Obraz zawierający Czcionka, logo, design, Grafika

Opis wygenerowany automatycznie

Cyberbezpieczeństwo

Rekomendowany model systemowego kształcenia wysokiej klasy specjalistów ICT na studiach II stopnia dla kierunku sztuczna inteligencja opracowany w ramach projektu „Akademia Innowacyjnych Zastosowań Technologii Cyfrowych (AI Tech)”, realizowanego w latach 2020-2023 przez Beneficjenta – Ministerstwo Cyfryzacji (wcześniej Kancelaria Prezesa Rady Ministrów) i 5 Partnerów (Uniwersytet Warszawski, Uniwersytet im. Adama Mickiewicza w Poznaniu, Politechnika Gdańska, Politechnika Poznańska, Politechnika Wrocławska)

Autorzy:

2023

Spis treści

[Abstrakt 2](#_Toc151916213)

[Wprowadzenie 3](#_Toc151916214)

[Koncepcja modelu systemowego kształcenia 5](#_Toc151916215)

[Rekomendowany plan studiów 8](#_Toc151916216)

[Rekomendowany program studiów 10](#_Toc151916217)

[Rekomendacje w zakresie dodatkowych form kształcenia 24](#_Toc151916218)

[Staże i wizyty studyjne 24](#_Toc151916219)

[Praktyki 24](#_Toc151916220)

[Staże 25](#_Toc151916221)

[Wizyty studyjne 25](#_Toc151916222)

[Współpraca krajowa w tym ze środowiskiem biznesowym 26](#_Toc151916223)

[Udział w konferencjach 27](#_Toc151916224)

[Szkoły letnie 27](#_Toc151916225)

[Współpraca międzynarodowa 28](#_Toc151916226)

[Projekty informatyczne 28](#_Toc151916227)

[Tutoring 29](#_Toc151916228)

[Materiały dydaktyczne 32](#_Toc151916229)

[Dodatkowe rekomendacje 33](#_Toc151916230)

[Podsumowanie 33](#_Toc151916231)

[Spis aneksów i załączników 35](#_Toc151916232)

# Abstrakt

W ramach projektu *AI Tech* Ministerstwo Cyfryzacji wraz z pięcioma uczelniami partnerskimi przygotowały modele systemowego kształcenia wysokiej klasy specjalistów ICT na studiach II stopnia. Niniejsze opracowanie bazuje na założeniach programowych Rady Programowej projektu oraz doświadczeniach Wydziału Matematyki i Informatyki Uniwersytetu im. Adama Mickiewicza w Poznaniu w zakresie kształcenia specjalistów cyberbezpieczeństwa.

Na podstawie analizy materiałów wypracowanych przez tę uczelnię opracowano rekomendowany system kształcenia na trzy- oraz czterosemestralnych studiach II stopnia na kierunku *Cyberbezpieczeństwo.* W skład rekomendowanego systemu kształcenia wchodzą plan iprogram studiów trzysemestralnych, plan i program studiów czterosemestralnych, zestaw rekomendowanych sylabusów przedmiotów oraz rekomendacje odnośnie dodatkowych form kształcenia. Omówione w niniejszym dokumencie dodatkowe formy to: projekty badawczo-rozwojowe, staże i wizyty studyjne, szkoły letnie, wyjazdy konferencyjne oraz wsparcie studentów w ramach programów tutoringowych i mentoringowych.

# Wprowadzenie

Od wielu lat Internet i technologie z nim związane stały się nieodłącznym elementem otaczającego nas świata oraz definiującym współczesne społeczeństwo. W tym czasie powstał nurt społeczny o nazwie *społeczeństwo informacyjne*, w którym wiedza i umiejętne jej wykorzystanie dają nam szeroki wachlarz możliwości pozwalających na podejmowanie decyzji i wprowadzanie zmian. Rozwinięciem tego nurtu jest tzw. *społeczeństwo sieciowe*. Mamy tu do czynienia nie tylko ze zwiększeniem możliwości komunikacji, ale i wzrostem dostępności wielu informacji.

Oprócz wielu korzyści mamy również bardzo dużo wyzwań, w tym konieczność zapewnienia prawidłowego funkcjonowania infrastruktury teleinformatycznej. Potrzebne są nowe umiejętności, nowi specjaliści, a zapotrzebowanie rynku pracy jest wciąż ogromne.

