

RAMOWY PROGRAM PRAKTYK NA KIERUNKU INFORMATYKA

1. Podczas trwania praktyki student powinien zapoznać się z:

- profilem działalności i organizacją pracy w przedsiębiorstwie,
- zasadami BHP i p.poż.,
- zasadami zachowania tajemnicy służbowej i państwowej oraz ochrony poufności danych w zakresie określonym przez Organizatora praktyk
- organizacją pracy zespołów odpowiedzialnych za projektowanie, rozwój, wdrażanie lub utrzymanie systemów informatycznych,
- stosowanymi w organizacji metodami, narzędziami i technologiami wykorzystywanymi w realizacji przedsięwzięć informatycznych,
- obowiązującymi w organizacji zasadami i procedurami dotyczącymi wytwarzania, eksploatacji, utrzymania i dokumentowania systemów informatycznych,
- standardami, normami technicznymi i dobrymi praktykami właściwymi dla realizowanych w organizacji zadań informatycznych.

2. Praktyka powinna obejmować zadania umożliwiające studentowi zdobycie doświadczenia w wybranych obszarach ICT, zgodnie z jego indywidualnymi zainteresowaniami i potrzebami. Zakres wykonywanych prac powinien być spójny z Programem Studiów oraz dostosowany do profilu i specyfiki działalności instytucji przyjmującej.

Program praktyki może obejmować wybrane zagadnienia z zakresu:

- Inżynieria oprogramowania i rozwój systemów informatycznych, w tym:
 - analizy wymagań oraz udziału w przygotowaniu specyfikacji systemu,
 - projektowania architektury i komponentów systemów informatycznych,
 - implementowania, rozwijania i modyfikowania oprogramowania z wykorzystaniem odpowiednich technologii i narzędzi,
 - stosowania narzędzi wspierających zespołowe wytwarzanie oprogramowania,
 - testowania, diagnozowania błędów i poprawy jakości oprogramowania,

- udziału we wdrażaniu, utrzymywaniu i dokumentowaniu oprogramowania.
- Systemy komputerowe i infrastruktura ICT, w tym:
 - instalowania, konfigurowania i aktualizowania systemów operacyjnych oraz oprogramowania systemowego,
 - administrowania systemami i usługami systemowymi,
 - zarządzania użytkownikami, uprawnieniami i zasobami systemowymi,
 - monitorowania pracy systemów oraz diagnozowania i usuwania problemów eksploatacyjnych,
 - automatyzowania wybranych zadań administracyjnych,
 - udziału w utrzymaniu dostępności, niezawodności i dokumentacji systemów komputerowych.
- Sieci komputerowe i infrastruktura sieciowa, w tym:
 - projektowania, budowania i konfigurowania sieci komputerowych,
 - konfigurowania urządzeń i usług sieciowych,
 - administrowania sieciami przewodowymi i bezprzewodowymi,
 - monitorowania działania sieci i analizowania ruchu sieciowego,
 - diagnozowania i usuwania problemów związanych z komunikacją siecią,
 - udziału w utrzymaniu, zabezpieczaniu i rozwoju infrastruktury sieciowej.
- Bazy danych i zarządzanie danymi, w tym:
 - projektowania struktur i modeli danych,
 - tworzenia, rozwijania i modyfikowania baz danych,
 - realizowania operacji związanych z przetwarzaniem, wyszukiwaniem i modyfikowaniem danych,
 - monitorowania działania i wydajności systemów bazodanowych,
 - integrowania baz danych z aplikacjami i innymi systemami informatycznymi.
- Przetwarzanie i analiza danych, w tym:
 - pozyskiwania, przygotowywania, przetwarzania i porządkowania danych,
 - analizowania danych, sygnałów i obrazów na potrzeby realizowanych zadań i projektów,
 - tworzenia, testowania i oceny modeli uczenia maszynowego oraz wykorzystywania innych metod sztucznej inteligencji do rozwiązywania problemów praktycznych,
 - wizualizacji i prezentowania wyników analiz,

