studiów:

| Nazwa dyscypliny wiodącej      | Procentowy udział dyscypliny wiodącej      |
|--------------------------------|--------------------------------------------|
| nauki prawne                   | 80,00                                      |
| Nazwy poszczególnych dyscyplin | Procentowy udział poszczególnych dyscyplin |
| nauki o zarządzaniu i jakości  | 10,48                                      |
| nauki o bezpieczeństwie        | 5,71                                       |
| informatyka                    | 1,90                                       |
| językoznawstwo                 | 1,90                                       |
| Razem:                         | 100 %                                      |

**Część II. Efekty uczenia się.**

| Symbol opisu charakterystyk drugiego stopnia PRK | Symbol efektu uczenia się | Opis efektu uczenia się                                                                                                             |
|--------------------------------------------------|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <b>Wiedza, absolwent zna i rozumie:</b>          |                           |                                                                                                                                     |
| <b>P7S_WG</b>                                    | <b>KP7_WG1</b>            | fakty, obiekty i zjawiska obejmujące zaawansowaną wiedzę z zakresu nowych technologii lub cyberbezpieczeństwa w pogłębionym stopniu |

|                                         |                |                                                                                                                                                                                                                                                                                        |
|-----------------------------------------|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                         | <b>KP7_WG2</b> | metody i teorie wyjaśniające złożone relacje między faktami, obiektami i zjawiskami, obejmujące zaawansowaną wiedzę ogólną z zakresu nauk prawnych, nauk o zarządzaniu i jakości lub nauk o bezpieczeństwie z zakresu nowych technologii lub cyberbezpieczeństwa w pogłębionym stopniu |
|                                         | <b>KP7_WG3</b> | kluczowe zagadnienia stanowiące podstawy teoretyczne nauk prawnych, nauk o zarządzaniu i jakości, o bezpieczeństwie i informatyki z zakresu nowych technologii lub cyberbezpieczeństwa w pogłębionym stopniu                                                                           |
|                                         | <b>KP7_WG4</b> | aspekty prawne i organizacyjne funkcjonowania sektora publicznego i prywatnego na płaszczyźnie krajowej lub międzynarodowej z zakresu nowych technologii lub cyberbezpieczeństwa w pogłębionym stopniu                                                                                 |
|                                         | <b>KP7_WG5</b> | w pogłębionym stopniu różne rodzaje więzi społecznych istniejących w ramach organizacji oraz o występujących między nimi prawidłowościach                                                                                                                                              |
|                                         | <b>KP7_WG6</b> | główne trendy w rozwoju i najnowsze osiągnięcia nauk prawnych, nauk o zarządzaniu i jakości lub o bezpieczeństwie z zakresu nowych technologii lub cyberbezpieczeństwa                                                                                                                 |
| <b>P7S_WK</b>                           | <b>KP7_WK1</b> | fundamentalne dylematy współczesnej cywilizacji w obszarze nowych technologii lub cyberbezpieczeństwa                                                                                                                                                                                  |
|                                         | <b>KP7_WK2</b> | złożone uwarunkowania etyczne, prawne lub ekonomiczne prowadzenia działalności zawodowej w obszarze nowych technologii lub cyberbezpieczeństwa                                                                                                                                         |
|                                         | <b>KP7_WK3</b> | zasady prognozowania i modelowania złożonych procesów społecznych                                                                                                                                                                                                                      |
|                                         | <b>KP7_WK4</b> | zasady ochrony własności przemysłowej, intelektualnej i prawa autorskiego                                                                                                                                                                                                              |
|                                         | <b>KP7_WK5</b> | podstawowe zasady tworzenia i rozwoju różnych form przedsiębiorczości w obszarze nowych technologii lub cyberbezpieczeństwa                                                                                                                                                            |
| <b>Umiejętności, absolwent potrafi:</b> |                |                                                                                                                                                                                                                                                                                        |
| <b>P7S_UW</b>                           | <b>KP7_UW1</b> | formułować i weryfikować hipotezy związane z prostymi lub złożonymi, a także nietypowymi problemami występującymi w obszarze nowych technologii lub cyberbezpieczeństwa                                                                                                                |

|               |                |                                                                                                                                                                                                                  |
|---------------|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               | <b>KP7_UW2</b> | dobrac, adekwatnie do założonych celów i stosować metody i narzędzia badawcze z zakresu nauk prawnych, nauk o zarządzaniu i jakości lub o bezpieczeństwie, odpowiednio je przystosować lub opracować nowe        |
|               | <b>KP7_UW3</b> | interpretować otrzymane wyniki i formułować wnioski na ich podstawie, także w oparciu o dane z odpowiednio dobranych źródeł informacji naukowej                                                                  |
|               | <b>KP7_UW4</b> | korzystając z różnych źródeł, właściwie dobierać literaturę naukową polsko- i obcojęzyczną do badanych problemów, uzyskane informacje syntetyzować i poddawać krytycznej analizie                                |
|               | <b>KP7_UW5</b> | posługiwać się zaawansowanymi technikami informacyjno-komunikacyjnymi w celu prezentacji, w formie ustnej, pisemnej lub multimedialnej, wyników badań w obszarze nowych technologii lub cyberbezpieczeństwa      |
| <b>P7S_UK</b> | <b>KP7_UK1</b> | posługiwać się specjalistyczną terminologią naukową z obszaru nowych technologii lub cyberbezpieczeństwa w języku polskim lub obcym, w praktyce zawodowej oraz w komunikacji ze zróżnicowanymi kręgami odbiorców |
|               | <b>KP7_UK2</b> | występować publicznie w języku polskim lub obcym, prezentując specjalistyczne zagadnienia z obszaru nowych technologii lub cyberbezpieczeństwa, uzasadniać swoje opinie lub prowadzić debatę                     |
|               | <b>KP7_UK3</b> | porozumiewać się w języku obcym na poziomie B2+ Europejskiego Systemu Opisu Kształcenia Językowego                                                                                                               |
| <b>P7S_UO</b> | <b>KP7_UO1</b> | podejmować obowiązki kierowania zespołem przy planowaniu i wykonywaniu powierzonych zadań                                                                                                                        |
|               | <b>KP7_UO2</b> | pracować w grupie, przyjmując w niej różne role, podejmować decyzje i wdrażać proponowane rozwiązania                                                                                                            |
| <b>P7S_UU</b> | <b>KP7_UU1</b> | samodzielnie planować własne uczenie się i karierę zawodową w obszarze nowych technologii lub cyberbezpieczeństwa oraz motywować innych do podejmowania takich działań                                           |
|               | <b>KP7_UU2</b> | motywować innych do uczenia się i planowania kariery zawodowej w obszarze nowych technologii lub cyberbezpieczeństwa                                                                                             |