Pojawienie się Internetu Rzeczy, nowych usług mobilnych, czy nawet inteligentnych domów nakłada na nas potrzebę kształcenia specjalistów posiadających kompetencje w zakresie tworzenia i użytkowania tych technologii. Kreuje się więc kluczowa kwestia dotycząca zabezpieczenia informacji, urządzeń oraz sieci.

Wraz ze wzrostem liczby ataków hakerskich oraz rozbudową systemów i usług cyfrowych lawinowo rośnie zapotrzebowanie na specjalistów od cyberbezpieczeństwa. Raport "Cybersecurity. Rynek pracy w Polsce 2023” przygotowany po raz drugi przez HackerU Polska i HRK ICT alarmuje, że w Polsce coraz bardziej brakuje specjalistów w dziedzinie cyberbezpieczeństwa. Badania zostały przeprowadzane we wrześniu i październiku 2022 wśród pracowników związanych z sektorem cybersecurity. W badaniu wzięli udział ponadto specjaliści, eksperci i managerowie zajmujący się zagadnieniami związanymi z bezpieczeństwem IT. Podkreśla się ogromne zapotrzebowanie społeczeństwa na wsparcie w zakresie kształcenia szeroko rozumianych kompetencji cyfrowych, ale również zapotrzebowanie na specjalistów w obszarze cyberdyplomacji i służb wojskowych zaangażowanych w cyberbezpieczeństwa kraju. Polska powinna jak najszybciej podjąć systemowe działania. Stawką jest bowiem nie tylko dalszy rozwój sektora produktów i usług dla cyberbezpieczeństwa, uznanego w ramach strategii Polskie Technologie opracowanej przez Ministerstwo Spraw Zagranicznych za kluczowy sektor nowoczesnych technologii, ale także bezpieczeństwo narodowe w dobie cyfrowej.

Już dziś wiemy także, że kwestii związanych z cyberbezpieczeństwem nie należy ograniczać do wymiaru technicznego i ściśle informatycznego. Ponieważ to, co dzieje się w cyberprzestrzeni coraz częściej wpływa na polityki publiczne i regulacje prawne oraz jest obszarem konfliktów czy przedmiotem relacji międzynarodowych. Bardzo ważne jest kształcenie świadomości wszystkich ludzi odnośnie roli cyberbezpieczeństwa we współczesnym świecie. Ostatnie lata zweryfikowały cyberobronność polskich instytucji, zarówno państwowych jak i prywatnych. Zapotrzebowanie na specjalistów zdecydowanie wzrosło.

Na przestrzeni ostatnich kilku lat na polskich uczelniach powstały nowe fakultety i jednostki organizacyjne specjalizujące się w cyberbezpieczeństwie. Trzeba działać tak, aby studia wyższe zapewniły studentom kompetencje adekwatne do potrzeb rozwojowych państwa i jego bezpieczeństwa. Już w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016-2020 powierzono przygotowanie oraz wdrożenie sprawnego i nowoczesnego systemu szkolenia w zakresie cyberbezpieczeństwa właśnie uczelniom wyższym. Wnioski z Okrągłego Stołu z udziałem rektorów polskich, który odbył się we wrześniu 2021 roku podczas konferencji 2nd Cybersec CEE Region&Cities jednoznacznie potwierdzają, że edukacja formalna, oprócz wyposażania uczniów i studentów w podstawowe kompetencje cyfrowe, musi szybko wykształcić specjalistyczne kadry, Polska musi zintensyfikować swoje przygotowania do odpowiedzi na wyzwania cyfrowe tak, aby system edukacji nadążył za potrzebami rynku, a także umożliwił zapełnienie ciągle powiększającej się luki zatrudnienia w sektorze teleinformatycznym. Istotne jest wykształcenie specjalistów odpowiedzialnych za dostosowanie legislacji i instytucji państwa, zwalczanie cyberterroryzmu i cyberprzestępczości, czy za budowanie współpracy międzynarodowej i zarządzanie zasobami ludzkimi.

Ministerstwo Cyfryzacji wyszło z inicjatywą realizacji, w ramach Programu Operacyjnego Polska Cyfrowa, projektu *Akademia Innowacyjnych Zastosowań Technologii Cyfrowych (AI Tech)* mającego na celu opracowanie modelu systemowego kształcenia specjalistów w zakresie sztucznej inteligencji, uczenia maszynowego oraz cyberbezpieczeństwa, który ma być wdrożony na szeroką skalę przez różne ośrodki akademickie. W ramach projektu uczelnie partnerskie miały przygotować programy studiów z wybranych obszarów oraz zrealizować na ich podstawie cykl kształcenia na tych studiach.

