PROGRAM STUDIÓW

I. Ogólna charakterystyka studiów

1) Nazwa kierunku studiów:
cyberbezpieczeństwo
Specjalności:
nie dotyczy

2) Poziom studiów:
studia pierwszego stopnia

3) Poziom Polskiej Ramy Kwalifikacji:
szósty

4) Forma studiów:
studia stacjonarne

5) Profil studiów:
ogólnoakademicki

6) Tytuł zawodowy nadawany absolwentom:
inżynier

7) Dziedzina nauki/sztuki oraz dyscyplina naukowa/artystyczna:

Procentowy udział dziedziny i dyscypliny.

Nazwa dziedziny	Nazwa dyscypliny	Procentowy udział punktów ECTS (%)	Dyscyplina wiodąca
Nauki inżynieryjno-techniczne	Informatyka techniczna i telekomunikacja	100%	Tak

8) Klasyfikacja ISCED:
0612 - Projektowanie i administrowanie baz danych i sieci

9) Liczba semestrów:

7

10) Liczba punktów ECTS wymagana do uzyskania kwalifikacji:

210

Liczba punktów ECTS wymagana do uzyskania kwalifikacji.

Przyporządkowanie punktów ECTS	Liczba punktów ECTS	Udział procentowy
W programie studiów do uzyskania kwalifikacji odpowiadającej poziomowi kształcenia.	210	100%
Do zajęć dydaktycznych wymagających bezpośredniego udziału nauczycieli akademickich i studentów.	108,5	51,7%
Zajęciom związanym z prowadzonymi badaniami naukowymi w dziedzinie/dziedzinach nauki właściwej / właściwych dla ocenianego kierunku studiów, służące zdobywaniu przez studenta pogłębionej wiedzy oraz umiejętności prowadzenia badań naukowych.	150	71,4%
Zajęciom z obszarów nauk humanistycznych lub nauk społecznych (w przypadku kierunków studiów przypisanych do obszarów innych niż odpowiednio nauki humanistyczne lub nauki społeczne).	8	
Przedmiotom obieralnym (zajęciom do wyboru).	75	35,7%
Praktykom zawodowym (jeżeli program studiów przewiduje praktyki).	6	
Z wykorzystaniem metod i technik kształcenia na odległość.	0	0%

11) Język kształcenia:

polski

12) Liczba godzin zajęć w programie studiów:

2835 godzin zajęć oraz 160 godzin praktyk

13) Efekty uczenia się:

Efekty uczenia się dla kierunku cyberbezpieczeństwo spełniają wymogi określone w Rozporządzeniu Ministra Nauki i Szkolnictwa Wyższego z dnia 14 listopada 2018 r. w sprawie charakterystyk drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6–8 Polskiej Ramy Kwalifikacji oraz w ustawie o Zintegrowanym Systemie Kwalifikacji z dnia 22 grudnia 2015 r. (Dz. U. 2016 poz. 64).

Na kierunku cyberbezpieczeństwo (studia I stopnia – PRK poziom 6) sformułowano 43 kierunkowych efektów uczenia się, w tym:

- 22 z zakresu wiedzy,
- 16 z zakresu umiejętności,
- 5 z zakresu kompetencji społecznych.

Poniżej przedstawiono tabelę kierunkowych efektów uczenia się dla studiów I stopnia na kierunku cyberbezpieczeństwo. Opracowany program studiów umożliwia skuteczne osiągnięcie efektów uczenia się określonych w ustawie o Zintegrowanym Systemie Kwalifikacji oraz w rozporządzeniu w sprawie charakterystyk drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6–8 Polskiej Ramy Kwalifikacji, w tym również efektów prowadzących do uzyskania kompetencji inżynierskich (punkt 20 Programu Studiów).

W załączniku PS.1 zamieszczono tabelę pokrycia efektów ogólnych charakterystyk drugiego stopnia dla poziomu PRK 6 oraz efektów inżynierskich efektami kierunkowymi. Natomiast w załączniku PS.2 znajduje się matryca pokrycia kierunkowych efektów uczenia się przez poszczególne przedmioty.

Tabela kierunkowych efektów uczenia się.

Kategoria PRK	Symbol	Kierunkowe efekty uczenia się	Kod składnika opisu
Wiedza: absolwent zna i rozumie	K1_W01	Ma rozszerzoną i pogłębioną wiedzę z zakresu algebry liniowej, analizy matematycznej, matematyki dyskretnej, probabilistyki i statystki niezbędną do opisu i analizy działania elementów i układów właściwych dla kierunku studiów	P6S_WG
	K1_W02	Ma zaawansowaną wiedzę z fizyki niezbędną do zrozumienia podstawowych zjawisk fizycznych występujących w elementach i układach elektronicznych oraz systemach komunikacyjnych	P6S_WG
	K1_W03	Posiada słownictwo ogólne języka obcego na poziomie B2 według ESOKJ oraz specjalistyczne słownictwo dotyczące wybranych obszarów informatyki i sztucznej inteligencji.	P6S_WG
	K1_W04	Zna kluczowe struktury gramatyczne potrzebne do opisywania i tłumaczenia zjawisk i procesów związanych ze studiowanym kierunkiem.	P6S_WG
	K1_W05	Ma zaawansowaną wiedzę w zakresie złożonych struktur danych; zna zasady administrowania danymi i związanymi z nimi standardami; zna zasady cyberbezpieczeństwa i prywatności wykorzystywane do zarządzania ryzykiem związanym z wykorzystywaniem, przetwarzaniem, przechowywaniem i przesyłaniem informacji lub danych	P6S_WG
	K1_W06	Ma zaawansowaną wiedzę w zakresie zasad tworzenia programów komputerowych, struktur języków programowania, ich poziomów oraz używanych algorytmów; ma zaawansowaną wiedzę z zakresu inżynierii oprogramowania;	P6S_WG
	K1_W07	Ma pogłębioną i wiedzę na temat typów i architektur sieci komputerowych oraz zasad ich projektowania, konfigurowania i utrzymania; zna i rozumie wykorzystywane w nich protokoły, algorytmy oraz mechanizmy.	P6S_WG
	K1_W08	Ma szczegółową wiedzę na temat budowy elektronicznych układów cyfrowych, w tym układów programowalnych; ma pogłębioną znajomość budowy komputerów oraz ich komponentów; zna i rozumie zachodzące w nich zjawiska oraz wykorzystywane mechanizmy	P6S_WG
	K1_W09	Ma pogłębioną wiedzę na temat cyklu życia, projektowania oraz eksploatacji odpornych na ataki programowych systemów informatycznych; zna i rozumie zasady ich działania; zna narzędzia wykorzystywanych do identyfikacji luk w oprogramowaniu komunikacyjnym; zna wpływ konfiguracji oprogramowania na bezpieczeństwo;	P6S_WG
	K1_W10	Rozumie pojęcie ataku sieciowego oraz jego powiązanie zarówno z zagrożeniami, jak i lukami w zabezpieczeniach; zna techniki wykrywania włamań do elementów infrastruktury sieciowej; Ma pogłębioną wiedzę na temat wektorów ataku na infrastrukturę sieciową oraz metod analizy ruchu sieciowego w celu wykrycia naruszeń bezpieczeństwa sieci; dysponuje zaawansowaną wiedzę w zakresie zabezpieczeń sieciowych	P6S_WG
	K1_W11	Ma pogłębioną wiedzę na temat projektowania, konfigurowania oraz utrzymania systemów komputerowych, w tym systemów rozproszonych; zna i rozumie wykorzystywane w nich mechanizmy	P6S_WG
	K1_W12	Ma pogłębioną wiedzę w zakresie uwierzytelniania, autoryzacji i zasad sterowania dostępem do systemów komputerowych; jest	P6S_WG

		świadom konieczności stosowania polityk sterowania dostępem oraz ich adaptacji do poziomu ryzyka; zna zasady uwierzytelniania biometrycznego;	
	K1_W13	Zna zasady ukrywania danych, tj. kryptografię i steganografię; ma zaawansowaną wiedzę z zakresu kryptografii, algorytmów kryptograficznych i ich ograniczeń oraz ich znaczenia dla cyberbezpieczeństwa; ma poszerzoną wiedzę w zakresie kompresji danych	P6S_WG
	K1_W14	Ma ogólną wiedzę na temat kluczowych zagadnień przetwarzania rozproszonego oraz zaawansowaną wiedzę szczegółową dotyczącą zagadnień przetwarzania chmurowego dostępnego na rynku; zna modele usług chmurowych oraz koncepcje związane z ich bezpieczeństwem, zarządzaniem, zamówieniami i administracją; zna ekonomiczne, prawne i inne uwarunkowania działalności firm świadczących usługi chmurowe.	P6S_WG
	K1_W15	Ma wiedzę na temat zasad, wymagań i procedur związanych z bezpieczeństwem łańcucha dostaw technologii informatycznych oraz zarządzania ryzykiem w łańcuchu dostaw; jest świadomy konieczności stosowania przepisów, polityk, procedur kluczowych dla cyberbezpieczeństwa infrastruktury krytycznej; zna procesy zarządzania ryzykiem, w tym metody jego oceny i ograniczania;.	P6S_WG
	K1_W16	Ma podstawową wiedzę na temat systemów maszynowego uczenia się i sztucznych sieci neuronowych; uporządkowaną wiedzę dotyczącą zasad oraz metod rozwiązywania problemów decyzyjnych i optymalizacyjnych, w tym algorytmów heurystycznych i nieheurystycznych do przeszukiwania przestrzeni stanów, również z uwzględnieniem ograniczeń zasobowych; zna metody sztucznej inteligencji stosowane w zagadnieniach związanych z cyberbezpieczeństwem.	P6S_WG
	K1_W17	Ma pogłębioną wiedzę na temat do przepisów prawa, regulacji, zasad i norm etycznych w zakresie cyberbezpieczeństwa i prywatności; jest świadom skutków operacyjnych naruszeń cyberbezpieczeństwa; ma również dogłębną znajomość zasad ochrony prywatności oraz wymagań organizacyjnych (obejmujących poufność, integralność, dostępność, uwierzytelnianie i niezaprzeczalność);	P6S_WG
	K1_W18	Zna i rozumie zagrożenia, na które narażona jest współczesna cywilizacji masowo wykorzystująca usługi cyfrowe; orientuje się w najnowszych trendach rozwojowych związanych ze studiowanym kierunkiem	P6S_WK
	K1_W19	Ma podstawową wiedzę dotyczącą zarządzania projektami informatycznymi i teleinformatycznymi	P6S_WK
	K1_W20	Ma podstawową wiedzę dotyczącą tworzenia, zarządzania i prowadzenia oraz rozwoju działalności gospodarczej związanej z nadaną kwalifikacją;	P6S_WK
	K1_W21	Ma podstawową wiedzę niezbędną do zrozumienia społecznych, etycznych, ekonomicznych, ekologicznych, prawnych i innych pozatechnicznych uwarunkowań działalności inżynierskiej	P6S_WK
	K1_W22	Ma podstawową wiedzę w zakresie patentów oraz stosowania prawa autorskiego, ustawy o ochronie danych osobowych oraz własności przemysłowej i intelektualnej	P6S_WK
Umiejętności: absolwent potrafi	K1_U01	Potrafi korzystać ze źródeł literaturowych, integrować pozyskane informacje, oceniać je oraz dokonywać ich interpretacji i wyciągać wnioski, w celu rozwiązania złożonych i nietypowych problemów w obszarze cyberbezpieczeństwa	P6S_UW

	K1_U02	Potrafi korzystać z odpowiednio dobranych metod i narzędzi, w tym zaawansowanych technik informacyjno-komunikacyjnych; umie również opracować proste aplikacje lub skonfigurować podstawowy system w celu przeprowadzenia symulacji, analizy oraz projektowania systemów lub aplikacji zgodnych z profilem kierunku studiów	P6S_UW
	K1_U03	Potrafi zaplanować i przeprowadzić testy oprogramowania oraz systemów i sieci komputerowych w celu wykrycia w nich podatności na ataki; potrafi zaproponować rozwiązania poprawiające bezpieczeństwo działania	P6S_UW
	K1_U04	Potrafi zaplanować i przeprowadzić symulacje komputerowe i pomiary, w tym symulacje i pomiary dotyczące działania systemów teleinformatycznych, potrafi przedstawić otrzymane wyniki w formie liczbowej i graficznej, dokonać ich interpretacji i wyciągnąć właściwe wnioski	P6S_UW
	K1_U05	Przy formułowaniu i rozwiązaniu zadań inżynierskich z zakresu cyberbezpieczeństwa potrafi wykorzystać znane modele matematyczne i algorytmy oraz metody symulacyjne, eksperymentalne i analityczne	P6S_UW
	K1_U06	Przy formułowaniu zadań inżynierskich potrafi dokonać wstępnej oceny ekonomicznej zaprojektowania, implementacji, konfiguracji i utrzymania oprogramowania i systemów spełniających wymogi cyberbezpieczeństwa i zachowania prywatności	P6S_UW
	K1_U07	Potrafi, przy formułowaniu i rozwiązywaniu zadań dotyczących cyberbezpieczeństwa, dostrzegać ich aspekty systemowe i pozatechniczne, w tym etyczne, ekonomiczne i prawne	P6S_UW
	K1_U08	Potrafi dokonać porównania różnych rozwiązań technicznych, ocenić je ze względu na wybrane kryteria użytkowe, ekonomiczne, ekologiczne, prawne oraz etyczne	P6S_UW
	K1_U09	Potrafi, z wykorzystaniem odpowiednio dobranych metod oraz narzędzi, dokonać krytycznej analizy i oceny funkcjonowania istniejących rozwiązań stosowanych w oprogramowaniu, przetwarzaniu danych oraz systemach i sieciach komputerowych	P6S_UW
	K1_U10	Na podstawie dostępnej dokumentacji i specyfikacji oraz standardów potrafi zaprojektować i zaimplementować w językach wysokiego poziomu bezpieczną aplikację internetową lub mobilną	
	K1_U11	Na podstawie dokumentacji technicznej, obowiązujących standardów, przy użyciu właściwych metod, narzędzi i elementów, potrafi zbudować, skonfigurować i uruchomić typowy system lub sieć komputerową spełniające wymogi cyberbezpieczeństwa	P6S_UW
	K1_U12	Potrafi przygotować i przedstawić prezentację w języku polskim i obcym na temat zadania związanego z kierunkiem studiów, komunikuje się z użyciem specjalistycznej terminologii, przedstawia i uzasadnia różne opinie i stanowiska	P6S_UK
	K1_U13	Potrafi przygotować i ustnie przedstawić w języku polskim i obcym zwarte opracowanie o aktualnych problemach cyberbezpieczeństwa; umie prowadzić dyskusję popularyzującą zagadnienia związane z kierunkiem studiów, a swoje poglądy popierać wiedzą inżynierską	P6S_UK
	K1_U14	Ma umiejętności w zakresie języka obcego na poziomie B2 Europejskiego Systemu Opisu Kształcenia Językowego, a także umie czytać ze zrozumieniem karty katalogowe, normy, dokumentacje techniczne oraz instrukcje obsługi układów i urządzeń właściwych dla kierunku studiów	P6S_UK

	K1_U15	Potrafi planować oraz organizować pracę indywidualną i w zespole (w tym opracować i zrealizować harmonogram prac zapewniający dotrzymanie terminu), stosuje zasady bezpieczeństwa i higieny pracy, a także umie pracować w zespołach o charakterze interdyscyplinarnym i wielokulturowym	P6S_UO
	K1_U16	Potrafi samodzielnie planować i realizować własne uczenie się przez całe życie (np. studia drugiego i trzeciego stopnia, studia podyplomowe, kursy prowadzane przez firmy i organizacje zawodowe) w celu podnoszenia kompetencji zawodowych i społecznych	P6S_UU
Kompetencje: absolwent jest gotów do	K1_K01	Rozumie znaczenie podnoszenia kompetencji zawodowych, osobistych i społecznych; ma świadomość, że wiedza i umiejętności w obszarze cyberbezpieczeństwa szybko ewoluują	P6U-KK
	K1_K02	Rozumie znaczenie wiedzy w rozwiązywaniu problemów z zakresu cyberbezpieczeństwa; jest świadomy konieczności wykorzystania wiedzy ekspertów podczas rozwiązywania zadań inżynierskich w zakresie wykraczającym poza własne kompetencje	P6U-KK
	K1_K03	Jest świadomy społecznej roli absolwenta uczelni technicznej, w szczególności rozumie potrzebę formułowania i przekazywania społeczeństwu informacji na temat cyberbezpieczeństwa, w tym jego pozytywnych i negatywnych aspektów, informacji oraz opinii dotyczących działalności inżynierskiej, osiągnięć techniki, a także dorobku i tradycji zawodu informatyka, a także jest gotowy do działania na rzecz interesu publicznego	P6U-KO
	K1_K04	Potrafi myśleć i działać w sposób przedsiębiorczy w obszarze cyberbezpieczeństwa	P6U-KO
	K1_K05	Ma świadomość znaczenia pracy własnej i konieczności przestrzegania zasad etyki zawodowej, jest gotowy do podporządkowania się zasadom pracy w zespole i ponoszenia odpowiedzialności za wspólnie realizowane zadania, a także dbałości o dorobek i tradycje zawodu	P6U-KR

Jako kluczowe efekty uczenia się uznano:

- w zakresie wiedzy:
    - K1_W05 - Ma zaawansowaną wiedzę w zakresie złożonych struktur danych; zna podstawy teorii, zna zasady administrowania danymi i związanymi z nimi standardami; zna zasady cyberbezpieczeństwa i prywatności wykorzystywane do zarządzania ryzykiem związanym z wykorzystywaniem, przetwarzaniem, przechowywaniem i przesyłaniem informacji lub danych;
    - K1_W07 - Ma pogłębioną i wiedzę na temat typów i architektur sieci komputerowych oraz zasad ich projektowania, konfigurowania i utrzymania; zna i rozumie wykorzystywane w nich protokoły, algorytmy oraz mechanizmy;
    - K1_W09 - Ma pogłębioną wiedzę na temat cyklu życia, projektowania oraz eksploatacji odpornych na ataki programowych systemów informatycznych; zna i rozumie zasady ich działania; zna narzędzia wykorzystywanych do identyfikacji luk w oprogramowaniu komunikacyjnym; zna wpływ konfiguracji oprogramowania na bezpieczeństwo;
    - K1_W010 - Ma pogłębioną wiedzę na temat cyklu życia, projektowania oraz eksploatacji odpornych na ataki programowych systemów informatycznych; zna i rozumie zasady ich działania; zna narzędzia wykorzystywanych do identyfikacji luk w oprogramowaniu komunikacyjnym; zna wpływ konfiguracji oprogramowania na bezpieczeństwo;
- w zakresie umiejętności
    - K1_U01 - Potrafi korzystać ze źródeł literaturowych, integrować pozyskane informacje,

oceniać je oraz dokonywać ich interpretacji i wyciągać wnioski, w celu rozwiązania złożonych i nietypowych problemów w obszarze cyberbezpieczeństwa;
    - K1_U02 - Potrafi, z wykorzystaniem odpowiednio dobranych metod oraz narzędzi, dokonać krytycznej analizy i oceny funkcjonowania istniejących rozwiązań stosowanych w oprogramowaniu, przetwarzaniu danych oraz systemach i sieciach komputerowych;
    - K1_U10 - Potrafi zaplanować i przeprowadzić symulacje komputerowe i pomiary, w tym symulacje i pomiary dotyczące działania systemów teleinformatycznych, potrafi przedstawić otrzymane wyniki w formie liczbowej i graficznej, dokonać ich interpretacji i wyciągnąć właściwe wnioski;
    - K1_U09 - Potrafi, z wykorzystaniem odpowiednio dobranych metod oraz narzędzi, dokonać krytycznej analizy i oceny funkcjonowania istniejących rozwiązań stosowanych w oprogramowaniu, przetwarzaniu danych oraz systemach i sieciach komputerowych;
- w zakresie kompetencji społecznych:
    - K1_K01 - Rozumie znaczenie podnoszenia kompetencji zawodowych, osobistych i społecznych; ma świadomość, że wiedza i umiejętności w obszarze cyberbezpieczeństwa szybko ewoluują;
    - K1_K05 - Ma świadomość znaczenia pracy własnej i konieczności przestrzegania zasad etyki zawodowej, jest gotowy do podporządkowania się zasadom pracy w zespole i ponoszenia odpowiedzialności za wspólnie realizowane zadania, a także dbałości o dorobek i tradycje zawodu.

14) Sposoby weryfikacji i oceny efektów uczenia się:

Ogólne zasady sprawdzania i oceniania stopnia osiągnięcia efektów uczenia się opisano szczegółowo w Regulaminie studiów pierwszego i drugiego stopnia (Uchwała Senatu Akademickiego Politechniki Poznańskiej Nr 42/2020-2024 z dnia 31 maja 2021). System weryfikacji efektów uczenia się jest kompleksowy i uwzględnia zasady zaliczeń oraz egzaminów w terminach podstawowych i poprawkowych dla odpowiednich form zajęć. Szczegółowy opis metod weryfikacji efektów uczenia się dla poszczególnych przedmiotów znajduje się w kartach opisu przedmiotów. Program zajęć, zasady oceny i zaliczenia przedmiotu oraz godziny konsultacji są podawane w trakcie pierwszego spotkania studentów z prowadzącym

Zgodnie z jego zapisami poszczególnym modułom zajęć przyporządkowana jest odpowiednia liczba punktów ECTS, która podana jest w karcie ECTS modułu. Liczba punktów przyporządkowana modułom w każdym semestrze wynosi 30. Dla uzyskania dyplomu ukończenia studiów na studiach stacjonarnych konieczne jest, poza spełnieniem wymagań programowych, zdobycie wymaganej w programie kształcenia liczby punktów ECTS.

Okresem rozliczeniowym jest semestr. Warunkiem zaliczenia semestru jest uzyskanie oceny co najmniej dostatecznej ze wszystkich zajęć przewidzianych w programie studiów oraz zaliczenie praktyk, zajęć z wychowania fizycznego i wymaganych szkoleń. Oceny semestralne z egzaminów, zaliczeń ćwiczeń, laboratoriów i projektów są wpisywane do arkusza w systemie elektronicznym USOS, zgodnie z obowiązującym zarządzeniem uczelnianym w przedmiotowej sprawie.

W przypadku, gdy student nie zaliczył wszystkich zajęć przewidzianych w danym semestrze, może zostać warunkowo wpisany na kolejny semestr, jeśli łączna liczba punktów ECTS przypisanych do niezaliczonych zajęć nie przekracza 14, a opóźnienie nie jest większe niż dwa semestry. Przy spełnieniu wymienionych warunków, decyzję o warunkowym zezwoleniu na kontynuowanie studiów może podjąć Dziekan Wydziału Informatyki i Telekomunikacji. Możliwe jest również podjęcie takiej decyzji przez Rektora Politechniki Poznańskiej, przy czym w tym przypadku nie muszą zostać spełnione wymienione warunki.

Do weryfikacji efektów uczenia się stosowane jest szerokie spektrum metod, które umożliwiają ich skuteczne sprawdzenie i ocenę zarówno w zakresie wiedzy, umiejętności i kompetencji

społecznych. Opracowany system sprawdzania i oceniania zapewnia przejrzystość, wiarygodność oceniania oraz daje możliwość porównywania wyników.

Sprawdzanie i ocenianie stopnia osiąganych efektów uczenia się przez studentów odbywa się zarówno na etapie procesu kształcenia, np. podczas:

- różnych form prac etapowych – egzaminy, kolokwia, projekty, referaty czy sprawdziany wejściowe,
- zaliczania praktyk studenckich,
- oceny prac dyplomowych,

jak również po zakończeniu procesu kształcenia, np. poprzez:

- ocenę pracodawców,
- monitorowanie losów absolwentów,
- ocenę rynku pracy.

Metody sprawdzania efektów uczenia się są dostosowane do rodzaju oraz formy prowadzonych zajęć dydaktycznych lecz zazwyczaj realizowane są następująco:

- wykłady – egzamin lub kolokwium zaliczeniowe,
- ćwiczenia audytoryjne – kolokwium,
- ćwiczenia laboratoryjne – sprawdziany wejściowe oraz sprawozdania,
- zajęcia projektowe – obrona zadania/projektu (etapowa i/lub końcowa).

W celu weryfikowania umiejętności inżynierskich stosuje się dodatkowo prezentację przygotowanych projektów. Zasady formalne przygotowania i oceniania projektów określa prowadzący i są one różne w zależności od typu przedmiotu, np. w przypadku tematów o charakterze podstawowym opis jest zwięzły, natomiast w przypadku przedmiotów o charakterze badawczym zakres projektu daje studentom możliwość odniesienia się do nowych pozycji literaturowych oraz analizy zagadnienia. Tematyka prac etapowych, egzaminacyjnych oraz projektowych jest ściśle związana z tematyką poszczególnych modułów.

Pracownicy dokumentują testy, kolokwia, egzaminy oraz projekty i inne prace, np. sprawozdania z realizacji zajęć (zgodnie z Wydziałowym Systemem Zapewnienia Jakości Kształcenia - WSZJK). Egzaminy i kolokwia ustne są dokumentowane w postaci krótkich notatek.

Na podstawie ocen formujących wyznaczana jest ocena podsumowująca wpisywana do obowiązującego systemu elektronicznego.

Wszystkie oceny muszą być wpisane do systemu elektronicznego. Uzyskanie oceny dostatecznej przez studenta jest równoznaczne z osiągnięciem przez niego w stopniu wystarczającym wszystkich wymaganych w danym module efektów uczenia się. Tabela poniżej zawiera wykorzystywaną skalę ocen.

Skala ocen używana w Uczelni

Ocena słowna	Symbol literowy	Ocena liczbowa
Bardzo dobry	A	5,0
Dobry plus	B	4,5
Dobry	C	4,0
Dostateczny plus	D	3,5
Dostateczny	E	3,0
Niedostateczny	F	2,0

Studentowi, który w wyniku bieżącej kontroli stopnia uzyskania efektów uczenia się otrzymał z zaliczenia lub egzaminu ocenę niedostateczną, przysługuje prawo do jednego zaliczenia lub egzaminu poprawkowego w danym semestrze.

Wielu nauczycieli akademickich daje studentom możliwość indywidualnego wykazania się podczas zajęć, promując ich aktywność oraz oceniając wypowiedzi i merytoryczny udział w dyskusjach. Na licznych przedmiotach studenci mogą poszerzać swoją wiedzę i umiejętności, biorąc udział w badaniach naukowych związanych z tematyką zajęć. W ramach wybranych kursów, takich jak seminaria, studenci mają również okazję przygotowywać prezentacje i prowadzić dyskusje, które są oceniane przez prowadzących.

Takie formy zajęć pozwalają na ocenę nie tylko efektów związanych z wiedzą i umiejętnościami, ale także stopnia nabycia kompetencji społecznych. Dodatkowo zwiększają atrakcyjność przekazywanej wiedzy, umożliwiają studentom zapoznanie się z narzędziami multimedialnymi oraz rozwijanie umiejętności interpersonalnych, takich jak autoprezentacja – kluczowy element kompetencji, na który często zwracają uwagę przedstawiciele przemysłu.

Zajęcia obejmujące pracę w grupach, na przykład laboratoryjne i projektowe, pozwalają również na ocenę kompetencji społecznych, takich jak umiejętność pracy w zespole, prowadzenie konstruktywnych dyskusji, uzasadnianie własnych stanowisk oraz krytyczna ocena argumentów.

Ostateczną metodą sprawdzenia nabytych w ramach pełnego cyklu kształcenia efektów uczenia się jest przygotowanie pracy dyplomowej. Proces dyplomowania określony został szczegółowo w Regulaminie Studiów. Wybór tematów prac dyplomowych, wybór opiekunów i recenzentów oraz przeprowadzenie egzaminów dyplomowych przebiegają pod nadzorem Dziekana i Komisji Zatwierdzającej Tematy Prac Dyplomowych w oparciu o zasady przyjęte w ramach całego Wydziału.

Warunkiem dopuszczenia do egzaminu dyplomowego jest spełnienie wszystkich wymagań stawianych w tym zakresie studentom Politechniki Poznańskiej. W szczególności należy zwrócić uwagę na:

- uzyskanie liczby punktów ECTS potwierdzających osiągnięcie wszystkich efektów przewidzianych w programie kształcenia oraz zaliczenie wszystkich wymaganych szkoleń,
- złożenie pracy dyplomowej w wersji elektronicznej (wersja edytowalna w pliku z rozszerzeniem doc, docx, odt, rtf, tex oraz nieedytowalna w pliku z rozszerzeniem pdf) do uczelnianego repozytorium pisemnych prac dyplomowych za pomocą systemu dostępnego dla studentów; wgrana praca automatycznie zostaje wysłana do sprawdzenia do Jednolitego Systemu Antyplagiatowego (JSA).
- pozytywną opinię o pracy dyplomowej promotora i co najmniej jednego recenzenta; W przypadku negatywnej oceny recenzenta pracy, decyzję o dopuszczeniu studenta do egzaminu dyplomowego podejmuje dziekan, po zasięgnięciu opinii dodatkowego recenzenta.
- złożenie kompletu dokumentów przed planowaną datą obrony,
- uzyskanie pozytywnego wyniku weryfikacji pracy w systemie JSA.

Procedura dyplomowania zawiera ocenę i końcowe potwierdzenie wiedzy, umiejętności oraz kompetencji społecznych.

W trakcie egzaminów dyplomowych komisje oceniają wiedzę, umiejętności i kompetencje społeczne studentów nabyte w trakcie realizacji programu studiów. Wiedza jest potwierdzona poprzez:

- opracowanie pracy dyplomowej (części teoretycznej i praktycznej);
- zdanie egzaminu dyplomowego w formie odpowiedzi na co najmniej trzy pytania z listy zagadnień egzaminacyjnych udostępnionej na stronie internetowej Wydziału

(https://cat.put.poznan.pl/ – strona główna; ścieżka nawigacji do odpowiedniej podstrony: Home/Listy zagadnień egzaminacyjnych: https://cat.put.poznan.pl/zagadnienia-na-egzamin-dyplomowy); listy zagadnień egzaminacyjnych prezentowane są w powiązaniu z weryfikowanymi efektami uczenia się.
- oceny z wykładów z przedmiotów zaliczonych w toku studiów.

Umiejętności są potwierdzone poprzez:
- opracowanie pracy dyplomowej (części praktycznej),
- oceny z ćwiczeń, laboratoriów i projektów z przedmiotów zaliczonych w toku studiów.

Kompetencje społeczne są potwierdzone poprzez:
- opracowanie pracy dyplomowej (w przypadku prac zespołowych),
- prezentację i obronę pracy w trakcie egzaminu dyplomowego,
- oceny z ćwiczeń i projektów z przedmiotów zaliczonych w toku studiów.

Przewodniczącym komisji egzaminu dyplomowego musi być osoba posiadająca tytuł profesora lub stopień doktora habilitowanego. Egzamin dyplomowy składa się z prezentacji pracy dyplomowej, dyskusji nad pracą oraz sprawdzenia wiedzy i umiejętności z programu studiów. Przebieg egzaminów dyplomowych i obron prac dyplomowych jest określony w Regulaminie Studiów. Egzamin dyplomowy jest zdany, gdy pozytywna jest ocena za obronę pracy dyplomowej i większość pozostałych ocen cząstkowych.

Ostateczny wynik studiów ustala komisja egzaminu dyplomowego, obliczając go na podstawie wzoru:

$$W_{st} = 0{,}6 \cdot P_{ś} + 0{,}2 \cdot P_{dyp} + 0{,}2 \cdot E_{dyp}$$

gdzie:

$P_{ś}$ – średnia ważona ocen z zajęć z przebiegu studiów (ocenę z zajęć stanowi średnia arytmetyczna wszystkich ocen z każdej formy prowadzonych zajęć),
P_{dyp} – ocena pracy dyplomowej,
E_{dyp} – ocena z egzaminu dyplomowego.

Ukończenie studiów następuje po złożeniu egzaminu dyplomowego z wynikiem pozytywnym. Absolwent uzyskuje dyplom ukończenia studiów drugiego stopnia wraz z suplementem do dyplomu oraz tytuł zawodowy magistra inżyniera.

15) Praktyki zawodowe:

Na kierunku cyberbezpieczeństwo praktyki zawodowe stanowią integralną część programu studiów i podlegają zaliczeniu. Zgodnie z harmonogramem studiów studenci odbywają praktykę w wymiarze 4 tygodni (160 h – 120 godz. zegarowych) w przerwie wakacyjnej po semestrze VI (6 punkty ECTS).

Podstawowymi celami praktyk studenckich są:
- rozwijanie dotychczas zdobytych umiejętności w rzeczywistych warunkach funkcjonowania firm,
- przygotowanie studenta do samodzielności i odpowiedzialności za powierzone mu zadania,
- rozwijanie kompetencji związanych z pracą zespołową oraz umiejętnością podejmowania decyzji,
- poznanie zakresu obowiązków i techniki pracy specjalistów na różnych stanowiskach, poznanie organizacji i metod funkcjonowania przykładowych przedsiębiorstw związanych z obszarem cyberbezpieczeństwa,

- pozyskiwanie kontaktów zawodowych pomocnych w okresie poszukiwania pracy po zakończeniu studiów.

Za organizację i nadzorowanie praktyk studenckich odpowiedzialny jest:
- na poziomie wydziału – koordynator praktyk ustanowiony przez dziekana spośród nauczycieli akademickich,
- na poziomie kierunku studiów – kierunkowy opiekun praktyk ustanowiony przez dziekana spośród nauczycieli akademickich prowadzących zajęcia na tym kierunku.
- na poziomie Przedsiębiorstwa – opiekun praktyk ze strony przedsiębiorstwa ustanowiony przez osobę decyzyjną w Przedsiębiorstwie.

Do zadań kierunkowego opiekuna praktyk należy w szczególności:
- przygotowanie harmonogramu praktyk studenckich,
- przedstawienie studentom programu praktyki, a także terminów realizacji oraz terminów i warunków zaliczenia praktyki,
- opiniowanie wyboru określonej praktyki przez studenta,
- nadzór merytoryczny nad pracą opiekunów praktyk,
- współpraca z opiekunem praktyk ze strony Przedsiębiorstwa w sprawach związanych z organizacją i przebiegiem praktyki,
- podejmowanie decyzji w sprawie zaliczenia praktyki i wprowadzenie jej do systemu informatycznego Uczelni.