| <b>Kompetencje społeczne, absolwent jest gotów do:</b> |                |                                                                                                                                                                                                                                       |
|--------------------------------------------------------|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>P7S_KK</b>                                          | <b>KP7_KK1</b> | systematycznego aktualizowania i weryfikowania posiadanej wiedzy oraz racjonalnego i krytycznego podejścia do informacji pochodzących z różnych źródeł, uznając znaczenie wiedzy w rozwiązywaniu problemów poznawczych i praktycznych |
|                                                        | <b>KP7_KK2</b> | kontaktu z ekspertami w przypadku niemożności samodzielnego rozwiązania problemu                                                                                                                                                      |
| <b>P7S_KO</b>                                          | <b>KP7_KO1</b> | wypełniania zobowiązań społecznych służących promowaniu odpowiedzialnego wykorzystania nowych technologii                                                                                                                             |
|                                                        | <b>KP7_KO2</b> | inspirowania i organizowania działalności na rzecz środowiska społecznego lub cyberbezpieczeństwa                                                                                                                                     |
|                                                        | <b>KP7_KO3</b> | myślenia i działania w sposób przedsiębiorczy w obszarze nowych technologii lub cyberbezpieczeństwa                                                                                                                                   |
| <b>P7S_KR</b>                                          | <b>KP7_KR1</b> | stałego rozwijania swoich kompetencji zawodowych oraz dostosowywanie ich do zmieniających się potrzeb społecznych i technologicznych                                                                                                  |
|                                                        | <b>KP7_KR2</b> | postępowania zgodnie z zasadami etyki w pracy zawodowej i podtrzymywanie etosu swojego zawodu                                                                                                                                         |

### **Część III. Opis procesu prowadzącego do uzyskania efektów uczenia się.**

#### **Treści programowe zajęć lub grup zajęć.**

##### **1. Systemy inteligentne**

###### **KP7\_WG1, KP7\_WG3, KP7\_WK1, KP7\_WG6, KP7\_KK1**

Celem przedmiotu jest przekazanie wiedzy z zakresu funkcjonowania systemów inteligentnych, w tym sztucznej inteligencji, w obszarze prawa nowych technologii. Omówione zostaną zasady działania takich systemów, ich zastosowanie, problemy związane z ich regulacją prawną oraz zagadnienia etyczne i prawne związane z ich wdrażaniem i funkcjonowaniem w różnych sferach życia społecznego i gospodarczego.

##### **2.Ochrona praw jednostki w erze cyfrowej**

###### **KP7\_WG2, KP7\_WG4, KP7\_WK2, KP7\_KO1**

Celem przedmiotu jest przekazanie wiedzy na temat ochrony praw jednostki w środowisku cyfrowym, w szczególności ochrony danych osobowych, prywatności, prawa do bycia zapomnianym oraz ochrony dóbr osobistych w cyberprzestrzeni.

Omówione zostaną także międzynarodowe i krajowe regulacje prawne oraz obowiązki administratorów danych.

### **3. Prawo autorskie w dobie nowych technologii**

**KP7\_WG3, KP7\_WK3, KP7\_UW4**

Celem przedmiotu jest przekazanie wiedzy z zakresu praw autorskich obejmującej, w szczególności, problematykę ochrony autorskich praw majątkowych i osobistych, instytucję dozwolonego użytku prywatnego i publicznego. W ramach przedmiotu zostaną omówione też kwestie plagiatu i prawa cytatu.

### **4. Prawo własności przemysłowej w dobie nowych technologii**

**KP7\_WG3, KP7\_WK3, KP7\_UW4**

Celem przedmiotu jest przekazanie wiedzy z zakresu prawa własności intelektualnej obejmującej problematykę mediów społecznościowych, w szczególności ochrony praw autorskich do treści publikowanych online, odpowiedzialności za naruszenia własności intelektualnej w mediach społecznościowych oraz zasad korzystania z cudzych utworów i znaków towarowych w sieci. W ramach przedmiotu zostaną omówione też kwestie licencjonowania treści cyfrowych, prawa do wizerunku oraz naruszeń dokonywanych przez użytkowników platform społecznościowych.

### **5. Nowoczesne technologie w prawie Unii Europejskiej**

**KP7\_UW3, KP7\_UW4, KP7\_UK1**

Celem przedmiotu jest przekazanie wiedzy z zakresu unijnych regulacji prawnych dotyczących funkcjonowania nowoczesnych technologii, w tym ochrony danych osobowych, sztucznej inteligencji, usług cyfrowych i jednolitego rynku cyfrowego. W ramach zajęć omówione zostaną najnowsze akty prawne UE oraz ich znaczenie dla przedsiębiorców i konsumentów.

### **6. Etyka a nowe technologie**

**KP7\_WK1, KP7\_WK2, KP7\_KR2**

Celem przedmiotu jest przekazanie wiedzy z zakresu teoretycznych i praktycznych podstaw etyki w kontekście nowych technologii. Przedstawione zostaną kwestie rozwiązywania dylematów natury moralno-prawnej występujących w obszarach takich jak prywatność danych, sztuczna inteligencja, big data, biotechnologia czy automatyzacja procesów decyzyjnych. W ramach zajęć omówione zostaną również standardy etyczne stosowane w działalności gospodarczej i naukowej związanej z technologiami cyfrowymi.