Niniejszy dokument prezentuje wyniki prac nad stworzeniem koncepcji modelu systemowego kształcenia specjalistów w zakresie cyberbezpieczeństwa. Prezentowana koncepcja powstała w oparciu o założenia programowe przygotowane przez Radę Programową projektu *AI Tech* oraz doświadczenia i materiały wypracowane przez uczelnie wyższe współpracujące w ramach tego projektu. Głównym punktem odniesienia stały się dokumenty zgromadzone podczas tworzenia, prowadzenia oraz podsumowania efektów studiów II stopnia na kierunku *Informatyka* na specjalności *Cyberbezpieczeństwo* na Uniwersytecie im. Adama Mickiewicza w Poznaniu. Są to studia stacjonarne 3-semestralne o profilu ogólnoakademickim przypisane do dyscyplin *Informatyka* (wiodąca) oraz *Matematyka*. Łączna liczba punktów ECTS możliwych do uzyskania to 90, z czego 14 przypada na grupę zajęć seminaryjnych, a 33 na przedmioty specjalistyczne.

Plan i program powyższych studiów stanowił punkt wyjścia, ale uwzględniono również cenne doświadczenia z realizacji dodatkowych form kształcenia wdrażanych na pozostałych uczelniach projektu *AI Tech*.

# Koncepcja modelu systemowego kształcenia

Głównym celem wprowadzenia nowego programu kształcenia jest przygotowanie na potrzeby runku pracy specjalisty od szeroko pojętego cyberbezpieczeństwa. Absolwent takich studiów obok wieloaspektowej gruntownej wiedzy teoretyczno-praktycznej powinien być wyposażony w kompetencje pozwalające mu na późniejsze samodoskonalenie, śledzenie najnowszych trendów oraz zestaw kompetencji, które pozwolą mu nawiązywać owocną współpracę oraz wymieniać doświadczenia w ramach zespołów interdyscyplinarnych.

Przygotowana koncepcja w wersji podstawowej odnosi się do 3-semestralnych studiów drugiego stopnia o profilu ogólnouniwersyteckim na kierunku *Cyberbezpieczeństwo*, ale zaproponowano również rozszerzony wariant 4-semestralny. Oba warianty dotyczą studiów w 100% przypisanych do dyscypliny *Informatyka* w dziedzinie nauk ścisłych i przyrodniczych. W przypadku tworzenia specjalności, a nie kierunku *Cyberbezpieczeństwo*, uczelnia powinna określić, które z przedmiotów są kluczowe, a które można zintegrować bądź zastąpić już istniejącymi wśród bazowych przedmiotów na kierunku, dla którego będzie opracowywana specjalność.

Proponowanym językiem wykładowym jest język polski, jednakże z uwagi na specyfikę kierunku oraz obecną dynamikę jego rozwoju, zalecane jest wykorzystywanie źródeł dydaktycznych w języku angielskim. Jednocześnie, jeżeli uczelnia posiada odpowiedni potencjał kadrowy, warto rozważyć prowadzenie tych studiów w języku angielskim. Takie podejście miałoby szereg korzyści. Rodzimym studentom dawałoby to poszerzone możliwości doskonalenia znajomości języka angielskiego, dzięki czemu znacznie lepiej będą sobie w przyszłości radzić z pozyskiwaniem najnowszych informacji branżowych (co jest kluczowe w kontekście śledzenia zagrożeń, ujawnianych stale podatności oraz nowych wektorów ataków). Absolwent takich studiów znacznie łatwiej będzie odnajdował się w międzynarodowych zespołach i firmach. Jednocześnie prowadzenie studiów całościowo w języku angielskim umożliwi dotarcie z ofertą edukacyjną do studentów zagranicznych (np. chcących przyjechać do Polski w ramach projektów Erasmus+ bądź CEEPUS).