Wszelkie zagadnienia związane z organizacją, realizacją i zaliczeniem praktyk opisane są w Regulaminie studiów §25 oraz Zarządzenia Nr 11 Rektora PP z dnia 29 marca 2023 r (Załącznik do Zarządzenia)

Na praktyki kieruje studenta Centrum Praktyk i Karier Studentów i Absolwentów Politechniki Poznańskiej (CPiKSiA). Studenci mogą odbywać praktyki również na podstawie: skierowania uzyskanego w organizacjach (w tym studenckich) oferujących praktyki oraz indywidualnego porozumienia zawartego przez studenta z zakładem pracy.

Uczelnia daje również możliwość zaliczenia praktyki studenckiej doświadczenia zawodowego. Warunkiem takiej formy zaliczenia jest:
- zatrudnienie studenta na podstawie umowy w wymiarze czasu, który spełnia wymagania przewidziane dla praktyki określone w programie studiów dla kierunku cyberbezpieczeństwo,
- osiągnięcie przez studenta przedmiotowych efektów uczenia się przewidzianych dla praktyki w wyniku realizacji powierzonych mu obowiązków,
- uzyskania zgody opiekuna praktyk na zaliczenie pracy zawodowej jako praktyki przed jej rozpoczęciem,
- wykonywanie obowiązków przez studenta pod nadzorem przełożonego lub innej osoby, która pełni rolę opiekuna praktyki ze strony Przedsiębiorstwa.

Szczegółowe zasady odbywania praktyk studenckich na Wydziale znajdują się w Regulaminie organizacji praktyk studenckich objętych programem studiów. Wg w/w zasad student, celem zaliczenia praktyki, zobowiązany jest do przedłożenia opiekunowi praktyk:
- *Zaświadczenia o odbyciu praktyk* wystawionego przez Podmiot Zewnętrzny,
- *Dziennika praktyk*, potwierdzonego przez zakładowego opiekuna praktykanta,
- ankiety opisującej efekty uczenia się (ocena odbytej praktyki przez studenta), w której student dokonuje oceny przydatności i satysfakcji z odbytej praktyki,
- przypadku zaliczenia praktyk na podstawie doświadczenia zawodowego student powinien dostarczyć także kopię umowy cywilno-prawnej potwierdzającej doświadczenie zawodowe.

Wpisu zaliczenia praktyki dokonuje opiekun na podstawie weryfikacji przedłożonej dokumentacji i uzyskania przez studenta przypisanych do praktyki efektów uczenia się. Student zaliczający praktykę na podstawie uzyskanego doświadczenia zawodowego zwolniony jest od obowiązku uzyskania podpisu opiekuna praktykanta w dzienniku praktyk.

16) Język obcy:

Na kierunku Cyberbezpieczeństwo język obcy realizowany jest na czterech pierwszych semestrach w łącznym wymiarze 120 godzin (8 pkt ECTS) i kończy się egzaminem na poziomie B2 Europejskiego Systemu Opisu Kształcenia Językowego (Tabela 1.4). Zajęcia w ramach nauki języka obcego prowadzone są przez kadrę wyspecjalizowanej jednostki międzywydziałowej – Centrum Języków i Komunikacji. Oferowanymi językami obcymi są język angielski i język niemiecki.
Studenci umiejętności językowe nabywają również podczas zajęć seminaryjnych (Seminarium Przeddyplomowe, Seminarium Dyplomowe), podczas których studenci bardzo często zapoznają się z anglojęzycznymi źródłami. Także w ramach przedmiotów Kompetencje globalne oraz Prace badawczo-wdrożeniowe studenci uczą się wykorzystywania materiałów anglojęzycznych do rozwiazywania różnorodnych problemów technicznych z zakresu teleinformatyki i informatyki.

Przedmioty uwzględniające efekty uczenia się w zakresie znajomości języka obcego (O – ogółem, W – wykład, C – ćwiczenia, L – laboratorium, P – projekt, ECTS – liczba punktów ECTS).

Sem.	Nazwa przedmiotu	Liczba godzin					Liczba punktów ECTS
		O	W	C	L	P	
1	Język obcy (Język angielski / język niemiecki)	**30**		30			2
2	Język obcy (Język angielski / język niemiecki)	**30**		30			2
3	Język obcy (Język angielski / język niemiecki)	**30**		30			2
4	Język obcy (Język angielski / język niemiecki)	**30**		30			2
Razem		**120**					**8**

17) Zajęcia z wychowania fizycznego:

Na kierunku cyberbezpieczeństwo zajęcia z wychowania fizycznego realizowane są w semestrze 1 i 2 w łącznym wymiarze 60 godzin (0 pkt. ECTS).

Zajęcia z wychowania fizycznego (O – ogółem, W – wykład, C – ćwiczenia, L – laboratorium, P – projekt, ECTS – liczba punktów ECTS).

Sem.	Nazwa przedmiotu	Liczba godzin					Liczba punktów ECTS
		O	W	C	L	P	
1	Wychowanie fizyczne	**30**		30			0
2	Wychowanie fizyczne	**30**		30			0
Razem		**60**					**0**

18) Szkolenia:

Szkolenia (O – ogółem, W – wykład, C – ćwiczenia, L – laboratorium, P – projekt, ECTS – liczba punktów ECTS).

Sem.	Nazwa przedmiotu	Liczba godzin					Liczba punktów ECTS
		O	W	C	L	P	

	Podstawowe szkolenie z zakresu BHP– z zakresu bezpiecznych i higienicznych warunków kształcenia.	**4**	4				0
	Szkolenie biblioteczne – z zakresu korzystania z zasobów bibliotecznych.	**1**		1			0
	Razem	**7**					**0**

19) Przedmioty obieralne (zajęcia do wyboru):

Przedmioty obieralne na kierunku Cyberbezpieczeństwo można podzielić na dwie grupy. Do pierwszej z nich zaliczamy przedmioty obieralne niezależne od profilu, czyli języki obce, przedmioty obieralne w zakresie nauk o bezpieczeństwie, przedmioty obieralne o bezpieczeństwie instytucji i państwa, seminarium przeddyplomowe, seminarium dyplomowe, przygotowanie pracy dyplomowej i praktyki. Drugą grupę stanowią przedmioty obieralne w obrębie profili kształcenia. Określono trzy profile kształcenia: BST – Bezpieczeństwo Sieci Teleinformatycznych, BPD – Bezpieczeństwo Przetwarzania Danych, BKM – Bezpieczeństwo Komunikacji Multimedialnej. W przypadku przedmiotów należących do profili kształcenia przyjmuje się, że studenci wybierają profil kształcenia (a tym samym wszystkie przedmioty wchodzące w jego skład) na czas jednego semestru. W każdym z semestrów zawierających takie przedmioty, tj. semestr 5,6 i 7, studenci dokonują niezależnego wyboru profili. W tabeli Wykaz przedmiotów obieralnych, grypy przedmiotów obieralnych oznaczona nazwą ,,Przedmioty obieralne X.Y", gdzie X oznacza semestr a Y numer kolejny przedmiotu obieralnego. Przedmioty wchodzące w skład przedmiotów obieralnych umieszczono w wierszach poniżej. Każdy taki przedmiot poprzedzony jest numerem semestru oraz symbolem profilu (BKM, BDP, BST). Student decydując się na dany profil wybiera w semestrze wszystkie przedmioty należące do danego profilu. Wybór profilu na semestr 5 i 6 dokonuje się na początku semestru 4, natomiast wyboru profilu na semestr 7 na początku semestru 6.

W ramach każdego z modułów obieralnych, oprócz seminarium dyplomowego, seminarium przeddyplomowego, przygotowania pracy dyplomowej i praktyki, student ma do wyboru co najmniej dwa przedmioty.

Łączna liczba punktów ECTS związanych z przedmiotami obieralnymi wynosi 75, co stanowi 35,7% wszystkich punktów ECTS wymaganych do uzyskania kwalifikacji na poziomie 6 PRK.

Wykaz przedmiotów obieralnych - zajęć do wyboru (O – ogółem, W – wykład, C – ćwiczenia, L – laboratorium, P – projekt, ECTS – liczba punktów ECTS).

Sem.	**Nazwa przedmiotu**	**Liczba godzin**					**Liczba punktów ECTS**
		O	**W**	**C**	**L**	**P**	
1	*Język obcy*	***30***		*30*			*2*
	Język angielski						
	Język niemiecki						
2	*Język obcy*	***30***		*30*			*2*
	Język angielski						
	Język niemiecki						
3	*Język obcy*	***30***		*30*			*2*
	Język angielski						

	Język niemiecki						
3	*Przedmiot obieralny w zakresie nauk o bezpieczeństwie*	***40***	*16*			*24*	*3*
	Kompetencje globalne						
	Krajowe zasoby informacyjne						
4	*Język obcy*	***30***		*30*			*2*
	Język angielski						
	Język niemiecki						
5	Przedmioty obieralne 5,X.1	***56***	*24*	*-*	*16*	*16*	*4*
	5.BST.1 Bezpieczeństwo sieci LAN i WAN						
	5.BPD.1 Synchronizacja						
	5.BKM.1 Synchronizacja						
5	Przedmioty obieralne 5.X.2	***56***	*24*	*-*	*16*	*16*	*4*
	5.BST.2 Bezpieczeństwo systemów IoT i IIoT						
	5.BPD.2 Bezpieczeństwo systemów IoT i IIoT						
	5.BKM.2 Ochrona dostępu w rozproszonych systemach multimedialnych						
5	*Przedmioty obieralne 5.X.3*	***64***	*24*	*-*	*24*	*16*	*5*
	5.BST.3 Sieci definiowane programowo						
	5.BPD.3 Sieci definiowane programowo						
	5.BKM.3 AI w cyberbezpieczeństwie multimediów						
6	Przedmioty obieralne 6.x.1	***58***	*16*	*-*	*30*	*12*	*4*
	6.BST.1 Wykrywanie anomalii sieciowych i detekcja zagrożeń w sieci z wykorzystaniem AI						
	6.BPD.1 Bezpieczeństwo systemów operacyjnych						
	6.BKM.1Techniki deepfake						
6	Przedmioty obieralne 6.x.2	***48***	*24*	*-*	*24*	*-*	*3*
	6.BST.2 Bezpieczeństwo systemów bezprzewodowych						
	6.BPD.2 Bezpieczeństwo funkcjonalne i łańcuchów dostaw						
	6.BKM.2 Techniki ochrony multimediów						
6	Przedmioty obieralne 6.x.3	***54***	*24*	*-*	*24*	*16*	*4*
	6.BST.3 Bezpieczeństwo w systemach chmurowych						
	6.BPD.3 Bezpieczeństwo w systemach chmurowych						
	6.BKM.3 Biometryczne uwierzytelnianie tożsamości						
6	Przedmioty obieralne 6.x.4	***48***	*16*	*-*	*16*	*16*	*3*
	6.BST.4 Podstawy analizy informacji						
	6.BPD.4 Urządzenia programowalne						
	6.BKM.4 Cyberkryminalistyka multimedialna						
6	Seminarium przeddyplomowe	***30***				*30*	*2*
6	Praktyka zawodowa						*6*
7	Przedmioty obieralne 7.X.1	***72***	*24*	*-*	*24*	*24*	*5*
	7.BST.1 Zarządzanie bezpieczeństwem sieci						

	7.BPD.1 Bezpieczeństwo fizyczne systemów i urządzeń IT						
	7.BKM.1 Bezpieczeństwo danych medycznych						
7	Przedmioty obieralne 7.x.2	***54***	*24*	*-*	*-*	*30*	*4*
	7.BSP.2 Bezpieczeństwo systemów bezzałogowych i komunikacji satelitarnej						
	7.BPD.2 Metody i zasady uwierzytelnienia						
	7.BKM.2 Cyberbezpieczeństwo w mediach publicznych i społecznościowych						
7	Przedmioty obieralne 7.x.3	***54***	*16*	*-*	*30*	*12*	*4*
	7.BST.3 Bezpieczeństwo systemów zarządzania bazami danych						
	7.BPD.3 Bezpieczeństwo systemów zarządzania bazami danych						
	7.BKM.3 Automatyzacja konfiguracji, utrzymania i testowania sieci systemów teleinformatycznych						
7	Przedmioty obieralne 7.X.4	***32***	*16*	*-*	*16*	*-*	*2*
	7.BST.4 Systemy komunikacji kwantowej						
	7.BPD.4 Systemy komunikacji kwantowej						
	7.BKM.4 Zarządzanie i ochrona własności intelektualnej w multimediach						
7	Przedmioty obieralne o bezpieczeństwie instytucji i państwa	***32***	*16*	*-*	*-*	*16*	*2*
	Bezpieczeństwo sektora finansowego						
	Bezpieczeństwo wewnętrzne						
7	Przygotowanie pracy dyplomowej	***-***	*-*	*-*	*-*	*-*	*10*
7	Seminarium dyplomowe	***30***	*-*	*-*	*-*	*30*	*2*
	Razem	***848***					***75***

20) Kompetencje inżynierskie:

Wykaz kierunkowych efektów uczenia się umożliwiających uzyskanie kompetencji inżynierskich.

Kategoria PRK	Opis i kod składnika opisu	Kierunkowe efekty uczenia się	Symbol efektu kierunkowego
Wiedza: absolwent zna i rozumie	podstawowe procesy zachodzące w cyklu życia urządzeń, obiektów i systemów technicznych (P6S_WG)	Ma pogłębioną i wiedzę na temat typów i architektur sieci komputerowych oraz zasad ich projektowania, konfigurowania i utrzymania; zna i rozumie wykorzystywane w nich protokoły, algorytmy oraz mechanizmy.	**K1_W07**
		Ma pogłębioną wiedzę na temat cyklu życia, projektowania oraz eksploatacji odpornych na ataki programowych systemów informatycznych; zna i rozumie zasady ich działania; zna narzędzia wykorzystywanych do identyfikacji luk w oprogramowaniu komunikacyjnym; zna wpływ konfiguracji oprogramowania na bezpieczeństwo;	**K1_W09**
		Ma pogłębioną wiedzę na temat projektowania, konfigurowania oraz utrzymania systemów komputerowych, w tym systemów rozproszonych; zna i rozumie wykorzystywane w nich mechanizmy	**K1_W11**
	podstawowe zasady tworzenia i rozwoju	Ma podstawową wiedzę dotyczącą zarządzania projektami informatycznymi i teleinformatycznymi;	**K1_W19**

	różnych form indywidualnej przedsiębiorczości (P6S_WK)	Ma podstawową wiedzę dotyczącą tworzenia, zarządzania i prowadzenia oraz rozwoju działalności gospodarczej związanej z nadaną kwalifikacją;	**K1_W20**
Umiejętności: absolwent potrafi	planować i przeprowadzać eksperymenty, w tym pomiary i symulacje komputerowe, interpretować uzyskane wyniki i wyciągać wnioski (P6S_UW)	Potrafi zaplanować i przeprowadzić testy oprogramowania oraz systemów i sieci komputerowych w celu wykrycia w nich podatności na ataki; potrafi zaproponować rozwiązania poprawiające bezpieczeństwo działania	**K1_U03**
		Potrafi zaplanować i przeprowadzić symulacje komputerowe i pomiary, w tym symulacje i pomiary dotyczące działania systemów teleinformatycznych, potrafi przedstawić otrzymane wyniki w formie liczbowej i graficznej, dokonać ich interpretacji i wyciągnąć właściwe wnioski	**K1_U04**
	przy identyfikacji i formułowaniu specyfikacji zadań inżynierskich oraz ich rozwiązywaniu: − wykorzystać metody analityczne, symulacyjne i eksperymentalne − dostrzegać ich aspekty systemowe i pozatechniczne, w tym aspekty etyczne − dokonać wstępnej oceny ekonomicznej proponowanych rozwiązań i podejmowanych działań inżynierskich (P6S_UW)	Przy formułowaniu i rozwiązaniu zadań inżynierskich z zakresu cyberbezpieczeństwa potrafi wykorzystać znane modele matematyczne i algorytmy oraz metody symulacyjne, eksperymentalne i analityczne	**K1_U05**
		Przy formułowaniu zadań inżynierskich potrafi dokonać wstępnej oceny ekonomicznej zaprojektowania, implementacji, konfiguracji i utrzymania oprogramowania i systemów spełniających wymogi cyberbezpieczeństwa i zachowania prywatności	**K1_U06**
		Potrafi, przy formułowaniu i rozwiązywaniu zadań dotyczących cyberbezpieczeństwa, dostrzegać ich aspekty systemowe i pozatechniczne, w tym etyczne, ekonomiczne i prawne	**K1_U07**
		Potrafi dokonać porównania różnych rozwiązań technicznych, ocenić je ze względu na wybrane kryteria użytkowe, ekonomiczne, ekologiczne, prawne oraz etyczne	**K1_U08**
	dokonać krytycznej analizy sposobu funkcjonowania istniejących rozwiązań technicznych i ocenić te rozwiązania (P6S_UW)	Potrafi, z wykorzystaniem odpowiednio dobranych metod oraz narzędzi, dokonać krytycznej analizy i oceny funkcjonowania istniejących rozwiązań stosowanych w oprogramowaniu, przetwarzaniu danych oraz systemach i sieciach komputerowych	**K1_U09**
	projektować – zgodnie z zadaną specyfikacją – oraz wykonać typowe dla kierunku studiów proste urządzenia, obiekty, systemy lub zrealizować procesy, używając odpowiednio dobranych metod, technik, narzędzi i materiałów (P6S_UW)	Na podstawie dostępnej dokumentacji i specyfikacji oraz standardów potrafi zaprojektować i zaimplementować w językach wysokiego poziomu bezpieczną aplikację internetową lub mobilną	**K1_U10**
		Na podstawie dokumentacji technicznej, obowiązujących standardów, przy użyciu właściwych metod, narzędzi i elementów, potrafi zbudować, skonfigurować i uruchomić typowy system lub sieć komputerową spełniające wymogi cyberbezpieczeństwa	**K1_U11**

21) Zajęcia z dziedziny nauk humanistycznych lub nauk społecznych:
Wykaz przedmiotów z dziedziny nauk humanistycznych lub nauk społecznych
(O – ogółem, W – wykład, C – ćwiczenia, L – laboratorium, P – projekt).