- integrowania komponentów analitycznych i rozwiązań AI z systemami informatycznymi.
- Systemy specjalizowane, w tym:
 - projektowania i implementowania oprogramowania dla urządzeń mobilnych, wbudowanych i IoT,
 - tworzenia i konfigurowania rozwiązań wykorzystujących urządzenia i komponenty systemów wbudowanych,
 - integrowania oprogramowania z urządzeniami, czujnikami i innymi elementami sprzętowymi,
 - realizowania komunikacji pomiędzy urządzeniami i komponentami systemów,
 - testowania, diagnozowania i optymalizowania działania systemów mobilnych, wbudowanych i IoT,
 - udziału we wdrażaniu i utrzymywaniu takich rozwiązań.
- Technologie interaktywne i multimedialne, w tym:
 - projektowania i implementowania interfejsów użytkownika,
 - stosowania zasad użyteczności, dostępności i projektowania uniwersalnego,
 - przygotowywania, przetwarzania i wykorzystywania elementów graficznych oraz multimedialnych w systemach informatycznych,
 - testowania interfejsów użytkownika oraz wprowadzania zmian wynikających z przeprowadzonej oceny,
 - udziału w projektowaniu i rozwijaniu interaktywnych oraz multimedialnych systemów informatycznych.
- Bezpieczeństwo systemów ICT i danych, w tym:
 - stosowania zasad bezpiecznej konfiguracji systemów, aplikacji i usług,
 - stosowania mechanizmów uwierzytelniania, autoryzacji i kontroli dostępu,
 - ochrony danych przechowywanych i przesyłanych,
 - identyfikowania podatności, błędów konfiguracji i innych zagrożeń bezpieczeństwa,
 - monitorowania zdarzeń i reagowania na incydenty zgodnie z procedurami organizacji,
 - stosowania dobrych praktyk bezpiecznego wytwarzania, utrzymywania i eksploatacji systemów.

Zakres praktyki nie musi obejmować wszystkich wskazanych obszarów. Dobór realizowanych zadań powinien wynikać ze specyfiki działalności Organizatora praktyk oraz umożliwiać studentowi zdobycie doświadczenia zawodowego związanego z kierunkiem studiów.

RAMOWY PROGRAM PRAKTYK NA KIERUNKU CYBERBEZPIECZEŃSTWO

1. Podczas trwania praktyki student powinien zapoznać się z:

- profilem działalności i organizacją pracy w przedsiębiorstwie/instytucji,
- zasadami BHP i p.poż.,
- zasadami zachowania tajemnicy służbowej i państwowej oraz ochrony poufności danych w zakresie określonym przez Organizatora praktyk,
- obowiązującymi w organizacji politykami i procedurami bezpieczeństwa informacji, w tym zasadami klasyfikacji informacji, zarządzania dostępem oraz postępowania z incydentami bezpieczeństwa,
- strukturą organizacyjną podmiotu w zakresie odpowiedzialności za bezpieczeństwo systemów ICT oraz rolę komórek/stanowisk odpowiedzialnych za cyberbezpieczeństwo,
- regulacjami prawnymi i standardami branżowymi właściwymi dla działalności Organizatora praktyk w obszarze cyberbezpieczeństwa (np. NIS2, DORA, RODO, ISO/IEC 27001, KSC).

2. Praktyka powinna obejmować zadania umożliwiające studentowi zdobycie doświadczenia w wybranych obszarach cyberbezpieczeństwa, zgodnie z jego indywidualnymi zainteresowaniami i potrzebami. Zakres wykonywanych prac powinien być spójny z Programem Studiów oraz dostosowany do profilu i specyfiki działalności instytucji przyjmującej.

Program praktyki może obejmować wybrane zagadnienia z zakresu:

- Bezpieczeństwo systemów i sieci komputerowych, w tym:
 - administrowania systemami operacyjnymi Linux i Windows z uwzględnieniem ich utwardzania oraz konfiguracji zabezpieczeń,
 - konfigurowania i zarządzania bezpieczeństwem sieci komputerowych, w tym segmentacji, VLAN, firewalli, systemów IDS/IPS oraz VPN,
 - monitorowania ruchu sieciowego i analizy protokołów pod kątem wykrywania anomalii i zagrożeń,