### **7. Przywództwo i zarządzanie zespołem**

**KP7\_WG7, KP7\_UO1, KP7\_UO2, KP7\_KR1**

Celem przedmiotu jest przekazanie wiedzy i umiejętności w zakresie zarządzania zespołami projektowymi i pracowniczymi w organizacjach funkcjonujących w środowisku nowych technologii. Omówione zostaną podstawy teorii przywództwa, budowania zespołów, zarządzania konfliktem, podejmowania decyzji oraz motywowania pracowników.

## **8. Prawne aspekty influencer marketingu lub**

**KP7\_WK2, KP7\_WK3, KP7\_UW5, KP7\_UK1**

Celem przedmiotu jest przekazanie wiedzy z zakresu prawnych aspektów działalności influencerów w mediach cyfrowych. Omówione zostaną obowiązki prawne związane z reklamą, oznaczaniem treści sponsorowanych, odpowiedzialnością za treści publikowane w Internecie, a także zagadnienia ochrony konsumentów i konkurencji w influencer marketingu.

## **8a. Działalność reklamowa w Internecie**

**KP7\_WK2, KP7\_WK3, KP7\_UW5, KP7\_UK1**

Celem przedmiotu jest przekazanie wiedzy z zakresu prawnych uwarunkowań prowadzenia działalności reklamowej w środowisku cyfrowym. Omawiane będą zasady uczciwej konkurencji, regulacje dotyczące reklamy internetowej, ochrony danych osobowych w reklamie spersonalizowanej oraz odpowiedzialność za naruszenie przepisów prawa reklamowego.

## **9. Język obcy**

**KP7\_UK1, KP7\_UK2, KP7\_UK3**

Celem przedmiotu jest prowadzenie lektoratu w formie praktycznych ćwiczeń pozwalających nabyć kompetencje językowe w zakresie mowy, pisania, czytania i słuchania. Obejmą one umiejętności posługiwania się językiem obcym na poziomie B2+ Europejskiego Systemu Kształcenia Językowego, analizy pisanych i mówionych tekstów obcojęzycznych oraz przygotowywania wystąpień ustnych i prac pisemnych.

## **10.Ochrona konkurencji na rynkach nowych technologii**

**KP7\_WG3, KP7\_WG4, KP7\_WK2, KP7\_KO1**

Celem przedmiotu jest przekazanie wiedzy z zakresu ochrony konkurencji na rynkach nowych technologii. Omówione zostaną m.in. praktyki antykonkurencyjne, nadużywanie pozycji dominującej, fuzje i przejęcia oraz rola organów ochrony konkurencji w kontekście dynamicznie rozwijających się rynków cyfrowych.

## **11.Ochrona konsumentów na rynkach nowych technologii**

**KP7\_WG3, KP7\_WG4, KP7\_WK2, KP7\_KO1**

Celem przedmiotu jest przekazanie wiedzy z zakresu ochrony konsumentów na rynkach nowych technologii. Omówione zostaną prawa konsumentów w transakcjach online, obowiązki informacyjne przedsiębiorców, nieuczciwe praktyki rynkowe oraz mechanizmy ochrony konsumentów w środowisku cyfrowym.

## **12. Obowiązki przedsiębiorców w kontekście nowych technologii lub**

**KP7\_WK2, KP7\_WK5, KP7\_UW4, KP7\_KR2**

Celem przedmiotu jest przekazanie wiedzy na temat obowiązków przedsiębiorców działających na rynkach nowych technologii. Omówione zostaną m.in. kwestie związane z regulacjami dotyczącymi ochrony danych osobowych, ochrony konsumentów, uczciwej konkurencji, własności intelektualnej oraz odpowiedzialności za szkody wyrządzone przez produkty cyfrowe.

## **12a. Obowiązki przedsiębiorców w kontekście cyberbezpieczeństwa**

## **KP7\_WK2, KP7\_WK5, KP7\_UW4, KP7\_KR2**

Celem przedmiotu jest przekazanie wiedzy na temat obowiązków przedsiębiorców w zakresie zapewnienia bezpieczeństwa systemów informatycznych i ochrony danych w związku z obowiązującymi regulacjami prawnymi oraz standardami cyberbezpieczeństwa. Omówione zostaną obowiązki związane z raportowaniem incydentów, ochroną infrastruktury krytycznej i zarządzaniem ryzykiem.

## **13. Sztuczna inteligencja a prawo własności intelektualnej (przedmiot oferowany także w j. angielskim) lub**

### **KP7\_WG3, KP7\_WK3, KP7\_WK4, KP7\_UW4**

Celem przedmiotu jest przekazanie wiedzy na temat wyzwań związanych z ochroną własności intelektualnej w kontekście wykorzystania sztucznej inteligencji. Omówione zostaną problemy autorstwa, ochrony wyników generowanych przez AI, patentowalności rozwiązań opartych na sztucznej inteligencji oraz regulacji międzynarodowych w tym zakresie.

## **13a. Prawo autorskie na jednolitym rynku cyfrowym**

### **KP7\_WG3, KP7\_WK3, KP7\_WK4, KP7\_UW4**

Celem przedmiotu jest przekazanie wiedzy z zakresu prawa autorskiego w kontekście funkcjonowania jednolitego rynku cyfrowego. Omówione zostaną m.in. zasady udostępniania utworów w sieci, zarządzanie prawami autorskimi online, odpowiedzialność dostawców platform cyfrowych oraz ochrona interesów twórców i użytkowników w środowisku cyfrowym.

## **14. Etyka specjalisty ds. compliance lub**

### **KP7\_WK1, KP7\_WK2, KP7\_KR2**

Celem przedmiotu jest przekazanie wiedzy z zakresu teoretycznych i praktycznych podstaw etyki w działalności specjalistów ds. compliance. Omówione zostaną dylematy moralno-prawne związane z przestrzeganiem przepisów prawa, identyfikacją naruszeń, przeciwdziałaniem konfliktom interesów oraz odpowiedzialnością prawną i etyczną w organizacjach.