Sem.	Nazwa przedmiotu	O	W	C	L	P	Liczba punktów ECTS
1	Teoria bezpieczeństwa i zarządzanie w sytuacjach kryzysowych	24	24				2
3	Przedmiot obieralny w zakresie nauk o bezpieczeństwie	40	16			24	3
	Kompetencje globalne						
	Krajowe zasoby informacyjne						
6	Zarządzanie incydentami i bezpieczeństwo instytucji	32	16			16	1
7	P.O. o bezpieczeństwie instytucji i państwa	32	16		16		2
	Bezpieczeństwo sektora finansowego						
	Bezpieczeństwo wewnętrzne						
	Razem	**104**					**8**

22) Zajęcia związane z prowadzoną w uczelni działalnością naukową:

Zajęcia związane z prowadzoną w uczelni działalnością naukową.

Nazwa przedmiotu	Liczba punktów ECTS	Udział studentów w zajęciach przygotowujących do prowadzenia działalności naukowej lub udział w tej działalności (TAK/NIE)	Opis działalności naukowej
Wstęp do cyberbezpieczeństwa	4	NIE	Badania efektywności rozwiązań zapewniających bezpieczeństwo sieci teleinformatycznych
Podstawy techniki cyfrowej	4	NIE	Wykorzystanie podstawowych elementów techniki cyfrowej do celów współczesnej informatyki i teleinformatyki
Programowanie skryptowe	3	NIE	Wykorzystanie języków skryptowych i dostępnych bibliotek do rozwiązywania problemów technicznych
Podstawy lokalnych sieci komputerowych	4	NIE	Badanie efektywności protokołów routingu wewnętrznego i usług sieciowych pod względem efektywności lub jakości usług
Architektura komputerów i systemy operacyjne	5	NIE	Wykorzystanie systemów komputerowych i systemów operacyjnych, w tym sieciowych systemów operacyjnych do przygotowania środowisk badawczych z zakresu informatyki i teleinformatyki
Algorytmy i struktury danych	4	NIE	Algorytmy przetwarzania danych w rozwiązaniach informatycznych i teleinformatycznych
Podstawy kryptografii	4	TAK	Projektowanie zarówno komponentów, jak i całych metod kryptograficznych.
Podstawy rozległych sieci komputerowych	4	TAK	Badanie efektywności algorytmów routingu wewnętrznego i usług realizowanych w sieciach rozległych pod względem efektywności lub jakości usług

Programowanie obiektowe	3	NIE	Wykorzystanie języków obiektowych i dostępnych bibliotek do rozwiązywania problemów technicznych
Wprowadzenie to multimediów	4	TAK	Badania związane z przesyłaniem i przetwarzaniem obrazu i dźwięku. Metody przetwarzania i kompresji danych multimedialnych
Podstawy sztucznej inteligencji i uczenia maszynowego	4	TAK	Uczenie maszynowe w zastosowaniach teleinformatycznych
Sieci i systemy bezprzewodowe	4	TAK	Metody transmisji danych w sieciach bezprzewodowych i mobilnych
Podstawy usług i aplikacji chmurowych	2	NIE	Modelowanie systemów kolejkowych w strukturach centrów danych
Podstawy IoT	3	NIE	Algorytmy transmisji danych w systemach sensorycznych
Synchronizacja	4	TAK	Algorytmy synchronizacji w systemach teleinformatycznych, metody rozsyłania sygnałów zegarowych
Bezpieczeństwo sieci LAN i WAN	4	TAK	Badania efektywności rozwiązań zapewniających bezpieczeństwo sieci lokalnych i rozległych
Ochrona dostępu w rozproszonych systemach multimedialnych	4	TAK	Projektowanie i badanie algorytmów w systemach rozproszonych
Bezpieczeństwo systemów IoT i IIoT	4	TAK	Badania efektywności rozwiązań zapewniających bezpieczeństwo w systemach sensorycznych
AI w cyberbezpieczeństwie multimediów	5	TAK	Uczenie maszynowe w zastosowaniach teleinformatycznych oraz w wykrywaniu anomalii
Sieci definiowane programowo	5	TAK	Badanie efektywności rozwiązań zapewniających bezpieczeństwo wykorzystujących cechy sieci SDN
Wirtualna i rozszerzona rzeczywistość	5	TAK	Przetwarzanie danych dla wirtualnej rzeczywistości. Badania w zakresie nowych technik śledzenia, renderowania i projekcji w kontekście rozszerzonej wirtualnej rzeczywistości, w celu zapewnienia bardziej realistycznych i immersyjnych doświadczeń użytkownikom
Wprowadzenie do obliczeń kwantowych	2	TAK	Przetwarzanie kwantowe i komunikacja kwantowa. Badania nad bezpiecznym przesyłaniem informacji przy użyciu zjawisk kwantowych, takich jak kwantowa kryptografia kwantowa.
Techniki deepfake	4	TAK	Klasyfikacja danych, w tym analiza wzorców i anomalii
Bezpieczeństwo systemów operacyjnych	4	NIE	Ocena efektywności rozwiązań programowych i sprzętowych zapewniających bezpieczeństwo systemów komputerowych i systemów operacyjnych
Wykrywanie anomalii sieciowych i detekcja zagrożeń w sieci z wykorzystaniem AI	4	TAK	Klasyfikacja danych, w tym analiza wzorców i anomalii
Techniki ochrony multimediów	3	TAK	Projektowanie zarówno komponentów, jak i całych metod kryptograficznych.

Bezpieczeństwo systemów zarządzania bazami danych	4	TAK	Projektowanie środowisk bazodanowych oraz zarządzenie systemami bazodanowymi. Ocena efektywności mechanizmów zapewniających bezpieczeństwo systemów bazodanowych
Bezpieczeństwo systemów bezprzewodowych	3	TAK	Metody transmisji danych w sieciach bezprzewodowych i mobilnych. Badanie efektywności rozwiązań zapewniających bezpieczeństwo systemów bezprzewodowych, w tym systemów otwartych
Biometryczne uwierzytelnianie tożsamości	4	TAK	Projektowanie zarówno komponentów, jak i całych metod kryptograficznych. Algorytmy przetwarzania danych multimedialnych
Bezpieczeństwo w systemach chmurowych	4	TAK	Algorytmy przetwarzania danych w sieciach rozproszonych. Analiza efektywności mechanizmów bezpieczeństwa w systemach chmurowych
Urządzenia programowalne	3	TAK	Wykorzystanie układów programowalnych dla celów współczesnej teleinformatyki
Podstawy analizy informacji	3	TAK	Metody uczenia maszynowego w przetwarzaniu danych. Algorytmy neurolingwistyczne
Bezpieczeństwo danych medycznych	5	TAK	Projektowanie zarówno komponentów, jak i całych metod kryptograficznych. Algorytmy przetwarzania danych multimedialnych
Bezpieczeństwo fizyczne systemów i urządzeń IT	5	TAK	Badanie algorytmów kryptograficznych. Analiza działania układów elektronicznych
Zarządzanie bezpieczeństwem sieci	5	TAK	Badania efektywności rozwiązań zapewniających bezpieczeństwo sieci teleinformatycznych
Cyberbezpieczeństwo w mediach publicznych i społecznościowych	4	NIE	Projektowanie zarówno komponentów, jak i całych metod kryptograficznych. Metody uczenia maszynowego w przetwarzaniu danych
Metody i zasady uwierzytelnienia	4	NIE	Projektowanie zarówno komponentów, jak i całych metod kryptograficznych. Mechanizmy autentykacji
Bezpieczeństwo systemów bezzałogowych i satelitarnych	4	TAK	Transmisja danych w systemach satelitarnych. Optymalizacja systemów transmisji danych satelitarnych w celu zwiększenia ich przepustowości i efektywności. Badania nad nowymi technologiami, takimi jak zaawansowane modulacje, multipleksowanie i kodowanie korekcyjne, aby zwiększyć wydajność transmisji. Badania nad zaawansowanymi technologiami antenowymi, takimi jak anteny o wysokiej rozdzielczości, anteny wielostrumieniowe (MIMO) czy anteny o adaptacyjnej kierunkowości.

Systemy komunikacji kwantowej	2	TAK	Przetwarzanie kwantowe i komunikacja kwantowa. Badania nad przenoszeniem i komunikacją kwantową w systemach telekomunikacyjnych, z uwzględnieniem wyzwań związanych z dystansem i warunkami środowiskowymi. Badania nad bezpiecznym przesyłaniem informacji przy użyciu zjawisk kwantowych, takich jak kwantowa kryptografia kwantowa.
Razem	**150**		

II. Informacje uzupełniające

1. Koncepcja kształcenia oraz zgodność efektów uczenia się z potrzebami rynku pracy

Misją Politechniki Poznańskiej jest zapewnienie wysokiej jakości kształcenia na wszystkich stopniach studiów wyższych oraz w ramach kształcenia ustawicznego, w ścisłym powiązaniu z prowadzonymi na Uczelni pracami naukowymi i badawczo-rozwojowymi. Uczelnia dąży do współpracy zarówno z przyszłymi pracodawcami swoich absolwentów, jak i ze społeczeństwem, odpowiadając na jego potrzeby i wyzwania. Priorytetem władz i całej społeczności akademickiej Politechniki Poznańskiej jest osiągnięcie statusu wiodącego uniwersytetu technicznego w kraju oraz uzyskanie międzynarodowego uznania jako partner dla czołowych uczelni europejskich i pozaeuropejskich, wyróżniającego się jakością kształcenia, wysokim poziomem badań naukowych oraz innowacyjnymi rozwiązaniami wdrożeniowymi.

Wydział Informatyki i Telekomunikacji kształci specjalistów na trzech stopniach studiów w obszarze szeroko rozumianych technologii informatyczno-komunikacyjnych, obejmujących informatykę, bioinformatykę, teleinformatykę, sztuczną inteligencję oraz elektronikę i telekomunikację. Proces kształcenia oparty jest na wynikach prowadzonych na Wydziale badań naukowych oraz na efektach współpracy z sektorem gospodarczym i instytucjami administracji samorządowej. Dzięki temu programy studiów uwzględniają zarówno potrzeby regionalne i krajowe, jak i międzynarodowe. Wydział odgrywa kluczową rolę w realizacji misji Politechniki Poznańskiej, wspierając budowanie pozycji Uczelni jako czołowego uniwersytetu technicznego w kraju, rozpoznawalnego i cenionego zarówno w Unii Europejskiej, jak i poza jej granicami.

Utworzenie nowego kierunku kształcenia cyberbezpieczeństwo wpisuje się w realizację przyjętej misji strategii rozwoju Uczelni i Wydziału poprzez realizację następujących celów strategicznych:

- wysokiej jakości kształcenie kadr przygotowujące do pracy i funkcjonowania w społeczeństwie opartym na wiedzy w obszarze cyberbezpieczeństwa,
- tworzenie atrakcyjnych i elastycznych programów dydaktycznych nakierowanych na zapotrzebowania rynku oraz wymagania społeczeństwa i cywilizacji,
- rozwój programów studiów (infrastruktura i umiędzynarodowienie) z uwzględnieniem niżu demograficznego i innych czynników, takich jak położenie

geopolityczne Polski,

- budowanie doskonałości naukowej – kreowanie i zdefiniowanie strategicznych obszarów badań, wysokiej jakości prac naukowych, wzrost cytowalności publikacji, pozycja lidera o uznaniu światowym, w obszarze cyberbezpieczeństwa,
- wzrost efektywności w zdobywaniu środków na rozwój nauki i badań – udział w projektach międzynarodowych i krajowych,
- transfer osiągnięć naukowych do przedsiębiorstw i społeczeństwa,
- zwiększenie zakresu i efektywności prac naukowych i badawczo rozwojowych prowadzonych we współpracy z podmiotami zewnętrznymi,
- wzrost rozpoznawalności Uczelni w kraju i za granicą.

Program studiów pierwszego stopnia na kierunku cyberbezpieczeństwo jest zgodny z przyjętą strategią Uczelni i Wydziału. Gwarantem wysokiego poziomu i jakości kształcenia, nowoczesności oraz innowacyjności opracowanego programu oraz warunków, w jakich proces ten będzie realizowany, jest Wydziałowy System Zapewnienia Jakości Kształcenia (WSZJK), który powstał przez połączenie WSZJK funkcjonujących na nieistniejących już Wydziale Informatyki oraz Wydziale Elektroniki i Telekomunikacji (oba te wydziały utworzyły obecny Wydział Informatyki i Telekomunikacji). Nowoczesność oraz innowacyjność programu są wynikiem wykorzystania doświadczenia interesariuszy wewnętrznych (pracowników, studentów), w tym osób wcześniej zaangażowanych w przygotowanie specjalności na II stopniu kierunku informatyka, zewnętrznych (współpraca dydaktyczna Wydziału z pracodawcami, szczególnie z obszaru cyberbezpieczeństwa, informatyki i teleinformatyki) oraz wykorzystania wyników prac naukowo-badawczych prowadzonych w Instytucie Informatyki, Instytucie Radiokomunikacji, Instytucie Sieci Teleinformatycznych oraz Instytucie Telekomunikacji Multimedialnej.

Koncepcja i program studiów obejmujący efekty uczenia się są spójne i innowacyjne, wynikają także z uwzględnienia potrzeb otoczenia społeczno-gospodarczego oraz zmian legislacyjnych związanych z koniecznością wdrażania dyrektyw Unii Europejskiej, w tym dyrektywy na rzecz wysokiego cyberbezpieczeństwa na terytorium Unii Europejskiej (NIS-2). W trakcie tworzenia programu studiów na kierunku cyberbezpieczeństwo uwzględniono również kompetencje w zakresie wiedzy, umiejętności i zdolności zawartych w ramach Krajowej inicjatywy na rzecz edukacji w zakresie cyberbezpieczeństwa NICE (National Initiative for Cybersecurity Education) zdefiniowanych przez Narodowy Instytut Norm i Technologii NIST (National Institute of Standards and Technology) działający przy Departamencie Handlu Stanów Zjednoczonych. Dokumenty NICE są obecnie podstawą współpracy w USA na styku uniwersytety-pracodawcy w zakresie cyberbezpieczeństwa.

Potrzeba utworzenia kierunku cyberbezpieczeństwo wynika z zapotrzebowania na wysokiej klasy specjalistów ds. cyberbezpieczeństwa. W roku 2024 odnotowano 19,1% wzrost zapotrzebowania w tym obszarze. Największy wzrost zapotrzebowania zaobserwowano w regionie Azji Pacyficznej, gdzie wyniósł aż 26,4 proc. (ponad 3,4 mln wakatów). Na drugim miejscu znalazła się Europa, z wzrostem w stosunku do 2023 roku wynoszącym 12,8 proc. (392 tys. wakatów). Zgodnie z raportem Microsoft Digital Defense Report Polska jest czwartym pod względem zagrożonych cyberprzestępczością krajem na świecie, zaraz po Ukrainie, Wielkiej Brytanii i Francji. Wpływ na to ma nie tylko położenie

geopolityczne, ale również postępująca cyfryzacja polskiej gospodarki, która wyróżnia nas na tle innych krajów Unii Europejskiej. Według raportu OECD „Building a Skilled Cyber Security Workforce in Europe" zapotrzebowanie na specjalistów ds. cyberbezpieczeństwa po lutym 2020 roku rosło w Polsce 3 razy szybciej niż zapotrzebowanie na pracowników innych specjalizacji. Szacuje się, że obecnie brakuje ponad 20 000 specjalistów. Zgodnie z raportem Fortinet „2024 Cybersecurity Skills Gap" 54% firm ciągle szuka pracowników z tej branży, natomiast 50% firm nie potrafi zatrzymać ich u siebie, narażając tym samym na poważne zagrożenia.

Zgodnie z opublikowanym w 2023 roku raporcie firmy Gartner, będącej przedsiębiorstwem analityczno-badawczym specjalizującym się w zagadnieniach strategicznego wykorzystania technologii oraz zarządzania technologiami, w 2025 roku połowa cyberataków będzie spowodowana brakiem specjalistów ds. cyberbezpieczeństwa oraz ludzkimi zaniedbaniami. Według raportu Global Cybersecurity Outlook 2023, opublikowanego przez World Econimic Forum, najbardziej pożądanymi obszarami cyberbezpieczeństwa będzie bezpieczeństwo infrastruktury chmurowej i usług chmurowych (46%), analiza cyberzagrożeń (37%), analiza złośliwego oprogramowania (34%).