Podstawowy program studiów zakłada, że kandydat posiadać będzie wiedzę i umiejętności z zakresu: podstawowej algorytmiki, programowania w języku C, podstawowej znajomości konfiguracji systemów z rodzin Windows i Linux, wiedzy na temat budowy prostych sieci komputerowych (na poziomie inżyniera informatyki) i posługiwał się językiem angielskim co najmniej na poziomie B1. W przypadku, gdy podczas rozmowy kwalifikacyjnej, egzaminu wstępnego bądź innej formy weryfikacji kompetencji kandydata, wykazane są braki w powyższych obszarach, zalecane jest skierowanie studenta na dodatkowe kursy wyrównujące kompetencje. Semestrem przeznaczonym na ewentualne kursy wyrównawcze jest semestr pierwszy (zarówno w przypadku studiów trzy- jak i czterosemestralnych).

W skład opracowanej koncepcji wchodzą dwa alternatywne plany i programy (dla studiów trzy- i czterosemestralnych), rekomendacje dotyczące organizacji indywidualnego wsparcia dla studenta w osobie tutora lub mentora, rekomendacje dotyczące sposobu organizacji dodatkowych form kształcenia tj. staże i wizyty studyjne, uczestnictwo w szkołach letnich oraz konferencjach branżowych i naukowych. Program studiów zawiera rekomendacje nt.:

* zestawu przedmiotów obowiązkowych tworzących minimum programowe na kierunku *Cyberbezpieczeństwo* (w tym zawarto kurs językowy oraz seminaria magisterskie),
* zestawu przedmiotów obieralnych (w tym humanistycznych), pozwalających na poszerzanie horyzontów i rozwój zainteresowań studenta,
* zestawu przedmiotów, które są obowiązkowe w przypadku tworzenia studiów czterosemestralnych, ale w przypadku budowania studiów trzysemestralnych mogą być oferowane studentom jako przedmioty dodatkowe, wyrównujące wiedzę kandydatów,
* niezwykle ważny dwusemestralny projekt badawczo-rozwojowy,
* powszechny udział w dodatkowych formach kształcenia (stażach, wizytach studyjnych oraz konferencjach naukowych).

Do programu studiów nie wpisano bezpośrednio kursu z zakresu bezpiecznych i higienicznych warunków kształcenia (BHP), wychodząc z założenia, że zorganizowanie takiego kursu jest, na podstawie odpowiednich przepisów prawa, obowiązkiem rektora i każda uczelnia ma wypracowane w tym zakresie standardowe procedury.

Powyższe zestawy zostały przygotowane na podstawie założeń programowych przygotowanych przez Radę Programową projektu *AI Tech* oraz planów i programów studiów przygotowanych przez Uniwersytet im. Adama Mickiewicza w Poznaniu. Plany i programy proponowanego modelowego kierunku studiów, wraz z zalecanymi sylabusami, stanowią załączniki do niniejszego dokumentu.

W obszarze metod kształcenia rekomendujemy odchodzenie od form biernych, w szczególności od klasycznych wykładów podawczych, na rzecz konwersatoriów, studium przypadku oraz przede wszystkim metod projektowych. Kluczowym elementem programu studiów jest dwusemestralny obowiązkowy przedmiot *Projekt badawczo-rozwojowy* w ramach którego studenci współpracują z opiekunem technologicznym (przedstawicielem otoczenia gospodarczego uczelni), bądź naukowym (przedstawiciel kadry naukowej danej uczelni), aby rozwiązać wieloaspektowy problem związany z bezpieczeństwem systemów i danych. Jednocześnie zaleca się, by zwiększyć ilość mniejszych projektów zaliczeniowych z poszczególnych przedmiotów, np. w miejsce pojedynczego kolokwium mającego potwierdzić nabycie odpowiednich kompetencji, zaliczenie laboratorium mogłoby być powiązane z koniecznością realizacji kilku pomniejszych projektów cząstkowych połączonych z publiczną prezentacją ich efektów.

Specyfiką kierunku *Cyberbezpieczeństwo* jest wymóg dostępu studenta do odpowiedniej infrastruktury sprzętowej, aby mógł (w szczególności po zajęciach) poszerzać swoją wiedzę i doskonalić umiejętności. Uczelnia planująca wdrożenie kierunku *Cyberbezpieczeństwo* powinna dysponować nie tylko infrastrukturą niezbędną do prowadzenia poszczególnych zajęć, ale powinna też zadbać o udostępnienie studentom odpowiednio przygotowanej i administrowanej pracowni np. w ramach Otwartego Laboratorium w ustalonych odgórnie godzinach. Należy przy tym mieć na uwadze, że sprzęt komputerowy podlega naturalnym procesom starzenia, a oprogramowanie powinno być często aktualizowane - zwłaszcza po wykryciu podatności. Laboratoria przeznaczone na zajęcia w ramach studiów nad cyberbezpieczeństwem powinny być co roku audytowane pod kątem przydatności i aktualności. Dotyczy to nie tylko oprogramowania i komputerów, ale również sprzętu sieciowego tj. routery czy sprzętowe firewalle.