## **14a. Etyka specjalisty ds. cyberbezpieczeństwa**

### **KP7\_WK1, KP7\_WK2, KP7\_KR2**

Celem przedmiotu jest przekazanie wiedzy na temat obowiązków przedsiębiorców działających na rynkach nowych technologii. Omówione zostaną m.in. kwestie związane z regulacjami dotyczącymi ochrony danych osobowych, ochrony konsumentów, uczciwej konkurencji, własności intelektualnej oraz odpowiedzialności za szkody wyrządzone przez produkty cyfrowe.

## **15. Funkcjonowanie przedsiębiorstw w erze nowych technologii**

### **KP7\_WG5, KP7\_WK2, KP7\_WK5, KP7\_KO3**

Celem przedmiotu jest przekazanie wiedzy dotyczącej funkcjonowania przedsiębiorstw w warunkach transformacji cyfrowej. Omówione zostaną m.in. modele biznesowe oparte na technologiach informacyjnych, adaptacja do zmian technologicznych, zarządzanie innowacjami oraz wyzwania etyczne i prawne w działalności przedsiębiorstw.



## **16. Zarządzanie ryzykiem**

**KP7\_WG7, KP7\_UW2, KP7\_UO1, KP7\_KK1**

Celem przedmiotu jest przekazanie wiedzy z zakresu identyfikacji, analizy i zarządzania ryzykiem w organizacjach funkcjonujących w środowisku nowych technologii. Omówione zostaną m.in. metody oceny ryzyka, procedury reagowania na incydenty oraz wdrażania systemów zarządzania ryzykiem.

## **17. Charakterystyka współczesnych cyberzagrożeń**

**KP7\_WG2, KP7\_WG3, KP7\_WK1, KP7\_KO1**

Celem przedmiotu jest przekazanie wiedzy na temat współczesnych cyberzagrożeń w kontekście nowych technologii i cyberbezpieczeństwa. Omówione zostaną m.in. typologie zagrożeń, analiza podatności systemów, metody ataków oraz środki przeciwdziałania incydentom bezpieczeństwa.

## **18. Proseminarium**

**KP7\_UW1, KP7\_UW3, KP7\_UW4, KP7\_UK1, KP7\_UU1, KP7\_KK1**

Celem przedmiotu jest przekazanie wiedzy z zakresu metodologii pracy naukowej, w szczególności obejmującej wybór tematu pracy magisterskiej, jego uzasadnienie, stan badań dotyczący analizowanego problemu i przygotowanie planu pracy. W ramach przedmiotu zostaną omówione też zasady prowadzenia kwerendy bibliotecznej i pozyskiwania innych źródeł wiedzy.

## **19. Bezpieczeństwo w prawie i politykach Unii Europejskiej**

**KP7\_WG1, KP7\_WG4, KP7\_WK2, KP7\_WK3**

Celem przedmiotu jest przekazanie wiedzy z zakresu europejskich regulacji prawnych i polityk w obszarze bezpieczeństwa, ze szczególnym uwzględnieniem aspektów związanych z cyberbezpieczeństwem, ochroną danych osobowych oraz zwalczaniem cyberprzestępczości.

## **20. Aspekty prawne zatrudnienia w erze cyfrowej**

**KP7\_WG4, KP7\_WG6, KP7\_WK2, KP7\_UK1**

Celem przedmiotu jest przekazanie wiedzy na temat wyzwań prawnych związanych z zatrudnieniem w środowisku cyfrowym, w tym pracy zdalnej, monitorowania pracowników, automatyzacji procesów pracy oraz ochrony praw pracowniczych w erze cyfrowej transformacji.

## **21. Zrównoważony rozwój w zarządzaniu dobrami własności intelektualnej**

**KP7\_WG3, KP7\_WK3, KP7\_UW4, KP7\_KO3**

Celem przedmiotu jest przekazanie wiedzy z zakresu zrównoważonego zarządzania dobrami własności intelektualnej. Omówione zostaną strategie ochrony własności intelektualnej, uwzględniające cele społeczne, ekonomiczne i ekologiczne w kontekście nowych technologii.

## **22. Odpowiedzialność prawna za szkody wyrządzone przez sztuczną inteligencję**

**KP7\_WG3, KP7\_WK2, KP7\_WK3, KP7\_UK1**

Celem przedmiotu jest przekazanie wiedzy na temat odpowiedzialności cywilnej i karnej za szkody wyrządzone przez systemy sztucznej inteligencji. Omówione zostaną zasady przypisywania odpowiedzialności, ryzyka technologiczne oraz aktualne propozycje legislacyjne na poziomie krajowym i unijnym

### **23. Prawo bankowe lub**

**KA7\_UW1, KA7\_UK1, KP7\_UU1, KA7\_KK1**

Celem przedmiotu jest analiza problematyki działalności bankowej w szczególności funkcjonowania systemu bankowego, instytucji wspierających system bankowy oraz czynności bankowych w oparciu o przepisy prawa oraz orzecznictwo sądowe. Szczególna uwaga zostanie zwrócona na umowę rachunku bankowego, umowę o kredyt bankowy oraz umowę gwarancji bankowej. Szeroko omawiana jest także problematyka prawnych zabezpieczeń wierzytelności banku (zabezpieczenia rzeczowe i osobiste).

### **23a. Prawo papierów wartościowych (przedmiot oferowany także w j. angielskim)**

**KA7\_UW1, KA7\_UK1, KP7\_UU1, KA7\_KK1**

Celem przedmiotu jest przekazanie wiedzy z zakresu prawa papierów wartościowych, w tym emisji, obrotu oraz nadzoru nad rynkiem kapitałowym.