Przyjęta koncepcja kształcenia zakłada powiązanie przedmiotów kierunkowych i specjalnościowych z tematyką badań naukowych i prac B+R pracowników Wydziału. Wiele z nich wynika z wyzwań i oczekiwań przed jakimi staje obecnie społeczeństwo cyfrowe, co przejawia się w potrzebach operatorów sieci teleinformatycznych, producentów sprzętu, służb mundurowych czy dostawców usług cyfrowych.

Opracowując program studiów kierunku Cyberbezpieczeństwo uwzględniono dyrektywy NIST NICE oraz NIS-2. Narodowa Inicjatywa Edukacji Cyberbezpieczeństwa jest programem Narodowego Instytutu Standardów i Technologii NIST w Stanach Zjednoczonych. Celem NICE jest stworzenie dobrze wykwalifikowanej siły roboczej w dziedzinie cyberbezpieczeństwa poprzez rozwój standardów edukacyjnych, ram kompetencji oraz wspieranie współpracy między sektorem publicznym, prywatnym i środowiskiem akademickim. Natomiast dyrektywa NIS-2 (Directive on Security of Network and Information Systems) jest nową wersją europejskiej dyrektywy o bezpieczeństwie sieci i systemów informatycznych. Została przyjęta przez Unię Europejską w 2022 roku jako następca pierwszej dyrektywy NIS z 2016 roku. Jej celem jest zwiększenie poziomu cyberbezpieczeństwa w krajach członkowskich oraz dostosowanie przepisów do zmieniających się zagrożeń w świecie cyfrowym. Uwzględniając wymienione dyrektywy oraz potencjał naukowy i dydaktyczny Wydziału Informatyki i Telekomunikacji zaproponowano 3 profile kształcenia: Bezpieczeństwo Sieci Teleinformatycznych (BST), Bezpieczeństwo Przetwarzania Danych (BPD) oraz Bezpieczeństwo Komunikacji Multimedialnej (BKM).

Student, który posiądzie kompetencje przewidziane dla obszaru Bezpieczeństwa Sieci Teleinformatycznych, zgodnie z dyrektywą NIST NICE, będzie mógł w przyszłości zostać

zatrudniony w następujących zawodach:

1) Specjalista ds. bezpieczeństwa sieci,
2) Inżynier ds. bezpieczeństwa systemów IoT/IIoT,
3) Specjalista ds. analizy zagrożeń,
4) Architekt bezpieczeństwa chmurowego,
5) Administrator bezpieczeństwa SOC,
6) Inżynier ds. automatyzacji konfiguracji sieci,
7) Specjalista ds. bezpieczeństwa systemów bezzałogowych i łączności satelitarnej,
8) Specjalista ds. bezpieczeństwa aplikacji internetowych i mobilnych,
9) Specjalista ds. białego wywiadu,,
10) Specjalista ds. informatyki śledczej,
11) Kryptograf / Specjalista ds. systemów kwantowych,
12) Konsultant ds. cyberbezpieczeństwa,
13) Menadżer ds. bezpieczeństwa IT / Kierownik działu SOC.

W obszarze Bezpieczeństwa Przetwarzania Danych przewidzianymi dla studenta zawodami są:

1) Inżynier ds. bezpieczeństwa IoT/IIoT,
2) Specjalista ds. sieci definiowanych programowo,
3) Inżynier ds. bezpieczeństwa systemów operacyjnych,
4) Specjalista ds. bezpieczeństwa funkcjonalnego i łańcucha dostaw,
5) Specjalista ds. bezpieczeństwa w chmurze,
6) Specjalista ds. urządzeń programowalnych,
7) Specjalista ds. bezpieczeństwa fizycznego urządzeń IT ,
8) Specjalista ds. uwierzytelniania i autoryzacji,
9) Specjalista ds. bezpieczeństwa baz danych,
10) Specjalista ds. systemów komunikacji kwantowej,
11) Administrator SOC / Analityk bezpieczeństwa,
12) Konsultant ds. cyberbezpieczeństwa.

Natomiast pozyskanie przez studenta kompetencji w obszarze Bezpieczeństwa Komunikacji Multimedialnej jest podstawą do zatrudnienia go w następujących zawodach:

1) Specjalista ds. bezpieczeństwa multimediów,
2) Koordynator ds. jakości usług multimedialnych,
3) Analityk autentyczności treści,
4) Inżynier ds. cyberkryminalistyki multimedialnej,
5) Specjalista ds. biometrii i uwierzytelniania tożsamości,
6) Specjalista ds. bezpieczeństwa danych medycznych,
7) Specjalista ds. cyberbezpieczeństwa mediów społecznościowych,
8) Konsultant ds. własności intelektualnej,
9) Menadżer ds. cyberbezpieczeństwa multimediów.

Ponadto, studenci kierunku *cyberbezpieczeństwo* będą mogli podnosić swoje kompetencje i wiedzę dzięki współpracy Politechniki z zagranicznymi jednostkami naukowo-badawczymi, w tym z uczelniami zrzeszonymi w ramach Uniwersytetu Europejskiego

EUNICE.

Kierunek Cyberbezpieczeństwo jest od niedawna oferowany przez uczelnie w Polsce. W Ogólnopolskim Systemie Monitorowania Ekonomicznych Losów Absolwentów (ELA) prezentowane są obecnie wyłącznie informacje o absolwentach tego kierunku z Politechniki Wrocławskiej. System zawiera następujące dane:

- Czas poszukiwania pracy etatowej – czas, który przeciętny absolwent (zatrudniony na etacie) potrzebował na znalezienie takiej pracy.
- Wynagrodzenie ogółem brutto – mediana średnich miesięcznych zarobków ze wszystkich źródeł w pierwszym roku po uzyskaniu dyplomu.
- Względny wskaźnik zarobków – wynagrodzenie absolwenta (ze wszystkich źródeł) w pierwszym roku po dyplomie w stosunku do średnich zarobków w jego miejscu zamieszkania.
- Bezrobocie – procent czasu, w którym przeciętny absolwent pozostawał bezrobotny w pierwszym roku po ukończeniu studiów.
- Względny wskaźnik bezrobocia – bezrobocie absolwentów w pierwszym roku po dyplomie w stosunku do stopy bezrobocia w ich miejscu zamieszkania.

W poniższej tabeli przedstawiono porównanie statystyk dotyczących sytuacji zawodowej absolwentów kierunku Cyberbezpieczeństwo (oferowanego przez Politechnikę Wrocławską) ze statystykami dotyczącymi absolwentów Wydziału Informatyki i Telekomunikacji Politechniki Poznańskiej (kierunki: Informatyka, Elektronika i Telekomunikacja oraz Teleinformatyka) oraz z danymi zagregowanymi dla wszystkich kierunków nauk inżynieryjno-technicznych. Jak można zauważyć, sytuacja zawodowa absolwentów Cyberbezpieczeństwa jest lepsza niż w przypadku pozostałych kierunków użytych do porównania. Potwierdza to tezę o ogromnym zapotrzebowaniu na specjalistów w tej dziedzinie.

Porównanie statystyk sytuacji zawodowej absolwentów studiów I st. kierunku Cyberbezpieczeństwo z kierunkami pokrewnymi.

	Kierunki w dziedzinie nauk inżynieryjno-technicznych	Informatyka Politechnika Poznańska	Elektronika i telekomunikacja Politechnika Poznańska	Teleinformatyka Politechnika Poznańska	Cyberbezpieczeństwo Politechnika Wrocławska
Czas poszukiwania pracy etatowej [mies.]	2,01	2,26	2,76	2,64	1,31
Wynagrodzenie ogółem brutto [zł]	4985	5485	5189	5366	7192
Względny wskaźnik zarobków [/]	0,76	0,85	0,69	0,81	1,12

Bezrobocie [%]	1,99	0,27	2,61	0,13	0,19
Względny wskaźnik bezrobocia [/]	0,37	0,05	1,66	0,01	0,03

2. Opis działań na rzecz doskonalenia programu studiów oraz zapewniania jakości kształcenia

W kontekście kierunku Cyberbezpieczeństwo należy podkreślić spójność podejmowanych działań z przyjętą w ramach Wydziału Informatyki i Telekomunikacji oraz w ramach Politechniki Poznańskiej polityką doskonalenia jakości kształcenia. Wszystkie przedstawione tutaj działania spełniają zasady dotyczące zapewnienia jakości kształcenia na Politechnice Poznańskiej regulowane Uchwałą nr 45 Senatu Akademickiego Politechniki Poznańskiej z dnia 31 maja 2021 roku w sprawie Uczelnianego Systemu Zapewnienia Jakości Kształcenia.

Zarządzanie kierunkiem i kompetencje organów zarządzającym kierunkiem i Wydziałem są określone w Statucie Uczelni i należą do Dziekana i Rady Wydziału Informatyki i Telekomunikacji. Zgodnie ze Statutem PP Dziekan m. in. organizuje i zapewnia prawidłowy przebieg procesu kształcenia. Programy i plany studiów są konsultowane ze studentami przed ich uchwaleniem. Na WIiT w kadencji 2024-2028 Dziekan powołał dwóch prodziekanów ds. kształcenia. Jednemu z prodziekanów podlegają sprawy studiów dotyczących zagadnień telekomunikacyjnych, natomiast drugiemu prodziekanowi – informatycznych.

Na Wydziale Informatyki i Telekomunikacji wewnętrzny system zapewnienia jakości kształcenia (WSZJK) został utworzony na podstawie odpowiednich uchwał Senatu PP, Statutu PP i zarządzeń Rektora PP. Zgodnie z tymi dokumentami Dziekan Wydziału powołał na kadencję 2020-2024 Wydziałowy Zespół ds. Jakości Kształcenia (WZJK) i Pełnomocnika Dziekana ds. Jakości Kształcenia jako przewodniczącego tego zespołu. W skład WZJK wchodzą studenci.

Analiza przygotowania kandydatów na studia

Rekrutacja kandydatów na wszystkie kierunki studiów na Uczelni odbywa się z wykorzystaniem elektronicznego systemu rekrutacji. Każdy kandydat na studia może deklarować kilka kierunków studiów, którymi jest zainteresowany. W kontekście studiów pierwszego stopnia na kierunku Cyberbezpieczeństwo przyjęcia na studia dokonuje się na podstawie wyników egzaminu maturalnego (konkurs świadectw).

W celu zapewnienia możliwie wysokiego przygotowania merytorycznego kandydatów, Wydział przedsiębierze różnego rodzaju działania mające zwiększyć zainteresowanie studentów kierunkiem. Należą do nich np.:

- eksponowanie na stronie internetowej oraz w mediach społecznościowych nagród i osiągnięć (zwłaszcza międzynarodowych) studentów i pracowników Wydziału, co ma na celu poinformowanie kandydatów o wysokim poziomie studiów na WIiT,
- promowanie wsparcia aktywności studenckiej,
- zwiększenie liczby ogłoszeń dla studentów w mediach w okresie poprzedzającym rekrutację,
- współpracę z wybranymi szkołami średnimi (wykłady i laboratoria dla uczniów),
- organizację wydziałowych Drzwi Otwartych,
- aktywny i liczny udział w imprezach uczelnianych takich jak Noc Naukowców, Dziewczyny na Politechniki, Targi Edukacyjne, itp.,
- opracowanie atrakcyjnego informatora o studiach na WIiT dostępnego na stronie WWW Wydziału oraz rozdawanego w formie drukowanej w szkołach licealnych (głównie województwa wielkopolskiego).

Działania mające na celu doskonalenie WSZJK

Dziekan, członkowie Rady Wydziału oraz studenci mają prawo zgłaszać swoje postulaty

członkom WSZJK. Postulaty te są dyskutowane na spotkaniach WSZJK odbywających się na zasadach zgodnych z regułami funkcjonowania WSZJK obowiązującymi na wydziale. Studenci biorą udział w tych spotkaniach, jeżeli sami zgłoszą swoje postulaty.

Wskazówki prowadzące do doskonalenia WSZJK płyną także z Uczelnianego Zespołu ds. Jakości Kształcenia, który ma możność obserwowania wszystkich systemów wydziałowych.

W celu zapewnienia wysokiej jakości kształcenia przeprowadza się regularne oceny stanu bazy laboratoryjnej na wydziale.

Monitorowanie efektów uczenia się

Krok 1. Monitorowanie efektów uczenia się odbywa się w pierwszej kolejności przez ocenę wyników egzaminów, zaliczeń, kolokwiów, systematyczną ocenę wykonania ćwiczeń laboratoryjnych, systematyczną kontrolę rozwiązywania przez studentów zadań domowych. Systematyczne ocenianie rezultatów różnego rodzaju zadań stawianych studentom (wymienionych wcześniej) pozwala ocenić zarówno wiedzę studenta, jak i jego umiejętności oraz postawę społeczną. Wyniki ocen uzyskanych przez studentów na różnych latach, z różnych przedmiotów są przygotowane przez prodziekanów i następnie dyskutowane przez WSZJK, Radę Wydziału i Dziekana. Wnioski z dyskusji są przekazywane prowadzącym zajęcia i mają wpływ na sposób oceniania studentów (np. czas trwania egzaminów, liczbę kolokwiów, charakter zadań dla studentów, itp.).

Krok 2. Drugim krokiem w procedurze monitorowania (kontrolowania) efektów uczenia się (w zakresie wiedzy, umiejętności i postaw) jest ocena jakości/możliwości/poziomu wykonania projektów i ćwiczeń, na których student powinien wykazać się wiedzą, umiejętnościami i odpowiedzialnością nabytą na wcześniejszych etapach kształcenia. Taka możliwość wynika z realizowanego programu studiów, który wymaga na kolejnych przedmiotach wykazaniem się wiedzą, umiejętnościami i kompetencjami nabytymi wcześniej.

Przykłady wybrane spośród wielu innych przykładów monitorowania efektów uczenia się wynikających z oceny realizacji programu studiów i oceny przez prowadzących zajęcia wiedzy, umiejętności i postaw studentów uzyskanych na poprzednich etapach kształcenia przytoczone są poniżej:

- na większości przedmiotów obowiązuje konieczność czytania literatury technicznej w j. angielskim, co pozwala sprawdzić prowadzącemu zajęcia umiejętności językowe studenta, a samemu studentowi udoskonalić i ewentualnie poprawić swoje umiejętności językowe,
- w trakcie realizacji wielu przedmiotów/projektów/laboratoriów wykorzystywane są efekty uczenia się w zakresie umiejętności programowania, które powinny być nabyte na wcześniejszych etapach studiów.

Opinie prowadzących zajęcia dotyczące uzyskanych przez studentów efektów uczenia się są w formie ustnej przekazywane przez poszczególnych pracowników kierownikom instytutów i prodziekanom.

Krok 3. Wyniki ocen uzyskanych przez studentów po zakończeniu semestru są w formie krótkiego sprawozdania przedstawiane przez odpowiedniego prodziekana w celu ich przedyskutowania. Forma sprawozdania zależy od prodziekana. Wynikiem dyskusji mogą być propozycje zmian kolejności przedmiotów, zmiany planu, zmiany osób prowadzących zajęcia, zmiany sposobu prowadzenia zajęć, podjęcie hospitacji na danym przedmiocie w celu zorientowania się w istocie problemu. Egzekwowanie zmian w sprawach, dla których osiągnięto konsensus, lub które nakazał Dziekan należy do Dziekana, prodziekanów lub dyrektorów instytutów zależnie od charakteru tych zmian.

Krok 4. Ostatnim dostępnym Wydziałowi w czasie studiów sposobem sprawdzenia osiągniętych efektów uczenia się w procesie kształcenia jest wykonanie przez studenta pracy dyplomowej, zrecenzowanie tej pracy i jej ocena, oraz zdanie przez studenta egzaminu dyplomowego.

Ocena jakości i warunków prowadzenia zajęć dydaktycznych

Inne działania mające na celu podniesienie jakości kształcenia oraz kontrolę i doskonalenie realizacji programu kształcenia obejmują:

- Co semestralne ogólnouczelniane ankiety studenckie oceny zajęć i prowadzących obejmujące I i II stopień studiów oraz związane z tym procesem systemy:
  - nagradzania wykładowców,
  - hospitacji zajęć.
- Ocena dyscypliny prowadzenia zajęć i konsultacji, opcjonalnie w przypadku napływających skarg studentów.
- Opcjonalne krótkie ankiety przeprowadzane przez nauczycieli akademickich we własnym zakresie, w przypadku zajęć przypisanych do klasy „obserwowalne" – ankieta zajęciowa umożliwia szybką reakcję na uwagi studentów.
- Zapewnienie odpowiedniej jakości kadry dydaktycznej poprzez:
  - zdefiniowanie zasad obsady zajęć dydaktycznych,
  - zdefiniowanie obowiązków prowadzących zajęcia,
  - co semestralne hospitacje zajęć,
- Obsługę procesu dyplomowania wg ściśle zdefiniowanych zasad i procedur określonych przez Uczelniany System Obsługi Studentów (USOS).
- Uwzględnianie w programie kształcenia wyników monitorowania karier zawodowych absolwentów.

Na kierunku studiów prowadzonych na Wydziale Informatyki i Telekomunikacji, przeprowadzane są badania ankietowe (poprzedzone akcją informacyjną) oceniające kompleksowo wszystkie przedmioty i nauczycieli akademickich. Aktualnie wykorzystywany kwestionariusz elektroniczny obejmuje grupy pytań dotyczące organizacji, poziomu merytorycznego i sposobu prowadzenia zajęć, stosunku prowadzącego do studentów. Ankietowanie jest realizowane z wykorzystaniem systemu informatycznego eAnkieta, który zapewnia anonimowość, umożliwia analizę wyników i generowanie raportów.