Opracowywane i udostępniane studentom materiały dydaktyczne powinny mieć nowoczesną formę, w szczególności umożliwiającą dostęp z różnych platform sprzętowych i systemów operacyjnych. Podstawowe materiały dydaktyczne powinny być przekazywane w formacie pdf z ewentualnymi kopiami w innych formatach (docx/odt, pptx/odp itp.). Jednocześnie stanowić to ma zaledwie bazę, którą rozszerzać powinny – w zależności od kontekstu danego przedmiotu – materiały interaktywne (np. notesy Jupyter Notebook), przykładowe kody i konfiguracje, nagrania wideo (zweryfikowane tutoriale online, nagrania wykładów, fragmenty nagrań z wizyt studyjnych, wideo-raporty z eksperymentów dużych agencji, itp.) oraz przygotowane wirtualne laboratoria (np. w postaci gotowych kontenerów typu docker czy obrazów systemów wirtualnych). Należy też pamiętać o jednym z celów dydaktycznych jakim jest pogłębienie u studentów świadomości konieczności stałego samodoskonalenia i pozyskiwania nowej wiedzy. Dlatego należy w procesie dydaktycznym zawrzeć elementy wymagające od studentów poszukiwania wiedzy w publikacjach naukowych i raportach głównych agencji CERT.

# Rekomendowany plan studiów

Plan studiów stanowi *Załącznik nr 1.* do niniejszego dokumentu. Zawiera on dwie wersje: studiów trzy- oraz czterosemestralnych. Za główny uznawany jest plan trzysemestralny. Poniżej opisano jego najważniejsze założenia.

Pierwszy semestr z założenia jest semestrem wprowadzającym studenta w tematykę bezpieczeństwa komputerowego. Składa się z trzech pełnych przedmiotów akademickich realizowanych w wymiarze 30 godzin wykładu i 30 godzin zajęć laboratoryjnych i dających studentowi po 6 punktów ECTS każdy. Są to przedmioty budujące fundamenty wiedzy teoretycznej, wiedzy praktycznej nt. projektowania i funkcjonowania rozbudowanych infrastruktur teleinformatycznych oraz rozbudowujące świadomość wyzwań związanych z zapewnieniem bezpieczeństwa danych cyfrowych w cyberprzestrzeni. Pierwszy semestr zawiera także przedmiot zaznamiający studentów z obowiązującymi w Polsce i w Europie kontekstami prawnymi, oraz kształcący umiejętność śledzenia i analizy obowiązujących regulacji prawnych dotyczących bezpieczeństwa danych, cyberprzestrzeni oraz praw autorskich. Przedmiot ten w założeniach to 30 godzin wykładu w formie konwersatorium za 3 punkty ECTS. Ponadto, aby ułatwić studentowi samodzielne pogłębianie wiedzy w trakcie studiów już na pierwszym semestrze organizowany jest kurs języka angielskiego skupiony wokół tematyki cyberbezpieczeństwa oraz rozwijający umiejętności czytania i pisania tekstów technicznych oraz naukowych. Na ten przedmiot składa się 45 godzin ćwiczeń i 3 punkty ECTS. Komplet przedmiotów na pierwszym semestrze zamyka przedmiot do wyboru w wymiarze 30 godzin pracy laboratoryjnej oraz 30-godzinne seminarium magisterskie I – oba przedmioty dają studentowi po 3 punkty ECTS. Zaleca się, aby seminarium magisterskie rozpoczynało się z opóźnieniem (nawet o pół semestru) w stosunku do pozostałych przedmiotów i było poprzedzone otwartymi spotkaniami z wykładowcami będącymi potencjalnymi opiekunami seminaryjnymi.