### **24. Prawo własności intelektualnej w mediach społecznościowych lub**

**KP7\_WG3, KP7\_WK3, KP7\_UW4**

Celem przedmiotu jest przekazanie wiedzy z zakresu prawa własności intelektualnej obejmującej problematykę mediów społecznościowych, w szczególności ochrony praw autorskich do treści zamieszczanych w serwisach społecznościowych, odpowiedzialności użytkowników i platform za naruszenia praw własności intelektualnej oraz zasad legalnego wykorzystywania materiałów online. W ramach przedmiotu zostaną omówione też kwestie licencjonowania treści w sieci, prawa do wizerunku, odpowiedzialności za udostępnianie i rozpowszechnianie treści, a także regulacje dotyczące ochrony znaków towarowych i innych dóbr niematerialnych w przestrzeni cyfrowej.

### **24a. Ochrona danych osobowych w mediach społecznościowych**

**KP7\_WG3, KP7\_WK3, KP7\_UW4**

Celem przedmiotu jest przekazanie wiedzy z zakresu ochrony danych osobowych przetwarzanych w mediach społecznościowych. Omówione zostaną obowiązki administratorów, prawa użytkowników, problematyka zgód, profilowania oraz transgranicznego transferu danych.

### **25. Design thinking**

**KP7\_UW2, KP7\_UO1, KP7\_UO2, KP7\_KK2**

Celem przedmiotu jest przekazanie umiejętności kreatywnego i innowacyjnego rozwiązywania problemów z wykorzystaniem metodyki design thinking. Uczestnicy poznają etapy projektowania rozwiązań zorientowanych na użytkownika w środowisku nowych technologii.

## **26. Zarządzanie zmianą**

**KP7\_UW2, KP7\_UW4, KP7\_UO1, KP7\_UO2**

Celem przedmiotu jest przekazanie wiedzy i umiejętności w zakresie zarządzania procesami zmian w organizacjach funkcjonujących w środowisku dynamicznego rozwoju nowych technologii. Omówione zostaną metody wdrażania i utrzymywania zmian organizacyjnych.

## **27. Prewencja i reagowanie na incydenty, a cyberbezpieczeństwo**

**KP7\_WG1, KP7\_WG3, KP7\_WK1, KP7\_KO1**

Celem przedmiotu jest przekazanie wiedzy na temat metod prewencji i reagowania na incydenty bezpieczeństwa informatycznego. Omówione zostaną procedury reagowania, raportowania oraz współpraca z odpowiednimi organami państwowymi i międzynarodowymi.

## **28. Specjalistyczne warsztaty językowe (w jęz. obcym)**

**KP7\_UK2, KP7\_UK3, KP7\_UU1,**

Konwersatorium przygotowane jest z myślą o studentach Prawo nowych technologii i cyberbezpieczeństwa. Szczególny nacisk kładziony jest na słownictwo związane z profilem studiów. W czasie zajęć nastąpi przygotowanie do samodzielnego korzystania z obcojęzycznych źródeł literatury fachowej, wprowadzenie słownictwa specjalistycznego i samodzielnego tłumaczeniu tekstów z zakresu nowych technologii i zagadnień z nią związanych. Konwersatorium ma na celu udoskonalenie umiejętności językowych, przydatnych w przyszłej karierze zawodowej. Program zajęć zawiera praktyczne słownictwo i naukę korzystania z anglojęzycznych tekstów źródłowych.

## **29. Bezpieczeństwo danych osobowych**

**KP7\_WG1, KP7\_WK2, KP7\_UW4, KP7\_KO1**

Celem przedmiotu jest przekazanie wiedzy z zakresu ochrony danych osobowych w świetle obowiązujących regulacji krajowych i unijnych. Omówione zostaną m.in. obowiązki administratorów i podmiotów przetwarzających dane, prawa osób, których dane dotyczą, oraz odpowiedzialność za naruszenia przepisów.

## **30. Zarządzanie zgodnością (compliance) a prawo pracy**

**KP7\_WG4, KP7\_WK2, KP7\_UW4, KP7\_KO2**

Celem przedmiotu jest przekazanie wiedzy na temat wdrażania i stosowania programów zgodności w obszarze prawa pracy. Omówione zostaną mechanizmy przeciwdziałania naruszeniom prawa, polityki antymobbingowe, whistleblowing oraz etyczne aspekty zarządzania zgodnością w zatrudnieniu.

## **31. Zgłaszanie naruszeń prawa i ochrona sygnalistów**

**KP7\_WG4, KP7\_WK2, KP7\_UW4, KP7\_KO2**

Celem przedmiotu jest przekazanie wiedzy dotyczącej systemów zgłaszania nieprawidłowości (whistleblowing), ochrony prawnej sygnalistów oraz obowiązków pracodawców w kontekście wdrażania procedur zgłaszania naruszeń prawa.

### **32. Praktyczne aspekty skutecznego wdrażania i zarządzania wewnętrznym systemem zgłaszania nieprawidłowości**

**KP7\_WG4, KP7\_WK2, KP7\_UO1, KP7\_KO2**

Celem przedmiotu jest przekazanie wiedzy oraz umiejętności praktycznych w zakresie projektowania, wdrażania i prowadzenia wewnętrznych systemów zgłaszania nieprawidłowości w organizacjach, w tym zasad ich działania, ochrony sygnalistów i zarządzania zgłoszeniami.

### **33. Zarządzanie własnością intelektualną dla celów bezpieczeństwa publicznego lub**

**KP7\_WG3, KP7\_WK3, KP7\_UW4**

Celem przedmiotu jest przekazanie wiedzy na temat wykorzystania i ochrony własności intelektualnej w kontekście bezpieczeństwa publicznego, w tym praw patentowych, tajemnicy przedsiębiorstwa i transferu technologii o znaczeniu strategicznym.

#### **33a. Znaki towarowe, wzory i wynalazki w erze cyfrowej jako składniki w majątku przedsiębiorców**

**KP7\_WG3, KP7\_WK3, KP7\_UW4**

Celem przedmiotu jest przekazanie wiedzy z zakresu ochrony i zarządzania znakami towarowymi, wzorami przemysłowymi oraz patentami w realiach gospodarki cyfrowej, a także ich znaczenia jako składników majątkowych przedsiębiorców.