Jeśli chodzi o sposoby wykorzystania wniosków z ocen nauczycieli akademickich dokonywanych przez studentów, to wyniki ankietowania zajęć są brane pod uwagę przez Komisję Dziekańską ds. Nagród przy rekomendowaniu Radzie Wydziału Informatyki i Telekomunikacji pracowników kandydujących do Nagrody JM Rektora PP za osiągnięcia dydaktyczne oraz przez Wydziałowego Pełnomocnika ds. Jakości Kształcenia przy opracowywaniu planu hospitacji zajęć w danym semestrze. Wyniki ankiet brane są również pod uwagę przy ocenie okresowej pracowników. W przypadku długotrwale powtarzających się negatywnych ocen, WPJK przeprowadza rozmowę wyjaśniającą z pracownikiem, a w przypadku braku reakcji na zastrzeżenia wnioskuje o odsunięcie pracownika od prowadzenia źle ocenianych zajęć.

Wnioski z ocen dokonywanych przez studentów wykorzystuje się również w procesie hospitacji zajęć. Każdy pracownik jest hospitowany okresowo. Równocześnie, na podstawie wyników ankiet, o których mowa powyżej – proces hospitacji realizowany jest w odniesieniu do wybranych zajęć, które w ankietach studenckich otrzymały średnią ocenę poniżej progu ustalonego przez WPJK. Listę takich dodatkowych osób, prowadzących zajęcia, kierowanych na hospitacje, określa Wydziałowy Pełnomocnik ds. Jakości Kształcenia.

Ocena warunków prowadzenia zajęć dydaktycznych przeprowadzana jest co semestr. Tryb jej przeprowadzania uzależniony jest od rodzaju sal, w których prowadzone są zajęcia. W przypadku sal, w których odbywają się wykłady, ćwiczenia, projekty (niewymagające pracy przy komputerze), oceny warunków dokonuje pracownik Dziekanatu Wydziału Informatyki i Telekomunikacji. Natomiast ocenę okresową warunków prowadzenia zajęć w laboratoriach przeprowadza się na poziomie Instytutów lub Zakładów. Ocenie podlega zarówno wyposażenie laboratoriów, jak również dostępność materiałów dydaktycznych związanych z prowadzonymi zajęciami.

Opis sposobów określania efektów uczenia się

Wdrożony na WIiT system oceniania prac zaliczeniowych, projektowych i egzaminacyjnych podporządkowany jest nadrzędnemu celowi, jakim jest przyswojenie przez studentów wiedzy przekazywanej im w trakcie zajęć, a także zdobycie umiejętności praktycznego wykorzystania wiedzy. Sprawdzaniu podlega także znajomość podstawowych zagadnień teoretycznych i umiejętność wykorzystania tej wiedzy do rozwiązywania problemów technicznych. Przyjęto, że warunkiem uzyskania pozytywnej oceny pracy zaliczeniowej lub egzaminacyjnej jest uzyskanie 50% możliwych punktów za wszystkie wykonane zadania oraz przedstawione odpowiedzi na pytania. Jest to zgodne z dokumentem „Dobre praktyki dla nauczycieli akademickich", który został przygotowany przez Uczelnianą Radę ds. Jakości Kształcenia Politechniki Poznańskiej w 2023r.

Ze względu na specyfikę niektórych przedmiotów ten próg jest w szczególnych przypadkach modyfikowany w granicach ±10%, o czym studenci są informowani z odpowiednim wyprzedzeniem. Wyższe oceny są wystawiane proporcjonalnie do uzyskanej oceny punktowej. Ogólnie przyjęto, że egzaminy i prace zaliczeniowe obejmują minimum trzy zadania, problemy lub pytania. Jednak ta liczba dla zdecydowanej większości przedmiotów jest wyraźnie większa, co umożliwia uzyskanie obiektywnego obrazu wiedzy i umiejętności studentów. Zasadą jest dobór pytań i zadań w taki sposób, by przekrojowo ocenić wiedzę i umiejętności zdającego.

Prace projektowe ocenia się biorąc pod uwagę zgodność końcowego opracowania z przyjętymi na wstępie założeniami technicznymi, oryginalność i samodzielność pracy, walory użytkowe i poziom techniczny zaprojektowanego systemu lub urządzenia, zgodność z zasadami dobrych praktyk inżynierskich oraz nakład pracy studenta, w tym zwłaszcza na zdobycie dodatkowej wiedzy wykraczającej poza zakres dotychczasowych studiów. Umiejętność uzyskiwania dodatkowej wiedzy jest ważną składową oceny kwalifikacji projektanta. Warunkiem uzyskania oceny dostatecznej jest spełnienie minimalnych warunków określonych przy wydawaniu projektu. Podobne zasady obowiązują przy ocenie prac dyplomowych, dla których dodatkowo ocenia się możliwość publikacji i możliwość zastosowań praktycznych pracy.

Studentom zwraca się uwagę, że bardzo surowo traktuje się wszystkie wykryte próby nieuczciwości, w tym zwłaszcza korzystanie z cudzych wyników. Studenci mają możliwość zapoznania się z ocenionymi pracami oraz uzyskania wyjaśnień na temat poprawnych rozwiązań oraz zasad oceny prac.

Prace zaliczeniowe, w tym szczególnie kolokwia zaliczeniowe stanowiące podstawę zaliczenia zajęć ćwiczeniowych (audytoryjnych lub laboratoryjnych), realizuje się w połowie semestru i pod koniec semestru, lub jedynie na koniec semestru, w zależności od liczby godzin przypadających na dane zajęcia. Ostateczna ocena z ćwiczeń (ocena związana z zaliczeniem ćwiczeń) zależy od ocen prac zaliczeniowych, ale także zaangażowania w ćwiczenia, znajomość treści wykładów i umiejętność rozwiązywania problemów. Zgodnie z Regulaminem Studiów przeprowadza się dodatkowe zaliczenia poprawkowe przed terminem egzaminu dla studentów, którzy nie uzyskali pozytywnej oceny.

System sprawdzenia efektów uczenia się w procesie dyplomowania

Proces dyplomowania jest bardzo ważnym okresem studiów pozwalającym na badanie realizacji efektów uczenia się. Prowadzący pracę dyplomową ma sposobność sprawdzania wyniesionej ze studiów wiedzy dyplomanta nadzorując systematycznie postępy w realizacji pracy dyplomowej. WSZJK kładzie nacisk na systematyczność spotkań opiekuna pracy dyplomowej z dyplomantem, co umożliwia weryfikację posiadanych przez studenta efektów uczenia się i w dużej mierze zapobiega plagiatowi. Sygnały przekazywane Dyrektorom Instytutów od wielu prowadzących dają łącznie szeroką orientację w realizacji efektów uczenia się całych studiów. Ponadto, prowadzący prace dyplomowe mają możliwość zgłaszania zaobserwowanych braków w tej dziedzinie do WSZJK normalną drogą, czyli przez Dyrektorów swoich Instytutów. Taka forma zgłaszania uwag jest

postulowana przez WZJK. Plan studiów na kierunku Cyberbezpieczeństwo zakłada istnienie trzech modułów (przedmiotów) wspomagających przygotowanie pracy dyplomowej na wysokim (także naukowym) poziomie. Warunkiem zaliczenia przedmiotu Pracownia Przeddyplomwa, której celem jest wspomaganie wyboru pracy dyplomowej, jest przygotowanie i przedstawienie trzech prezentacji dotyczących zagadnień związanych z pracą dyplomową oraz przedstawienie wyniku przeglądu literatury. W ostatnim semestrze studiów studenci w trakcie zajęć z przedmiotu Seminarium Dyplomowe przedstawiają postępy w realizacji swoich prac dyplomowych. Ostatni moduł, Prace Badawczo-wdrożeniowe ma na celu przygotowanie studentów do prowadzenia prac badawczo-wdrożeniowych oraz komercjalizacji wyników badań. Studenci poznają zasady realizacji projektów B+R (badawczo-rozwojowych) oraz technologicznych wdrożeń w przemyśle.

Innym narzędziem badania realizacji efektów uczenia się jest analiza przez WSZJK sygnałów osób biorących udział w obronach prac dyplomowych (egzaminach dyplomowych). Z jednej strony prodziekani przygotowują ocenę statystyczną wyników egzaminów dyplomowych, z drugiej strony przez Dyrektorów Instytutów do WSZJK płyną informacje na temat trudności dyplomantów w odpowiedzi na pytania egzaminacyjne.

Opis udziału interesariuszy wewnętrznych i zewnętrznych w procesie określania i weryfikacji zakładanych efektów uczenia się

Zmiany efektów uczenia się lub chęć wprowadzenia nowych efektów uczenia się mogą być zgłaszane przez studentów, pracowników lub przedstawicieli przedsiębiorstw ICT pracownikom WIiT, którzy przekazują propozycje zespołowi WSZJK. Taka forma zgłaszania zmian jest postulowana przez WZJK.

Zespół rozważa zasadność propozycji (w przypadkach dużej wagi w obecności osób zainteresowanych), analizuje jej wykonalność i przedstawia swoją opinię Kolegium Dziekańskiemu, na którym po dyskusji Dziekan podejmuje decyzję o dalszym toku sprawy. Propozycja może zostać odrzucona, przekazana do uszczegółowienia na drodze dalszych rozmów zainteresowanych osób, mogą zostać zaproponowane zmiany w treści przedmiotów, których efekty uczenia się dotyczą, ewentualnie mogą zostać sporządzone wnioski do Rady Wydziału o zmiany w programie studiów.

Opis zapobiegania zjawiskom patologicznym, związanym z procesem kształcenia

Zjawiska patologiczne związane z procesem kształcenia mogą występować z powodu studentów lub pracowników.

Z powodu studentów możemy mieć do czynienia przede wszystkim z:

- Nieusprawiedliwioną nieobecnością na zajęciach.
- Odpisywaniem w trakcie egzaminów/kolokwiów.
- Niewykonaniem lub wykonaniem niesamodzielnym zadań domowych/ projektów/symulacji/programów.
- Plagiatem lub niesamodzielnym wykonaniem pracy dyplomowej. Zapobieganie:
- Studenci są informowani na początku każdego przedmiotu o obowiązku obecności na zajęciach. Prowadzący sprawdzają obecność na każdych ćwiczeniach i laboratoriach. Regulamin Studiów precyzuje sankcje za nieobecność na zajęciach. Obecność na wykładach sprawdzana jest wyrywkowo zależnie od woli prowadzącego wykład.
- Odpisywanie („ściąganie") w trakcie egzaminów lub kolokwiów jest zabronione i kontrolowane przez prowadzących egzamin lub kolokwium. W większości przypadków udowodnienie niesamodzielnego wykonywania pracy kończy się oceną niedostateczną.
- Samodzielność wykonywania pracy dyplomowej jest kontrolowana przez sprawdzanie postępów realizacji pracy dyplomowej. Kontrolę taką przeprowadza promotor pracy, który ma obowiązek spotykać się z studentem co najmniej przez liczbę godzin wynikającą z przydziału godzin dydaktycznych dla promotora pracy. Systematyczność pracy studenta jest także sprawdzana w trakcie seminarium dyplomowego, w trakcie którego student ma obowiązek kilkakrotnego

prezentowania kolejnych wyników i postępów w pisaniu pracy prowadzącemu seminarium oraz pozostałym uczestnikom seminarium.

Z winy pracowników możemy mieć do czynienia z:

- Niepełną realizacją programu i treści danego przedmiotu, ich niewystarczającym poziomem lub nieatrakcyjnym sposobem jej przedstawienia, co może wiązać się z niepełną realizacją przedmiotowych i kierunkowych efektów uczenia się.
- Nieobyczajnym zachowaniem w stosunku do studentów.
- Nieusprawiedliwioną nieobecnością na zajęciach lub spóźnianiem się na zajęcia.
- Niesprawiedliwym ocenianiem prac i egzaminów studenckich.

Zapobieganie:

- Na WIiT obowiązuje bezwzględny zakaz podważania poziomu intelektualnego studentów przez lekceważące pytania. Pracownik może oceniać studenta tylko na podstawie pracy, którą student przedstawił do oceny, stosując obowiązującą w Uczelni skalę ocen. Słowne złośliwości poniżające studenta są zakazane i są tępione przez władze Wydziału.
- Obecność pracowników na zajęciach jest sprawdzana przez dziekanat, dyrektorów instytutów i Dział Audytu PP. Studenci mają obowiązek zgłoszenia nieobecności prowadzącego zajęcia do dziekanatu, który wyjaśnia powód braku zajęć w danym terminie i wyznacza termin odrobienia zajęć.

Osoba oceniająca egzamin, kolokwium lub jakąkolwiek pracę studenta ma obowiązek wyjaśnić studentowi, co jest przyczyną wystawionej oceny. Student, który nie zgadza się z oceną ma prawo zwrócić się do przełożonego pracownika, który postawił niesprawiedliwą, zdaniem studenta, ocenę o weryfikację tej oceny. Przy dalszej niezgodności opinii student może odwołać się do prodziekana lub dziekana, którzy mają obowiązek sprawę wyjaśnić.

3. Opis prowadzonej działalności naukowej w dyscyplinie lub dyscyplinach

Instytut Informatyki Politechniki Poznańskiej to prężnie działające centrum badawcze, gdzie prowadzone są innowacyjne prace badawcze w obszarze sztucznej inteligencji, obliczeń ewolucyjnych, uczenia maszynowego, inżynierii oprogramowania oraz analizy danych.

Jednym z ważnych kierunków jest rozwój algorytmów ewolucyjnych i metaheurystyk – od opracowywania reprezentacji genetycznych dla złożonych problemów optymalizacyjnych po automatyczną syntezę programów. Badacze zajmują się również sterowaniem preferencjami i konstrukcją wielokryterialnych algorytmów optymalizacyjnych. Ważny element tej działalności stanowi też uczenie maszynowe, obejmujące optymalizację ciągłą i kombinatoryczną, a także zaawansowane techniki, takie jak uczenie głębokie, aktywne, ze wzmocnieniem czy przyrostowe. Zagadnienia te znajdują zastosowanie m.in. w rozpoznawaniu obrazów, opracowywaniu klasyfikatorów złożonych czy analizie danych niezbalansowanych i niekompletnych.

Instytut ma bogate doświadczenie w optymalizacji transportu, logistyki czy zarządzania produkcją, jak również w optymalizacji aplikacji internetowych, w tym rozwiązań e-commerce i metod dostarczania treści. Prace naukowe obejmują optymalizację ewolucyjną, programowanie genetyczne oraz inne metaheurystyki. Ważnym zagadnieniem jest także szeregowanie zadań w różnorodnych systemach obliczeniowych: od systemów wieloprocesorowych i obliczeń równoległych na superkomputerach po szeregowanie on-line w warunkach zmieniającej się dostępności zasobów. W obszarze inżynierii oprogramowania zespoły badawcze rozwijają zwinne metodyki wytwarzania, metody inżynierii wymagań, pielęgnacji oprogramowania czy szacowania pracochłonności. Eksplorowane są też aspekty automatyzacji działań programistycznych (ang. automated software engineering) i programowania dla użytkowników końcowych (ang. end-user programming). Równolegle prowadzone są prace nad programowaniem współbieżnym, rozproszonym i równoległym, w tym nad rozproszoną pamięcią transakcyjną, ostatecznie spójną replikacją czy synchronizacją deklaratywną. Ważną rolę odgrywają tu bezpieczne abstrakcje i języki

programowania oraz automatyczna weryfikacja programów.
Zespoły Instytutu opracowują i doskonalą metody wielokryterialnego oraz grupowego podejmowania decyzji, także w warunkach ryzyka i niepewności. Szczególne miejsce zajmuje modelowanie preferencji (m.in. z zastosowaniem odpornej regresji porządkowej) oraz optymalizacja wielokryterialna. Rozwijane są też kliniczne systemy wspomagania decyzji, wspierające personel medyczny w diagnozach i wyborze metod terapii.
Badacze z Instytutu intensywnie działają w obszarze Big Data, analizy danych oraz eksploracji sieci społecznościowych. Opracowywane są metody eksploracji strumieni danych, analizy danych przestrzennych, grafów, szeregów czasowych i informacji z WWW. Prowadzone prace dotyczą też systemów rekomendacyjnych i wykrywania anomalii (np. nadużyć) w dużych zbiorach danych. W ramach badań nad informatyką społeczną analizowane są mechanizmy rozprzestrzeniania się informacji w sieciach społecznościowych oraz wpływ zjawisk społecznych na działanie systemów informatycznych.
Ważną częścią działalności Instytutu jest projektowanie i optymalizacja hurtowni danych oraz procesów ETL/ELT, a także zarządzanie ewolucją ich architektury. Realizowane są projekty z zakresu analityki biznesowej (m.in. dla Big Data), opracowywane są metody analizy danych sekwencyjnych punktowych i interwałowych. Zagadnienia te łączą się z inżynierią wymagań dla systemów klasy BI, by opracowywać rozwiązania wydajne i łatwe w utrzymaniu.
W obszarze bioinformatyki prowadzone są badania nad analizą danych biomedycznych i sekwencjonowaniem nowej generacji (NGS). Ważne zagadnienia obejmują modelowanie i analizę złożonych systemów biologicznych, a także wykorzystanie grafów i sieci w biologii. Zespoły naukowe zajmują się również złożonością obliczeniową problemów biologicznych oraz obliczeniami kwantowymi, gdzie analizowana jest teoretyczna strona algorytmów i potencjał komputerów DNA.
Oprócz wysoce specjalistycznych dziedzin, Instytut rozwija również podstawowe zagadnienia związane z logiką obliczeniową, algorytmami i strukturami danych, metodami probabilistycznymi czy architekturą systemów komputerowych. Naukowcy zajmują się także badaniami operacyjnymi, elementami analizy numerycznej oraz komunikacją człowiek–komputer. W obszarze zastosowań praktycznych istotne miejsce zajmują systemy wbudowane, aplikacje mobilne czy przetwarzanie języka naturalnego.