- zarządzania infrastrukturą sieciową z wykorzystaniem protokołów routingu i przełączania oraz automatyzacji konfiguracji,
- wdrażania i utrzymania mechanizmów ochrony przed zaawansowanymi zagrożeniami (np. NGFW, mikrosegmentacja),
- projektowania i wdrażania bezpiecznych architektur sieciowych z uwzględnieniem stref DMZ i segmentacji.
- Bezpieczeństwo środowisk chmurowych, wirtualnych i kontenerowych, w tym:
 - konfigurowania i zarządzania bezpieczeństwem środowisk chmurowych (IAM, polityki dostępu, szyfrowanie danych, segmentacja ruchu),
 - wdrażania i utrzymania środowisk zwirtualizowanych oraz kontenerowych z uwzględnieniem zasad bezpieczeństwa,
 - zarządzania cyklem życia kontenerów i obrazów kontenerowych oraz ich bezpieczeństwem,
 - stosowania podejścia Infrastructure as Code (IaC) z uwzględnieniem kontroli zmian i bezpieczeństwa konfiguracji,
 - monitorowania infrastruktury chmurowej i wykrywania zagrożeń z wykorzystaniem natywnych narzędzi chmurowych.
- Monitorowanie bezpieczeństwa i reagowanie na incydenty (Security Operations), w tym:
 - obsługi systemów klasy SIEM – zbierania, normalizacji i korelacji zdarzeń bezpieczeństwa,
 - analizy logów i detekcji anomalii z wykorzystaniem metod analitycznych i uczenia maszynowego,
 - prowadzenia triage alertów, klasyfikacji incydentów oraz ich eskalacji zgodnie z obowiązującymi procedurami,
 - wykorzystania narzędzi automatyzacji i orkiestracji reagowania na incydenty (SOAR),
 - stosowania threat intelligence w codziennej pracy analityka bezpieczeństwa,
 - tworzenia dashboardów i raportowania operacyjnego dla potrzeb SOC.
- Identyfikacja podatności i testowanie bezpieczeństwa, w tym:
 - prowadzenia rozpoznania pasywnego i aktywnego środowiska docelowego,
 - analizy podatności systemów, sieci i aplikacji z wykorzystaniem metodologii skanowania aktywnego i pasywnego,

- korzystania z baz podatności (CVE, NVD, Exploit-DB) oraz systemów oceny krytyczności (CVSS),
 - przeprowadzania testów penetracyjnych z zachowaniem uwarunkowań prawnych i etycznych,
 - dokumentowania wyników testów bezpieczeństwa oraz formułowania rekomendacji naprawczych,
 - zarządzania procesem obsługi podatności, w tym priorytetyzacji i śledzenia postępów naprawczych,
 - przeprowadzania testów bezpieczeństwa aplikacji, w tym analizy kodu i testów dynamicznych.
- Kryptografia i zarządzanie tożsamością, w tym:
 - stosowania mechanizmów kryptograficznych (funkcje skrótu, szyfrowanie symetryczne i asymetryczne, podpis cyfrowy),
 - wdrażania i utrzymania infrastruktury klucza publicznego (PKI) oraz zarządzania certyfikatami X.509,
 - konfigurowania mechanizmów uwierzytelniania wieloskładnikowego (MFA) oraz federacji tożsamości,
 - wdrażania modeli kontroli dostępu (RBAC, ABAC, DAC, MAC) oraz zasad Zero Trust,
 - zarządzania cyklem życia tożsamości użytkowników w systemach lokalnych i chmurowych,
 - monitorowania i audytu dostępu w kontekście wykrywania nadużyć.
 - Bezpieczeństwo baz danych i aplikacji, w tym:
 - wdrażania mechanizmów kontroli dostępu, uwierzytelniania i autoryzacji w systemach zarządzania bazami danych,
 - stosowania szyfrowania danych w spoczynku i w transmisji oraz zarządzania kluczami kryptograficznymi,
 - projektowania bezpiecznych schematów baz danych z uwzględnieniem separacji danych wrażliwych,
 - prowadzenia audytu i rejestrowania zdarzeń w bazach danych,
 - identyfikowania i przeciwdziałania podatnościom aplikacji webowych,
 - bezpiecznego projektowania i konsumpcji API oraz zarządzania sesjami użytkowników.