### **34. Zarządzanie projektami lub**

**KP7\_WG5, KP7\_WG7, KP7\_UW2, KP7\_UO1, KP7\_KR1**

Celem przedmiotu jest przekazanie wiedzy i umiejętności w zakresie zarządzania projektami, w tym planowania, realizacji, kontroli i oceny projektów związanych z wdrażaniem nowych technologii oraz cyberbezpieczeństwa.

#### **34a. Zarządzanie konfliktem i kryzysem w organizacji**

**KP7\_WG5, KP7\_WG7, KP7\_UW2, KP7\_UO1, KP7\_KR1**

Celem przedmiotu jest przekazanie wiedzy i umiejętności w zakresie zarządzania konfliktami i kryzysami w organizacjach funkcjonujących w środowisku nowych technologii, w tym metod rozwiązywania sporów, mediacji, negocjacji oraz działań prewencyjnych.

### **35. Cyberbezpieczeństwo w procesie wytwarzania i utrzymania oprogramowania**

**KP7\_WG2, KP7\_WG3, KP7\_WK1, KP7\_KO1**

Celem przedmiotu jest przekazanie wiedzy z zakresu cyberbezpieczeństwa w cyklu życia oprogramowania, w tym zarządzania podatnościami, bezpiecznego programowania, testowania bezpieczeństwa oraz reagowania na incydenty związane z błędami programistycznymi.

### **36. Seminarium**

**KP7\_UW1, KP7\_UW3, KP7\_UW4, KP7\_UK1, KP7\_UU1, KP7\_KK1**

Celem przedmiotu jest przekazanie wiedzy z zakresu przygotowania i obrony pracy magisterskiej. W jego ramach zostaną omówione zasady i sposoby analizy źródeł wiedzy, formułowania tez badawczych, gromadzenia i opracowywania materiału empirycznego oraz weryfikacji przyjętych założeń. W ramach przedmiotu zostaną omówione też poszczególne metody, techniki i narzędzia badawcze właściwe naukom prawnym stosowane podczas przygotowywania pracy magisterskiej oraz formalne aspekty jej opracowywania.

### **Sposoby weryfikacji i oceny efektów uczenia się osiągniętych przez studenta w trakcie całego cyklu kształcenia.**

Metody kształcenia określone w części A sylabusu. Sposoby weryfikacji: zaliczenie, egzamin i inne sposoby weryfikacji określone w części B sylabusu na dany rok akademicki.

### **Warunki ukończenia studiów oraz uzyskiwany tytuł zawodowy.**

1. Zasady dopuszczenia do egzaminu dyplomowego: zdanie egzaminów i uzyskanie zaliczenia przedmiotów przewidzianych programem studiów, napisanie pracy dyplomowej.
2. Zakres i sposób przeprowadzenia egzaminu dyplomowego określony jest odrębną uchwałą Rady Wydziału Prawa UwB w sprawie zasad przeprowadzania egzaminu dyplomowego.
3. Absolwent uzyskuje tytuł zawodowy magister po spełnieniu wymogów określonych w pkt. 1 i 2

Objaśnienia oznaczeń:

P6, P7 – poziom PRK (6 - studia pierwszego stopnia, 7 – studia drugiego stopnia i jednolite magisterskie)

S – charakterystyka typowa dla kwalifikacji uzyskiwanych w ramach szkolnictwa wyższego

|                           |                          |
|---------------------------|--------------------------|
| W – wiedza                | G – głębia i zakres      |
|                           | K – kontekst             |
| U – umiejętności          | W – wykorzystanie wiedzy |
|                           | K – komunikowanie się    |
|                           | O – organizacja pracy    |
|                           | U – uczenie się          |
| K – kompetencje społeczne | K – krytyczna ocena      |
|                           | O – odpowiedzialność     |
|                           | R – rola zawodowa        |

**Program studiów - wskaźniki ilościowe**

forma studiów: stacjonarne

Kierunek studiów: Prawo nowych technologii i cyberbezpieczeństwa

Poziom studiów: drugi stopień

Profil studiów: ogólnoakademicki

Forma studiów: stacjonarne

Zaopiniowany na Radzie Wydziału

W dniu: 21 listopada 2025 r.