Instytut Sieci Teleinformatycznych to dynamiczne centrum badań, w którym naukowcy koncentrują się na najnowszych technologiach telekomunikacyjnych i teleinformatycznych. Ich prace obejmują między innymi cyberbezpieczeństwo, sieci szerokopasmowe, Internet Rzeczy, sieci definiowanych programowo, elastyczne sieci optyczne i teorię ruchu. W ramach działalności dydaktycznej czternastoosobowy zespół ekspertów prowadzi zajęcia, które nie tylko wprowadzają w podstawowe zasady technologii sieciowych, ale również dogłębnie omawiają złożoność architektury sieci, protokołów, sterowania, realizacji oraz ekonomicznych aspektów teleinformatyki.

Naukowcy z Instytutu odegrali kluczową rolę w projekcie PO IG Inżynieria Internetu Przyszłości. Celem tego przedsięwzięcia było przygotowanie metodyki stopniowego zastępowania obecnej wersji IP (IPv4) protokołem IPv6 oraz opracowanie nowych usług i rozwiązań sieciowych możliwych dzięki IPv6. Równolegle, w ramach zagadnień związanych z Internetem Przyszłości, zespół zaproponował i przetestował innowacyjną architekturę opartą na wirtualizacji zasobów – uzupełnioną o nowe mechanizmy i algorytmy niezbędne do sprawnego funkcjonowania przyszłych sieci.
Projekt zakładał również budowę krajowego środowiska testowego dla Internetu IPv6 i Internetu Przyszłości, tworząc unikalną platformę badawczo-rozwojową, w której eksperymentalna weryfikacja pomysłów pozwala na szybkie wdrażanie nowatorskich rozwiązań. Dzięki zaangażowaniu Instytutu Sieci Teleinformatycznych Polska ma szansę stać się liderem we wprowadzaniu i rozwijaniu

przyszłościowych technologii sieciowych. Dzięki wsparciu finansowemu projektu, powstało laboratorium, w którym ciągle prowadzone są badania w obszarze sieci komputerowych, w tym sieci definiowanych programów.

Instytut Sieci Teleinformatycznych od wielu lat prowadzi zaawansowane badania nad algorytmami i protokołami routingu, a także nad wpływem różnych topologii sieci na ich efektywność. Równocześnie, istotnym obszarem zainteresowań pozostają mechanizmy zarządzania siecią – w tym zarządzanie mobilnością oraz adresacją, jak również zagadnienia związane z przepływami ruchu, rezerwacją i priorytetyzacją połączeń. W ramach prac nad sieciami komórkowymi zespół opracował modele rezerwacji zasobów, priorytetów, a także mechanizmy przenoszenia połączeń i przelewu ruchu, korzystając z metod progowych i bezprogowych kompresji przepływności.

W obszarze cyberbezpieczeństwa badania naukowe prowadzone są w wielu kierunkach. Jednym z kierunków jest analiza stanu urządzeń IoT w celu ich uwierzytelniania oraz wykrywania ich podatności na ataki. Wykorzystuje się tutaj zaawansowane narzędzia kryptograficzne oraz analizę dostępnych publicznie baz danych zawierających informacje o znanych podatnościach. Drugim kierunkiem badań w obszarze cyberbezpieczeństwa jest wykorzystanie funkcji sieci definiowanych programowo SDN (Software Defined Network) do implementacji mechanizmów ochrony przez cyberatakami przez ciągłe przemieszczanie celu ataku. Technika ta, zwaną techniką MTD (Moving Target Defense), ma na celu przerwanie łańcucha cyberataku już na samy jego początku, to znaczy na rekonesansie.

Badania Instytutu koncentrują się także na właściwym wymiarowaniu zasobów sieciowych. Dzięki długoletniej współpracy z operatorami sieci komórkowych opracowano modele interfejsów oraz specjalistyczne oprogramowanie wspierające proces optymalizacji i planowania sieci. W sferze sieci IP, pracownicy Instytutu skupiają się na analizie właściwości strumieni ruchu i tworzą efektywne metody przechwytywania oraz modelowania dużych wolumenów transmisji pakietowej. Równie ważne są dla nich zagadnienia bezpieczeństwa zarówno w sieciach przewodowych, jak i bezprzewodowych – zespół prowadzi tu szczegółową analizę bezpieczeństwa urządzeń stosowanych w sieciach IP.

Obok prac naukowo-badawczych Instytut aktywnie angażuje się w kształcenie podyplomowe oraz szkolenia. Oferowane studia podyplomowe koncentrują się na obszarach:

- Bezpieczeństwo Sieci Komputerowych,
- Projektowanie i utrzymanie sieci Carrier Ethernet,
- Sieci komputerowe: urządzenia i protokoły.

Tak szeroka oferta dowodzi wysokich kompetencji zespołu Instytutu w dziedzinie nowoczesnych sieci komputerowych i telekomunikacyjnych. Dodatkowo, w Instytucie działają tzw. akademie – kursy szkoleniowe z zakresu sieci komputerowych, telekomunikacyjnych i zagadnień pokrewnych. Są to:

- Akademia Sieci Cisco – powstała w 2002 roku i obecnie jest największym ośrodkiem tego typu w Wielkopolsce. Realizuje autoryzowane szkolenia w ramach programu Cisco Networking Academy Program (CNAP), który dzieli się na 7 semestrów. Pierwsze cztery semestry przygotowują do zdobycia certyfikatu CCNA, natomiast kolejne trzy – do egzaminów CCNP. Uczestnicy programu zyskują wiedzę teoretyczną i umiejętności praktyczne, m.in. dzięki licznym ćwiczeniom laboratoryjnym i materiałom multimedialnym. Całość jest regularnie aktualizowana, by odzwierciedlać najnowsze trendy w branży.
- Akademia Huawei – uruchomiona w 2016 roku w następstwie podpisania przez Rektora Politechniki Poznańskiej, prof. dr. hab. inż. Tomasza Łodygowskiego, umowy w obecności prezydentów Rzeczypospolitej Polskiej i Chińskiej Republiki Ludowej. Jej misją jest kształcenie w zakresie sieci telekomunikacyjnych i komputerowych na bazie technologii Huawei – jednej z kluczowych firm tej branży na świecie.
- Akademia Palo Alto - to inicjatywa edukacyjna, która ma na celu kształcenie studentów i specjalistów w zakresie nowoczesnych rozwiązań bezpieczeństwa sieciowego. W ramach

programu uczestnicy zdobywają praktyczne umiejętności konfigurowania i zarządzania zaawansowanymi systemami firewall oraz uczą się, jak chronić infrastrukturę IT przed współczesnymi zagrożeniami cybernetycznymi. Ukończenie akademii Palo Alto może pomóc w zdobyciu certyfikatów branżowych, ułatwiając wejście na rynek pracy w sektorze cyberbezpieczeństwa. Jest to także doskonała okazja do budowania sieci kontaktów z doświadczonymi;

- Akademia Check Point pozwala poznać studentom, jak również specjalistom, najnowsze technologie i rozwiązania z zakresu bezpieczeństwa sieciowego oferowane przez firmę Check Point. Program obejmuje zarówno zagadnienia teoretyczne, jak i praktyczne ćwiczenia w laboratoriach, podczas których uczestnicy uczą się konfigurować i zarządzać platformą bezpieczeństwa Check Point, w tym zaawansowanymi funkcjami zapór sieciowych, zapobiegania włamaniom (IPS) czy ochrony przed atakami typu zero-day.
  Współpraca Instytutu z Check Point zapewnia uczestnikom dostęp do materiałów dydaktycznych i środowisk zbliżonych do rzeczywistych warunków pracy. Akademia umożliwia ponadto zdobycie cenionych na rynku certyfikatów (takich jak CCSA czy CCSE), co znacznie ułatwia rozpoczęcie kariery w sektorze cyberbezpieczeństwa. Dzięki praktycznym warsztatom i możliwości wymiany doświadczeń z ekspertami, studenci mają unikatową okazję do rozwijania umiejętności odpowiadających wymaganiom współczesnych pracodawców.

Dzięki tak zróżnicowanym działaniom w obszarze badań, rozwoju i kształcenia Instytut Sieci Teleinformatycznych nie tylko kształtuje przyszłość nowoczesnych technologii sieciowych, ale też aktywnie wspiera kadrę inżynierską w Polsce, zapewniając jej narzędzia i wiedzę niezbędną do wdrażania innowacyjnych rozwiązań w branży teleinformatycznej.

W **Instytucie Radiokomunikacji** badania naukowe, prowadzone wśród szerokiej innej tematyki badawczej, a istotne dla tematyki teleinformatycznej, obejmują następujące zagadnienia:

- systemy i sieci komórkowe, w szczególności dostęp radiowy do sieci danych za ich pomocą,
- sieci WiFi i ich rozwój,
- metody symulacji cyfrowej.

W zakresie badań nad przyszłymi sieciami komórkowymi zespół Instytutu Radiokomunikacji specjalizuje się w pracach nad warstwą fizyczną oraz warstwą dostępu do mediów (MAC - Medium Access Control) oraz zastosowaniem kodowania sieciowego – nowej techniki powiększania przepustowości sieci, w szczególności bezprzewodowych. W tej dziedzinie pracownicy Instytutu biorą udział w projektach finansowanych przez Unię Europejską, realizowanych przez konsorcja składające się z najlepszych globalnych firm sektora telekomunikacyjnego (np. Ericsson, Alcatel-Lucent, Nokia, Nokia Networks, Huawei, DoCoMo Labs, Deutsche Telekom, France Telecom, Telecom Italia, Telefonica i wybranych uczelni wyższych z UE). W dyspozycji zespołu Instytutu jest najnowsza wiedza i wyniki naukowe dotyczące przyszłych systemów komórkowych (tzw. piątej generacji - 5G), które aktualnie są standaryzowane i będą wdrażane do działania po roku 2020. Wśród tych systemów są również tak zwane systemy o szczególnie wysokiej niezawodności (URC - Ultra Reliable Communications), które aktualnie są przedmiotem badań realizowanych zgodnie z umową z firmą Nokia Networks i które wiążą się z planowanym systemem łączności między pojazdami oraz z systemami działającymi w sytuacjach krytycznych, przy częściowo zniszczonej infrastrukturze. W ramach projektu PO IG Inżynieria Internetu Przyszłości zajmowano się wieloskokowymi sieciami komputerowymi. W wyniku tych badań w Instytucie wytworzono tzw. testbed – ponad 40-węzłową sieć wieloskokową. W przyszłym Internecie jednym z trybów komunikacji będzie masowa wymiana danych pomiędzy urządzeniami (Machine-to-Machine Communications), co jest również przedmiotem badań. Kolejnym przedmiotem zainteresowań umiejscowionych na styku radiokomunikacji i informatyki są aplikacje na urządzenia mobilne. Tematyka ta jest zarówno przedmiotem badań, jak i pracy dydaktycznej. Ściśle z techniką systemów

radiokomunikacji ruchomej wiążą się również zagadnienia tak zwanego radia kognitywnego, czyli tego rodzaju transmisji cyfrowej za pomocą fal radiowych, w którym wykorzystuje się chwilowo wolne zakresy częstotliwości. Oprócz zagadnień czysto telekomunikacyjnych, mamy w tej dziedzinie do czynienia z tematyką optymalizacji, rozdziału zasobów, teorii gier i podobnych zagadnień istotnych również w teleinformatyce.
W ostatnim okresie w Instytucie Radiokomunikacji prowadzone są również badania dla polskiego przemysłu obronnego powiązane z komunikacją z bezzałogowymi statkami powietrznymi o zastosowaniach wojskowych i cywilnych. Konstruowane są więc i uruchamiane łącza transmisji danych według własnych projektów.
W Instytucie Radiokomunikacji prowadzone są również badania na temat sieci WiFi i ich udoskonaleń a także zapewnienia bezpieczeństwa transmisji w takich sieciach. Prowadzone prace mają na celu podniesienie szybkości transmisji, ulepszenie odbiorników i metod wielodostępu na zasadzie współzawodnictwa dostępu do medium transmisyjnego, którym jest kanał w pasmie 2.4 GHz lub w innym zakresie wykorzystywanym w nowych standardach serii IEEE 802.11. Wynikiem prac nad sieciami WiFi jest szereg wartościowych publikacji.
Symulacja cyfrowa jest potężnym narzędziem badawczym w wielu dziedzinach nauki i techniki, w tym również w teleinformatyce. W Instytucie Radiokomunikacji do realizacji poważnych badań symulacyjnych niezbędnych w projektach UE oraz we współpracy z przemysłem (np. z firmą Nokia Networks) zbudowano i oprogramowano klaster komputerowy, który pozwala na równoczesną realizację prawie trzystu przebiegów symulacyjnych. Sama metodyka symulacji cyfrowych jest przedmiotem kompetencji pracowników Instytutu i była również przedmiotem publikacji w formie rozdziału w książce opublikowanej w międzynarodowym wydawnictwie o światowej renomie.

W **Instytucie Telekomunikacji Multimedialnej** prowadzone są badania naukowe w wielu obszarach:

- Nowe techniki kompresji sygnałów wizyjnych

Przesyłanie sygnałów obrazu ruchomego stanowi ok. 70% ruchu w światowych sieciach teleinformatycznych. Ten udział rośnie każdego roku i dlatego badania dotyczące kompresji obrazów ruchomych są jednym z najbardziej istotnych obszarów badań w zakresie teleinformatyki. W Instytucie prowadzi się badania obejmujące: zaawansowane techniki adaptacyjnego kontekstowego kodowania arytmetycznego, metody szybkiego wyboru trybów predykcji wewnątrzobrazowej i międzyobrazowej, metody szybkiej predykcji wektorów ruchu, techniki szybkiej predykcji rozmiaru jednostek kodowania i ich podziałów, nowe metody predykcji międzyobrazowej z wykorzystaniem złożonych modeli ruchów, techniki transkodowania homogenicznego strumieni wizyjnych HEVC, techniki transkodowania heterogenicznego strumieni AVC i HEVC, elementy techniki kompresji będącej następcą techniki opisanej w normie HEVC. Prace prowadzone są we współpracy międzynarodowej rozpoczętej projektami badawczym NATO i 5. Programu Ramowego UE. Obecnie współpraca odbywa się w ramach koordynującej badania naukowe grupy ekspertów MPEG (Moving Picture Experts Group) działającej pod auspicjami ISO i IEC.

- Kompresja ruchomych obrazów przestrzennych

W badaniach zespołu szczególną rolę odgrywają prace w zakresie nowych metod kompresji obrazów przestrzennych i wielowidokowych. Obecnie prowadzi się prace dotyczące kompresji obrazów wielowidokowych uzyskiwanych z kamer o dowolnych położeniach. Takie badania są istotne dla przesyłania i przechowywania reprezentacji scen przestrzennych. Już udało się uzyskać bardzo ciekawe wyniki pozwalające poprawić efektywność kompresji najnowocześniejszej znanej na świecie techniki 3D-HEVC. W ramach tej tematyki zrealizowano dwa projekty OPUS oraz dwa projekty PRELUDIUM.

- Obrazy ruchome swobodnego punktu widzenia i wirtualna rzeczywistość

Celem badań jest budowa efektywnego praktycznego systemu złożonego ze sprzętu i

oprogramowania, który widzowi połączonemu przez Internet będzie dawał możliwość wirtualnego przemieszczania się wokół sceny oraz wchodzenia w samą scenę. Takie interaktywne systemy mogą w przyszłości znaleźć zastosowanie w przekazie relacji z zawodów sportowych (np. koszykówka, siatkówka, boks, zapasy, judo), przedstawień teatralnych oraz różnych inscenizacji artystycznych. Systemy mogą służyć także celom dydaktycznym (interaktywne kursy, interaktywny instruktaż). Zespół jest jednym z wiodących na świecie ośrodków badań w tej dziedzinie i może się poszczycić wieloma ciekawymi wynikami dotyczącymi budowy takiego systemu. Obecne prace obejmują głównie następujące zagadnienia: estymacja głębi, korekcja geometryczna i kolorymetryczna obrazów wielowidokowych, szybka kalibracja scen przestrzennych, synteza widoków wirtualnych, synteza wirtualnego pola dźwięku, obiektowe przetwarzanie audiowizualnych scen przestrzennych.

- Automatyczna analiza obrazu

Od wielu lat prowadzi się prace dotyczące segmentacji sekwencji wizyjnych, ekstrakcji cech z obrazów ruchomych i nieruchomych, analizy obrazów stereoskopowych oraz analizy wysokiego poziomu dokonywanej dla obrazów ruchomych jedno- i wielokamerowych. Badania te prowadzone są przede wszystkim pod kątem zastosowania w inteligentnych systemach dozoru wizyjnego, systemach bezpieczeństwa, systemach pomiarowych oraz w przemysłowych systemach wizji komputerowej.