- Bezpieczeństwo systemów IoT i infrastruktury przemysłowej, w tym:
 - analizy podatności urządzeń IoT i systemów wbudowanych,
 - wdrażania mechanizmów bezpieczeństwa w systemach IoT z uwzględnieniem ograniczeń zasobowych,
 - bezpieczeństwa przemysłowych systemów sterowania (ICS/SCADA/OT) oraz konwergencji IT/OT,
 - stosowania standardów i dobrych praktyk bezpieczeństwa IoT,
 - uwzględniania implikacji IoT dla prywatności i ochrony danych osobowych.
- Analiza złośliwego oprogramowania i informatyka śledcza, w tym:
 - prowadzenia analizy statycznej i dynamicznej złośliwego oprogramowania,
 - stosowania narzędzi inżynierii wstecznej w analizie malware,
 - identyfikowania wskaźników kompromitacji (IoC) i powiązania ich z technikami ataków,
 - zabezpieczania cyfrowego materiału dowodowego z zachowaniem integralności i łańcucha dowodowego,
 - prowadzenia analizy powłamaniowej i rekonstrukcji przebiegu incydentów,
 - dokumentowania wyników analiz zgodnie ze standardami informatyki śledczej.
- Zarządzanie ryzykiem, audyt i zgodność regulacyjna, w tym:
 - przeprowadzania analizy ryzyka związanego z bezpieczeństwem informacji i systemów ICT,
 - uczestniczenia w procesach audytu bezpieczeństwa systemów teleinformatycznych,
 - stosowania standardów i norm z zakresu cyberbezpieczeństwa (ISO/IEC 27001, NIST CSF, COBIT),
- wdrażania wymagań regulacyjnych (NIS2, DORA, RODO, KSC) w praktyce organizacyjnej,
 - opracowywania i utrzymywania dokumentacji bezpieczeństwa (polityki, procedury, rejestry),
 - planowania ciągłości działania i odtwarzania po awarii (BCM/DR),
 - zarządzania zgodnością i podejściem GRC w organizacji.
- Sztuczna inteligencja i analityka danych w cyberbezpieczeństwie, w tym:
 - wykorzystania metod uczenia maszynowego do detekcji zagrożeń i identyfikowania wzorców anomalnych,

- stosowania narzędzi AI w automatyzacji procesów bezpieczeństwa,
 - analizy danych z różnych źródeł pod kątem wykrywania incydentów bezpieczeństwa,
 - wykorzystania narzędzi analitycznych i statystycznych do oceny ryzyka i prognozowania zagrożeń.
- Aspekty prawne, etyczne i społeczne cyberbezpieczeństwa, w tym:
 - stosowania przepisów prawa krajowego i unijnego w zakresie cyberbezpieczeństwa,
 - uwzględniania aspektów etycznych w działaniach ofensywnych i defensywnych,
 - przestrzegania zasad odpowiedzialnego ujawniania podatności,
 - rozumienia społecznych i środowiskowych uwarunkowań projektowania i eksploatacji systemów ICT,
 - stosowania zasad zrównoważonego rozwoju w kontekście bezpieczeństwa systemów informatycznych.

oraz innych pokrewnych dziedzin.

Zakres praktyki nie musi obejmować wszystkich wskazanych obszarów. Dobór realizowanych zadań powinien wynikać ze specyfiki działalności Organizatora praktyk oraz umożliwiać studentowi zdobycie doświadczenia zawodowego związanego z kierunkiem studiów.

**RAMOWY PROGRAM PRAKTYK NA KIERUNKU
DATA SCIENCE**

1. Podczas trwania praktyki student powinien zapoznać się z:

- profilem działalności i organizacją pracy w przedsiębiorstwie lub instytucji,
- rolą danych, analityki i systemów informatycznych w działalności organizacji,
- zasadami BHP i p.poż.,
- zasadami ochrony informacji, poufności i bezpieczeństwa danych oraz zachowania tajemnicy służbowej i państwowej w zakresie określonym przez Organizatora praktyk,
- podstawowymi zasadami prawnymi i etycznymi dotyczącymi pozyskiwania, przetwarzania, przechowywania i wykorzystywania danych, w tym danych osobowych,
- organizacją pracy zespołowej oraz stosowanymi w organizacji metodami realizacji projektów związanych z danymi.

2. Praktyka powinna obejmować zadania umożliwiające studentowi zdobycie doświadczenia w wybranych obszarach Data Science, zgodnie z jego indywidualnymi zainteresowaniami i potrzebami. Zakres wykonywanych prac powinien być spójny z Programem Studiów oraz dostosowany do profilu i specyfiki działalności instytucji przyjmującej.