Obowiązuje od roku akademickiego: 2026/2027

|      |                                                         |                      |                     |             | Punkty ECTS uzyskiwane<br>w ramach zajęć: |                                                                                                                                |                                                        |                                                                                                                                                                                    |                                                                           |
|------|---------------------------------------------------------|----------------------|---------------------|-------------|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| L.P. | NAZWA GRUPY ZAJĘĆ/<br>NAZWA ZAJĘĆ                       | KOD<br>ZAJĘĆ<br>USOS | Liczba godzin zajęć | punkty ECTS | do wyboru                                 | z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia i studentów (dot. studiów stacjonarnych) | z dziedziny nauk humanistycznych lub nauk społecznych* | związanych z prowadzoną w uczelni działalnością naukową w dyscyplinie lub dyscyplinach, do których przyporządkowany jest kierunek studiów, dla studiów o profilu ogólnoakademickim | kształtujących umiejętności praktyczne, dla studiów o profilu praktycznym |
| 1    | 2                                                       | 3                    | 4                   | 5           | 6                                         | 7                                                                                                                              | 8                                                      | 9                                                                                                                                                                                  | 10                                                                        |
| 1    | Systemy inteligentne                                    | 370-CS2-1SIN         | 18                  | 2           |                                           | 1                                                                                                                              |                                                        | 2                                                                                                                                                                                  |                                                                           |
| 2    | Ochrona praw jednostki w erze cyfrowej                  | 370-CS2-1OPJ         | 18                  | 2           |                                           | 1                                                                                                                              |                                                        | 2                                                                                                                                                                                  |                                                                           |
| 3    | Prawo autorskie w dobie nowych technologii              | 370-CS2-1PAD         | 42                  | 4           |                                           | 3                                                                                                                              |                                                        | 4                                                                                                                                                                                  |                                                                           |
| 4    | Prawo własności przemysłowej w dobie nowych technologii | 370-CS2-1PWP         | 42                  | 4           |                                           | 3                                                                                                                              |                                                        | 4                                                                                                                                                                                  |                                                                           |
| 5    | Nowoczesne technologie w prawie Unii Europejskiej       | 370-CS2-1NTP         | 42                  | 4           |                                           | 3                                                                                                                              |                                                        | 4                                                                                                                                                                                  |                                                                           |
| 6    | Etyka a nowe technologie                                | 370-CS2-1ENT         | 18                  | 2           |                                           | 1                                                                                                                              |                                                        | 2                                                                                                                                                                                  |                                                                           |
| 7    | Przywództwo i zarządzanie zespołem                      | 370-CS2-1PZZ         | 18                  | 2           |                                           | 1                                                                                                                              |                                                        | 2                                                                                                                                                                                  |                                                                           |
| 8    | Prawne aspekty influencer marketingu lub                | 370-CS2-1PAI         | 18                  | 2           | 2                                         | 1                                                                                                                              |                                                        | 2                                                                                                                                                                                  |                                                                           |
| 8a   | Działalność reklamowa w Internecie                      | 370-CS2-1DRI         |                     |             |                                           |                                                                                                                                |                                                        |                                                                                                                                                                                    |                                                                           |
| 9    | Język obcy                                              | 370-CS2-1LJ          | 30                  | 2           | 2                                         | 1                                                                                                                              |                                                        | 2                                                                                                                                                                                  |                                                                           |
| 10   | Ochrona konkurencji na rynkach nowych technologii       | 370-CS2-1OKR         | 42                  | 4           |                                           | 3                                                                                                                              |                                                        | 4                                                                                                                                                                                  |                                                                           |

| 1   | 2                                                                                                                                                       | 3            | 4  | 5 | 6 | 7 | 8 | 9 | 10 |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|----|---|---|---|---|---|----|
| 11  | Ochrona konsumentów na rynkach nowych technologii                                                                                                       | 370-CS2-1OKN | 42 | 4 |   | 3 |   | 4 |    |
| 12  | Obowiązki przedsiębiorców w kontekście nowych technologii lub                                                                                           | 370-CS2-1OPK | 18 | 2 | 2 | 1 |   | 2 |    |
| 12a | Obowiązki przedsiębiorców w kontekście cyberbezpieczeństwa                                                                                              | 370-CS2-1OPC |    |   |   |   |   |   |    |
| 13  | Sztuczna inteligencja a prawo własności intelektualnej (Artificial Intelligence and Intellectual Law)** (przedmiot oferowany także w j. angielskim) lub | 370-CS2-1SIP | 18 | 2 | 2 | 1 |   | 2 |    |
| 13a | Prawo autorskie na jednolitym rynku cyfrowym                                                                                                            | 370-CS2-1PAR |    |   |   |   |   |   |    |
| 14  | Etyka specjalisty ds. compliance lub                                                                                                                    | 370-CS2-1ESC | 18 | 2 | 2 | 1 |   | 2 |    |
| 14a | Etyka specjalisty ds. cyberbezpieczeństwa                                                                                                               | 370-CS2-1ECB |    |   |   |   |   |   |    |
| 15  | Funkcjonowanie przedsiębiorstw w erze nowych technologii                                                                                                | 370-CS2-1FPE | 18 | 2 |   | 1 |   | 2 |    |
| 16  | Zarządzanie ryzykiem                                                                                                                                    | 370-CS2-1ZAR | 18 | 2 |   | 1 |   | 2 |    |
| 17  | Charakterystyka współczesnych cyberzagrożeń                                                                                                             | 370-CS2-1CWC | 18 | 2 |   | 1 |   |   |    |
| 18  | Proseminarium                                                                                                                                           | 370-CS2-1PRO | 28 | 6 | 6 | 2 |   | 6 |    |
| 19  | Bezpieczeństwo w prawie i politykach Unii Europejskiej                                                                                                  | 370-CS2-2BPP | 42 | 4 |   | 3 |   | 4 |    |
| 20  | Aspekty prawne zatrudnienia w erze cyfrowej                                                                                                             | 370-CS2-2APZ | 42 | 4 |   | 3 |   | 4 |    |
| 21  | Zrównoważony rozwój w zarządzaniu dobrami własności intelektualnej                                                                                      | 370-CS2-2ZRZ | 18 | 2 |   | 1 |   | 2 |    |
| 22  | Odpowiedzialność prawna za szkody wyrządzone przez sztuczną inteligencję                                                                                | 370-CS2-2OPS | 42 | 4 |   | 3 |   | 4 |    |
| 23  | Prawo bankowe lub                                                                                                                                       | 370-CS2-2PBA | 18 | 2 | 2 | 1 |   | 2 |    |
| 23a | Prawo papierów wartościowych (Securities Law)** (przedmiot oferowany także w j. angielskim)                                                             | 370-CS2-2PPW |    |   |   |   |   |   |    |
| 24  | Prawo własności intelektualnej w mediach społecznościowych lub                                                                                          | 370-CS2-2PMS | 18 | 2 | 2 | 1 |   | 2 |    |
| 24a | Ochrona danych osobowych w mediach społecznościowych                                                                                                    | 370-CS2-2ODO |    |   |   |   |   |   |    |
| 25  | Design thinking                                                                                                                                         | 370-CS2-2DET | 18 | 2 |   | 1 |   | 2 |    |
| 26  | Zarządzanie zmianą                                                                                                                                      | 370-CS2-2ZAZ | 18 | 2 |   | 1 |   | 2 |    |
| 27  | Prewencja i reagowanie na incydenty, a cyberbezpieczeństwo                                                                                              | 370-CS2-2PRI | 18 | 2 |   | 1 |   |   |    |
| 28  | Specjalistyczne warsztaty językowe (w jęz. obcym)                                                                                                       | 370-CS2-2SWJ | 30 | 2 |   | 1 |   | 2 |    |
| 29  | Bezpieczeństwo danych osobowych                                                                                                                         | 370-CS2-2BDO | 42 | 4 |   | 3 |   | 4 |    |
| 30  | Zarządzanie zgodnością (compliance) a prawo pracy                                                                                                       | 370-CS2-2ZZP | 42 | 4 |   | 3 |   | 4 |    |
| 31  | Zgłaszanie naruszeń prawa i ochrona sygnalistów                                                                                                         | 370-CS2-2ZNP | 18 | 2 |   | 1 |   | 2 |    |
| 32  | Praktyczne aspekty skutecznego wdrażania i zarządzania wewnętrznym systemem zgłaszania nieprawidłowości                                                 | 370-CS2-2PAS | 42 | 4 |   | 3 |   | 4 |    |
| 33  | Zarządzanie własnością intelektualną dla celów bezpieczeństwa publicznego lub                                                                           | 370-CS2-2ZWI | 18 | 2 | 2 | 1 |   | 2 |    |
| 33a | Znaki towarowe, wzory i wynalazki w erze cyfrowej jako składniki w majątku przedsiębiorców                                                              | 370-CS2-2ZTW |    |   |   |   |   |   |    |
| 34  | Zarządzanie projektami lub                                                                                                                              | 370-CS2-2ZPR | 18 | 3 | 3 | 1 |   | 3 |    |
| 34a | Zarządzanie konfliktem i kryzysem w organizacji                                                                                                         | 370-CS2-2ZKK |    |   |   |   |   |   |    |