- Systemy multimedialne

W Instytucie prowadzone są prace badawcze dotyczące systemów multimedialnych, w tym telewizji internetowej. W szczególności zrealizowano duży projekt dotyczący bezpieczeństwa w sieciach hotelowych, w którego ramach zrealizowano m in. oryginalną technikę pozwalającą wyszukiwać w Internecie nielegalne kopie filmów.

- Systemy wbudowane

Badania dotyczą systemów wbudowanych i systemów w układzie (SoC – System on Chip) i są prowadzone przede wszystkim pod kątem programowania złożonych układów wykonywanych w technice FPGA. Osiągnięto ciekawe wyniki dotyczące projektowania systemów wbudowanych z wykorzystaniem sieci w układach (NoC – Network on Chip). W tym zakresie wykonano projekt celowy MNiSW. W roku 2014 zrealizowano dla wielkiej chińskiej firmy Huawei duży projekt badawczy dotyczący budowy systemu przetwarzania obrazów stereoskopowych z wykorzystaniem programowania układów FPGA.

- Szerokopasmowa transmisja sygnałów i kompatybilność elektromagnetyczna w systemach cyfrowych

Prace dotyczą modelowania szerokopasmowej transmisji sygnałów za pomocą fal radiowych oraz obliczeń elektromagnetycznych w połączeniach złożonych układów cyfrowych. Badania prowadzi się w kontekście przesyłania i przetwarzania sygnałów cyfrowych o bardzo dużej prędkości transmisji.

4. Opis kompetencji oczekiwanych od kandydata ubiegającego się o przyjęcie na studia

Od kandydatów ubiegających się na kierunek cyberbezpieczeństwo oczekuje się zainteresowania zagadnieniami technicznymi, szczególnie związanymi z informatyką i teleinformatyką, zaangażowania we wszystkich wymaganych programem studiów działaniach, pomysłowości i otwartości na nowe technologie, a także aktywności w innych obszarach życia studenckiego (w kołach naukowych rozwijających indywidualne zainteresowania, predyspozycje oraz zdolności studenta, a także w organizacjach studenckich i sekcjach sportowych). Rekrutacja na studia pierwszego stopnia na kierunek *cyberbezpieczeństwo* o profilu ogólnoakademickim odbywać się będzie zgodnie z ogólnymi zasadami rekrutacji podanymi w Uchwale Senatu PP nr 185 z dnia

24 kwietnia 2024r. w sprawie warunków i trybu przyjmowania na studia w roku akademickim 2025/2026.

Rekrutacja na pierwszy rok studiów odbywa się na podstawie wyników egzaminu maturalnego (konkurs świadectw), a liczbę punktów „W" w rankingu świadectw określa się poniższym wzorem na podstawie świadectwa maturalnego:

$$W = 0{,}5\ J_P + 0{,}5\ J_O + 2{,}5\ M + 2\ X$$

gdzie dla tzw. „nowej matury":

J_P – liczba punktów odpowiadająca procentowemu wynikowi pisemnego egzaminu maturalnego z języka polskiego na poziomie podstawowym,

J_O – liczba punktów odpowiadająca procentowemu wynikowi pisemnego egzaminu maturalnego z języka obcego nowożytnego na poziomie podstawowym; w przypadku zdawania egzaminu z dwóch języków wybierany jest wynik korzystniejszy dla kandydata,

$$M = M_{PODST} + M_{ROZ}$$

M_{PODST} – liczba punktów odpowiadająca procentowemu wynikowi egzaminu maturalnego z matematyki na poziomie podstawowym,

M_{ROZ} – liczba punktów odpowiadająca procentowemu wynikowi egzaminu maturalnego z matematyki na poziomie rozszerzonym (0 w przypadku niezdawania egzaminu),

$$X = X_{PODST} + X_{ROZ}$$

X_{PODST} – liczba punktów odpowiadająca procentowemu wynikowi egzaminu maturalnego z biologii, chemii, fizyki/fizyki i astronomii lub informatyki na poziomie podstawowym (wynik korzystniejszy dla kandydata z uwzględnieniem, że X_{ROZ} odnosi się do tego samego przedmiotu;
0 – w przypadku niezdawania egzaminu z żadnego z tych przedmiotów),

X_{ROZ} – liczba punktów odpowiadająca procentowemu wynikowi egzaminu maturalnego z biologii, chemii, fizyki/fizyki i astronomii lub informatyki na poziomie rozszerzonym (wynik korzystniejszy dla kandydata z uwzględnieniem, że X_{PODST} odnosi się do tego samego przedmiotu;
0 – w przypadku niezdawania egzaminu z żadnego z tych przedmiotów).

Wynik egzaminu maturalnego w części pisemnej na poziomie podstawowym z przedmiotu, który zdawany był w części pisemnej na poziomie rozszerzonym lub na poziomie dwujęzycznym, ustala się następująco:

a) dla wyników w przedziale do 29%: $P_{PODST} = 2\ P_{ROZ}$,

b) dla wyników w przedziale od 30%: $P_{PODST} = 0{,}5\ P_{ROZ} + 50$,

gdzie:

P_{PODST} – wynik egzaminu maturalnego w części pisemnej z przedmiotu na poziomie podstawowym,

P_{ROZ} – wynik egzaminu maturalnego w części pisemnej z przedmiotu, który zdawany był na poziomie rozszerzonym lub na poziomie dwujęzycznym.

Za P_{PODST} przyjmuje się wynik korzystniejszy dla kandydata (wynik uzyskany na egzaminie maturalnym lub wynik wyliczony na podstawie powyższych wzorów), w przypadku gdy kandydat zdawał egzamin w części pisemnej zarówno na poziomie podstawowym i rozszerzonym lub dwujęzycznym.

Z pominięciem postępowania kwalifikacyjnego na I rok studiów przyjmowani są finaliści olimpiad stopnia centralnego, zgodnie z Uchwałą Senatu nr 44 z dnia 31 maja 2021r. Finaliści olimpiad zobowiązani są do dostarczenia zaświadczenia potwierdzającego status finalisty wydanego przez komitet organizacyjny danej olimpiady lub konkursu. Dla osób niepełnosprawnych (w rozumieniu ustawy z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych - Dz.U. z 2024 r., poz. 44, z późn. zm.) tworzy się dodatkowy 2% limit miejsc, nie mniejszy niż 2 miejsca na każdym kierunku studiów. Pozostałe, szczegółowe zasady rekrutacji znajdują się w Uchwale Senatu PP nr 185 z dnia 24 kwietnia 2024r.

Rekrutacja studentów zagranicznych przeprowadzana zostanie zgodnie z zasadami podanymi w zarządzeniu nr 11 Rektora Politechniki Poznańskiej z dnia 15 kwietnia 2024 (RO/IV/11/2024) w sprawie podejmowania studiów w Politechnice Poznańskiej przez osoby nie będące obywatelami polskimi w roku akademickim 2024/2025 lub zgodnie z zarządzeniem Rektora Politechniki Poznańskiej, które zostanie wydane w odniesieniu do rekrutacji na rok akademicki 2025/2026. Zasady te opisane są na stronie internetowej Politechniki Poznańskiej w zakładce „Kształcenie" – „Rekrutacja (I, II stopień)" – „Rekrutacja dla cudzoziemców" oraz na stronie Działu Współpracy Międzynarodowej. Dokumenty składane przez kandydatów-obcokrajowców sprawdzane są pod względem formalnym przez pracowników tego działu, a następnie oceniane przez Komisję Rekrutacji Cudzoziemców, w skład której wchodzą nauczyciele akademiccy oraz pracownicy administracyjni PP.

5. Przewidywany harmonogram realizacji programu studiów w poszczególnych semestrach i latach cyklu kształcenia.

Harmonogram realizacji programu studiów (O – ogółem, W – wykład, C – ćwiczenia, L – laboratorium, P – projekt, ECTS – liczba punktów ECTS, E – egzamin).
Nazwy profili: BST – Bezpieczeństwo Sieci Teleinformatycznych, BPD – Bezpieczeństwo Przetwarzania Danych, BKM – Bezpieczeństwo Komunikacji Multimedialnej.

Lp.	Nazwa przedmiotu	Liczba godzin					ECTS	E
		O	W	C	L	P		
SEMESTR I								
1.	Analiza matematyczna	60	30	30	-	-	5	Tak
2.	Algebra liniowa	60	30	30	-	-	5	Tak
3.	Wprowadzenie do programowania	60	30	-	30	-	5	Tak
4.	Teoria bezpieczeństwa i zarządzanie w sytuacjach kryzysowych	24	24	-	-	-	2	-
5.	Wprowadzenie do teleinformatyki	60	30	-	30	-	5	-
6.	Język obcy	30	-	30	-	-	2	-
6.a.	P.O. Język angielski							
6.b.	P.O. Język niemiecki							

7.	Zarządzanie projektami IT	30	15	-	-	15	2	-
8.	Wstęp do cyberbezpieczeństwa	60	30	-	-	30	4	-
9.	Wychowanie fizyczne	30	-	30	-	-	-	-
10.	Szkolenie biblioteczne	1	-	1	-	-	-	-
11.	Podstawowe szkolenie z zakresu BHP	4	4	-	-	-	-	-
	Razem w semestrze I:	**419**	193	121	60	45	30	3
SEMESTR II								
1.	Matematyka dyskretna	60	30	30	-	-	5	Tak
2.	Metody probabilistyczne	40	16	24	-	-	3	Tak
3.	Podstawy techniki cyfrowej	60	24	12	24	-	4	-
4.	*Programowanie skryptowe*	48	*24*	-	*24*	-	3	-
5.	Podstawy lokalnych sieci komputerowych	60	30	-	30	-	4	-
6.	Architektura komputerów i systemy operacyjne	60	30	-	30	-	5	-
7.	Język obcy	30	-	30	-	-	2	-
7.a.	P.O. Język angielski							
7.b.	P.O. Język niemiecki							
8.	Algorytmy i struktury danych	54	30	-	-	24	4	Tak
9.	Wychowanie fizyczne	30	-	30	-	-	-	-
	Razem w semestrze II:	**442**	184	126	108	24	**30**	**3**
SEMESTR III								
1.	Fizyka dla informatyków	70	30	16	24	-	5	Tak
2.	Statystyka	40	16	-	24	-	3	-
3.	Podstawy krytpografii	60	30	-	30	-	4	Tak
4.	Język obcy	30	-	30	-	-	2	-
4.a.	P.O. Język angielski							
4.b.	P.O. Język niemiecki							
5.	Podstawy rozległych sieci komputerowych	60	30	-	30	-	4	-
6.	Programowanie obiektowe	46	30	-	16	-	3	Tak
7.	Narzędzia informatyki	32	16	-	16	-	2	-
8.	Metody wirutalizacji	56	8		24	24	4	-
9.	Przedmiot obieralny w zakresie nauk o bezpieczeństwie	40	16	-	-	24	3	-
9.a.	Kompetencje globalne							
9.b.	Krajowe zasoby informacyjne							
	Razem w semestrze III:	**434**	176	46	164	48	**30**	**3**
SEMESTR IV								
1.	Wprowadzenie to mulitimediów	54	30	-	24	-	4	Tak
2.	Podstawy sztucznej inteligencji i uczenia maszynowego	54	30	-	24	-	4	Tak
3.	*Sieci i systemy bezprzewodowe*	54	30	-	*24*	-	*4*	-
4.	Informatyka śledcza	24	8	-	16	-	2	-
5.	*Podstawy usług i aplikacji chmurowych*	32	*16*	-	*16*	-	*2*	-
6.	*Język obcy*	30	-	*30*		-	*2*	Tak
6.a.	*Język angielski*							
6.b.	*Język niemiecki*							

7.	Podstawy IoT	48	16	-	24	8	3	-
8.	Podstawy projektowania aplikacji internetowych	48	16	-	16	16	3	-
9.	Podstawy projektowania aplikacji mobilnych	48	24	-	24	-	3	-
10.	Bazy danych i aplikacje bazodanowe	44	16	-	16	12	3	-
	Razem w semestrze IV:	**436**	186	30	184	36	30	3
	SEMESTR V							
1.	Przedmioty obieralne 5.X.1	56	24	-	16	16	4	Tak
5.BST.1	Bezpieczeństwo sieci LAN i WAN							
5.BPD.1	Synchronizacja							
5.BKM.1	Synchronizacja							
2.	Przedmioty obieralne 5.X.2	56	*24*	-	*16*	*16*	*4*	Tak
5.BST.2	Bezpieczeństwo systemów IoT i IIoT							
5.BPD.2	Bezpieczeństwo systemów IoT i IIoT							
5.BKM.2	Ochrona dostępu w rozproszonych systemach multimedialnych							
3.	*Przedmioty obieralne 5.X.3*	64	*24*	-	*24*	*16*	*5*	Tak
5.BST.3	Sieci definiowane programowo							
5.BPD.3	Sieci definiowane programowo							
5.BKM.3	AI w cyberbezpieczeństwie multimediów							
4.	*Wirtualna i rozszerzona rzeczywistość*	72	*24*	-	*24*	*24*	5	-
5.	Analiza złośliwego oprogramowania	76	16	-	30	30	5	-
6.	Testy penetracyjne	32	8	-	24	-	2	-
7.	Wprowadzenie do obliczeń kwantowych	32	16	-	16	-	2	-
8.	Wprowadzenie do białego wywiadu	46	16	-	-	30	3	-
	Razem w semestrze V:	**434**	152	-	150	132	**30**	**3**
	SEMESTR VI							
1.	Przedmioty obieralne 6.X.1	58	16	-	30	12	4	Tak
6.BST.1	Wykrywanie anomalii sieciowych i detekcja zagrożeń w sieci z wykorzystaniem AI							
6.BPD.1	Bezpieczeństwo systemów operacyjnych							
6.BKM.1	Techniki deepfake							
2.	Przedmioty obieralne 6.X.2	48	*24*	-	*24*	-	*3*	Tak
6.BST.2	Bezpieczeństwo systemów bezprzewodowych							
6.BPD.2	Bezpieczeństwo funkcjonalne i łańcuchów dostaw							
6.BKM.2	Techniki ochrony multimediów							
3.	Przedmioty obieralne 6.X.3	64	*24*	-	*24*	*16*	*4*	Tak
6.BST.3	Bezpieczeństwo w systemach chmurowych							
6.BPD.3	Bezpieczeństwo w systemach chmurowych							
6.BKM.3	Biometryczne uwierzytelnianie tożsamości							
4.	Przedmioty obieralne 6.X.4	48	*16*	-	*16*	*16*	*3*	-
6.BST.4	Podstawy analizy informacji							
6.BPD.4	Urządzenia programowalne							
6.BKM.4	Cyberkryminalistyka multimedialna							
5.	Bezpieczeństwo aplikacji internetowych	48	24	-	24	-	3	-
6.	Bezpieczeństwo aplikacji mobilnych	48	24	-	24	-	3	-

7.	Zarządzanie incydentami i bezpieczeństwo instytucji	32	16	-	-	16	2	-
8.	Seminarium przeddyplomowe	30		-	-	*30*	2	-
9.	Praktyka zawodowa	-	-	-	-	-	6	-
	Razem w semestrze VI:	**376**	144	0	142	90	**30**	**3**
SEMESTR VII								
1	Przedmioty obieralne 7.X.1	*72*	*24*	-	*24*	*24*	*5*	Tak
7.BST.1	Zarządzanie bezpieczeństwem sieci							
7.BPD.1	Bezpieczeństwo fizyczne systemów i urządzeń IT							
7.BKM.1	Bezpieczeństwo danych medycznych							
2	Przedmioty obieralne 7.X.2	*54*	*24*	-	-	*30*	*4*	Tak
7.BST.2	Bezpieczeństwo systemów bezzałogowych i satelitarnych							
7.BPD.2	Metody i zasady uwierzytelnienia							
7.BKM.2	Cyberbezpieczeństwo w mediach publicznych i społecznościowych							
3	Przedmioty obieralne 7..X.3	*58*	*16*	-	*30*	*12*	*4*	Tak
7.BST.3	Bezpieczeństwo systemów zarządzania bazami danych							
7.BPD.3	Bezpieczeństwo systemów zarządzania bazami danych							
7.BKM.3	Automatyzacja konfiguracji, utrzymania i testowania sieci systemów teleinformatycznych							
4	Przedmioty obieralne 7.X.4	*32*	16	-	16	-	2	-
7.BST.4	Systemy komunikacji kwantowej							
7.BPD.4	Systemy komunikacji kwantowej							
7.BKM.4	Zarządzanie i ochrona własności intelektualnej w multimediach							
5	Przedmioty obieralne o bezpieczeństwie instytucji i państwa	*32*	16	-	-	16	2	-
5.a	Bezpieczeństwo sektora finansowego							
5.b	*Bezpieczeństwo wewnętrzne*							
6	Przygotowanie pracy dyplomowej	-	-	-	-	-	10	-
7	Seminarium dyplomowe	*30*	-	-	-	30	2	-
8	Prace badawczo-wdrożeniowe	*16*	16	-	-	-	1	-
	Razem w semestrze VII:	**294**	112	-	70	112	**30**	**3**
	Razem:	**2835**	**1147**	**323**	**878**	**487**	**210**	**21**

6. Karty opisu przedmiotów (karty ECTS) są publikowane na stronie internetowej Politechniki Poznańskiej.