Program praktyki może obejmować wybrane zagadnienia z zakresu:

- Pozyskiwanie, przygotowanie i zarządzanie danymi, w tym:
 - o pozyskiwania, gromadzenia, przygotowywania, przetwarzania i integracji danych pochodzących z różnych źródeł,
 - o czyszczenia danych, oceny ich jakości oraz przygotowywania zbiorów danych do dalszej analizy,
 - o projektowania, implementacji, obsługi i wykorzystywania baz danych, hurtowni danych oraz innych systemów przechowywania danych,

- o projektowania, tworzenia i rozwijania procesów ETL/ELT oraz potoków przetwarzania danych.
- Analiza danych i statystyka, w tym:
 - o eksploracyjnej analizy danych,
 - o stosowania metod statystycznych do analizy i interpretacji danych,
 - o oceny jakości danych, modeli i wyników analiz z wykorzystaniem odpowiednich metod, miar i narzędzi,
 - o tworzenia analiz, raportów oraz wizualizacji danych.
- Programowanie i inżynieria danych, w tym:
 - o programowania i automatyzacji procesów związanych z pozyskiwaniem, przetwarzaniem i analizą danych,
 - o przetwarzania danych wielkoskalowych,
 - o wykorzystywania rozwiązań chmurowych w projektach związanych z danymi,
 - o stosowania narzędzi, technologii i metodyk wykorzystywanych w realizacji projektów Data Science.
- Uczenie maszynowe i sztuczna inteligencja, w tym:
 - o projektowania, tworzenia, testowania i oceny modeli uczenia maszynowego oraz sztucznej inteligencji,
 - o wykorzystania metod uczenia głębokiego, przetwarzania języka naturalnego, analizy obrazów, sygnałów oraz innych danych nieustrukturyzowanych,
 - o wdrażania, integracji, monitorowania i utrzymywania modeli oraz rozwiązań wykorzystujących uczenie maszynowe i sztuczną inteligencję,
 - o wykorzystania danych i metod analitycznych do rozwiązywania problemów inżynierskich, technologicznych, naukowych lub biznesowych,
 - o optymalizacji i automatyzacji procesów z wykorzystaniem danych, metod statystycznych oraz narzędzi sztucznej inteligencji.
- Wizualizacja danych i komunikacja wyników, w tym:
 - o tworzenia raportów, dashboardów i wizualizacji danych,
 - o prezentowania wyników analiz,
 - o komunikowania wniosków odbiorcom technicznym i nietechnicznym,
 - o dokumentowania realizowanych prac.

- Realizacja projektów Data Science, w tym:
 - o pracy w interdyscyplinarnych zespołach realizujących projekty analityczne, informatyczne, badawczo-rozwojowe lub związane ze sztuczną inteligencją,
 - o doboru metod, algorytmów i technologii odpowiednich do charakteru realizowanych zadań,
 - o wykorzystywania danych i metod analitycznych do wspierania procesów decyzyjnych,
 - o udziału w projektowaniu, realizacji i rozwoju rozwiązań opartych na danych.
- Bezpieczeństwo, etyka i odpowiedzialne wykorzystanie danych, w tym:
 - o zapewnienia bezpieczeństwa i prywatności danych,
 - o stosowania zasad odpowiedzialnego wykorzystania danych i systemów sztucznej inteligencji,
 - o uwzględniania aspektów prawnych, etycznych i organizacyjnych związanych z przetwarzaniem danych,
 - o stosowania dobrych praktyk w zakresie zarządzania danymi oraz rozwoju systemów opartych na danych.

3. Praktyka powinna umożliwić studentowi wykorzystanie wiedzy i umiejętności zdobytych podczas studiów w rzeczywistym środowisku zawodowym oraz rozwijanie kompetencji inżynierskich, analitycznych i organizacyjnych.

W szczególności praktyka powinna sprzyjać rozwijaniu umiejętności:

- rozwiązywania rzeczywistych problemów z wykorzystaniem danych i odpowiednich narzędzi informatycznych,
- doboru metod, algorytmów i technologii odpowiednich do charakteru realizowanego zadania,
- krytycznej oceny danych, wyników analiz oraz stosowanych rozwiązań,
- samodzielnego zdobywania wiedzy i poznawania nowych technologii,
- pracy indywidualnej oraz współpracy w zespołach, w tym interdyscyplinarnych,
- dokumentowania wykonywanych prac oraz komunikowania wyników i wniosków,

- uwzględniania aspektów technicznych, biznesowych, prawnych, etycznych i społecznych związanych z wykorzystaniem danych i sztucznej inteligencji.