| 1             | 2                                                                      | 3            | 4          | 5          | 6         | 7         | 8        | 9         | 10       |
|---------------|------------------------------------------------------------------------|--------------|------------|------------|-----------|-----------|----------|-----------|----------|
| 35            | Cyberbezpieczeństwo w procesie wytwarzania i utrzymania oprogramowania | 370-CS2-2CWO | 18         | 2          |           | 1         |          |           |          |
| 36            | Seminarium                                                             | 370-CS2-2SEM | 56         | 8          | 8         | 3         |          | 8         |          |
| <b>OGÓŁEM</b> |                                                                        |              | <b>984</b> | <b>105</b> | <b>33</b> | <b>61</b> | <b>0</b> | <b>99</b> | <b>0</b> |

|                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                      |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| * liczbę punktów ECTS, jaką student musi uzyskać w ramach zajęć z dziedziny nauk humanistycznych lub nauk społecznych, nie mniejszą niż 5 punktów ECTS – w przypadku kierunków studiów przyporządkowanych do dyscyplin w ramach dziedzin innych niż odpowiednio nauki humanistyczne lub nauki społeczne.                                                                            | 0                                                                                                                                                    |
| Procentowy udział liczby punktów ECTS każdej z dyscyplin, do których jest przyporządkowany kierunek studiów, w liczbie punktów ECTS koniecznej do ukończenia studiów, ze wskazaniem dyscypliny wiodącej.                                                                                                                                                                            | nauki prawne - 80,00%,<br>nauki o zarządzaniu i jakości - 10,48%, nauki o bezpieczeństwie - 5,71%,<br>informatyka - 1,90%,<br>językoznawstwo - 1,90% |
| Procentowy udział liczby punktów ECTS w ramach zajęć do wyboru w liczbie punktów ECTS koniecznej do ukończenia studiów, w wymiarze nie mniejszym niż 30% liczby punktów ECTS koniecznej do ukończenia studiów.                                                                                                                                                                      | 31,43                                                                                                                                                |
| Procentowy udział liczby punktów ECTS w ramach zajęć z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia i studentów w liczbie punktów ECTS koniecznej do ukończenia studiów, w wymiarze nie mniejszym niż 50% liczby punktów ECTS koniecznej do ukończenia studiów (dot. studiów stacjonarnych).                                                 | 58,10                                                                                                                                                |
| Dla studiów o profilu ogólnoakademickim – procentowy udział liczby punktów ECTS w ramach zajęć związanych z prowadzoną w uczelni działalnością naukową w dyscyplinie lub dyscyplinach, do których przyporządkowany jest kierunek studiów w liczbie punktów ECTS koniecznej do ukończenia studiów, w wymiarze większym niż 50% liczby punktów ECTS koniecznej do ukończenia studiów. | 94,29                                                                                                                                                |
| Dla studiów o profilu praktycznym – procentowy udział liczby punktów ECTS w ramach zajęć kształtujących umiejętności praktyczne w liczbie punktów ECTS koniecznej do ukończenia studiów, w wymiarze większym niż 50% liczby punktów ECTS koniecznej do ukończenia studiów.                                                                                                          | 0                                                                                                                                                    |

\*\* Powyższe zajęcia student może zaliczyć również poprzez:

1) uczestnictwo w oferowanych przez Uniwersytet w Białymstoku zajęciach, w szczególności:

- a) na kierunkach studiów prowadzonych w językach obcych,
- b) prowadzonych dla studentów programu Erasmus+,
- c) prowadzonych w języku obcym przez profesorów wizytujących,
- d) w formie wykładów gościnnych prowadzonych w języku obcym,
- e) w ramach specjalistycznych szkół prowadzonych w języku obcym,
- f) określonych w programach innych kierunków studiów i prowadzonych w językach obcych,



|   |   |   |   |   |   |   |   |   |    |
|---|---|---|---|---|---|---|---|---|----|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|----|

2) realizację zajęć w języku obcym na innej uczelni w ramach międzynarodowej wymiany studentów, w tym programu Erasmus+ lub w ramach programu MOST.

3. realizację części studiów lub praktyk za granicą w ramach programu Erasmus+ lub zajęć realizowanych w języku obcym w uczelni zagranicznej w ramach międzynarodowych umów o współpracy – w okresie nie krótszym niż 3 miesiące.