Zakres praktyki nie musi obejmować wszystkich wskazanych obszarów. Dobór realizowanych zadań powinien wynikać ze specyfiki działalności Organizatora praktyk oraz umożliwiać studentowi zdobycie doświadczenia zawodowego związanego z kierunkiem studiów.

**RAMOWY PROGRAM PRAKTYK NA KIERUNKU
MATEMATYKA STOSOWANA**

1. Podczas trwania praktyki student powinien zapoznać się:

- profilem działalności i organizacją pracy w przedsiębiorstwie,
- zasadami BHP i p.poż.,
- zasadami zachowania tajemnicy służbowej i państwowej oraz ochrony poufności danych w zakresie określonym przez Organizatora praktyk.

2. Praktyka powinna obejmować zadania rozwijające umiejętności matematyczne, informatyczne i statystyczne, co pozwoli absolwentowi na skuteczne odnalezienie się na rynku pracy w sektorach związanych z matematyką stosowaną, IT i nowoczesnymi technologiami. Zakres wykonywanych prac powinien być spójny z Programem Studiów oraz dostosowany do profilu i specyfiki działalności instytucji przyjmującej. Program praktyki może obejmować wybrane zagadnienia z zakresu:

- analityki danych, w tym
 - analizy i modelowania danych,
 - wykorzystywania narzędzi statystycznych,
 - analizy rynków finansowych, prognozowania trendów i oceny ryzyka,
 - pracy z dużymi zbiorami danych,
 - bezpieczeństwa danych,
 - wykorzystania metod uczenia maszynowego i sztucznej inteligencji do identyfikowania wzorców i prognozowania,
 - optymalizacji procesów biznesowych i innych,
- stosowania narzędzi matematyki wyższej do rozwiązywania realnych problemów biznesowych lub technologicznych, w tym
 - projektowania i optymalizacji systemów technicznych,
 - modelowania i symulacji matematycznej,
 - zastosowania algorytmów matematycznych,
- bankowości i finansów, w tym

- obsługi programów księgowych,
 - pomocy w sporządzaniu sprawozdań finansowych,
 - analizy i rozliczania kosztów,
- informatyki, w tym
 - projektowania i programowania aplikacji,
 - administrowania sieciami komputerowymi,
 - zarządzania bazami danych,
 - grafiki komputerowej,
 - multimediiów,
- działań edukacyjnych i popularyzujących matematykę, w szczególności w zastosowaniach w modelowaniu matematycznym,
- oraz innych pokrewnych dziedzin.

RAMOWY PROGRAM PRAKTYK NA KIERUNKU INFORMATYKA I EKONOMETRIA

1. Podczas trwania praktyki student powinien zapoznać się:

- profilem działalności i organizacją pracy w przedsiębiorstwie,
- zasadami BHP i p.poż.,
- zasadami zachowania tajemnicy służbowej i państwowej oraz ochrony poufności danych w zakresie określonym przez Organizatora praktyk.

2. Praktyka powinna także obejmować zadania rozwijające umiejętności techniczne, analityczne i menedżerskie, aby kompleksowo przygotować absolwentów do pracy w różnych obszarach biznesu i IT. Zakres wykonywanych prac powinien być spójny z Programem Studiów oraz dostosowany do profilu i specyfiki działalności instytucji przyjmującej. Program praktyki może obejmować wybrane zagadnienia z zakresu:

- informatyki, w tym
 - projektowania i programowania aplikacji,
 - administrowania sieciami komputerowymi,
 - zarządzania bazami danych,
 - sztucznej inteligencji,
 - grafiki komputerowej,
 - multimediiów,
- ekonometrii i statystyki, w tym
 - analizy danych,
 - modelowania finansowego,
 - pracy z narzędziami analitycznymi,
- zastosowań w biznesie i finansach, w tym
 - praktycznej obsługi systemów wspierających procesy finansowe, księgowe i zarządcze,
 - analizy finansowej,

- wspomagania decyzji zarządczych i tworzenie systemów raportowania,
- oraz innych pokrewnych dziedzin.