Na drugim semestrze wprowadzona jest znacznie większa modularność. Z ośmiu przedmiotów zaledwie trzy mają konkretną ustaloną tematykę i formę. Są to dwa duże przedmioty akademickie za 6 punktów ECTS każdy i mające wymiar 30 godzin wykładu + 30 godzin ćwiczeń bądź laboratoriów oraz przedmiot konwersatoryjny za 2 punkty ECTS przygotowujący studentów do pracy i raportowania w ramach projektu badawczo-rozwojowego. Pozostałe przedmioty to 30 godzinna kontynuacja seminarium magisterskiego, dwa kierunkowe przedmioty do wyboru (po 3 punkty ECTS) oraz jeden przedmiot ogólnouniwersytecki (2 ECTS). Ostatnim przedmiotem na tym semestrze jest pierwszy etap projektu badawczo-rozwojowego, w ramach którego studenci dobrani w 5 osobowe zespoły i pod kierownictwem przydzielonego opiekuna naukowego bądź technologicznego rozpoczynają pracę nad problemem przedstawionym im przez opiekuna.

Trzeci i zarazem ostatni semestr podsumowuje zdobyte doświadczenia. Na tym semestrze kończy się projekt badawczo-rozwojowy. Zalecane jest skomasowanie pracy nad projektem w pierwszej części semestru, aby drugą część studenci mogli przeznaczyć na dokończenie pracy nad projektem magisterskim. Prace te są elementem trzeciego semestru seminarium magisterskiego, który (z uwagi na konieczność ostatecznego przygotowania i obrony pracy magisterskiej) ma tym razem przypisane aż 8 punktów ECTS. Dodatkowo ostatni semestr zawiera jeden duży przedmiot akademicki (6 ECTS), jeden przedmiot do wyboru spośród przedmiotów kierunkowych, oraz trzy 30-godzinne przedmioty, z czego jeden poświęcony jest penetracyjnemu testowaniu systemów a dwa pozostałe dotyczą zagadnień bardziej humanistycznych. Przedmiotem odpowiadającym na zgłaszane przez pracodawców sugestie odnośnie brakujących kwalifikacji absolwentów jest *Warsztat kompetencji miękkich dla cyberspecjalisty,* zaś kwestie ataków z wykorzystaniem socjotechnik, ich mechanizmy i przyczyny skuteczności oraz wpływ na kształtowanie się polityk bezpieczeństwa w firmach omawiane są na drugim z 30 godzinnych przedmiotów obowiązkowych.

W czterosemestralnym planie studiów dwa końcowe semestry są identyczne z planem trzysemestralnym. Pierwszy semestr studiów czterosemestralnych zawiera cztery przedmioty z pierwszego semestru studiów trzysemestralnych: *Język angielski, Prawne aspekty cyberprzestrzeni, Matematyczne podstawy cyberbezpieczeństwa* oraz *Przedmiot do wyboru* I. Pojawiają się dwa dodatkowe duże przedmioty akademickie mające za zadanie uzupełnić ewentualne braki z wcześniejszych etapów edukacyjnych studenta. Są to: *Administracja usługami sieciowymi* oraz *Programowanie sieciowe w języku C.* W przypadku, gdy kandydat na te studia będzie już posiadał kompetencje przekazywane przez te przedmioty, powinien w ich miejsce wybrać odpowiednią ilość kierunkowych przedmiotów do wyboru o odpowiedniej sumarycznej ilości punktów ECTS. Ostatni przedmiot wyrównującym wiedzę to 30 godzinne *Zaawansowane algorytmy kombinatoryczne* budujący fundamenty pod przyszły przedmiot *Kryptologia*.

Drugi semestr studiów czterosemestralnych zawiera dodatkowy kurs *Języka angielskiego*, dwa duże przedmioty akademickie z pierwszego semestru studiów trzysemestralnych (*Budowa dużych sieci teleinformatycznych* oraz *Podstawy bezpieczeństwa danych cyfrowych)*. Na tym semestrze rozpoczyna się też seminarium magisterskie. Dodatkowymi przedmiotami obowiązkowymi (które można wybrać jako kierunkowe przedmioty do wyboru na studiach trzysemestralnych) są *Kryminalistyka cyfrowa* oraz *Inżynieria wsteczna złośliwego oprogramowania*. Semestr zamykają dwa kierunkowe przedmioty do wyboru.

W przypadku obu planów studiów nazwy przedmiotów oraz przypisanie godzinowe do konkretnych form (np. wykład bądź konwersatorium) należy traktować jako propozycje. Uczelnia może je modyfikować wedle własnych potrzeb, o ile zrealizowane zostaną podstawowe założenia dla przedmiotów omówione w sekcji *Rekomendacje w zakresie treści nauczania - sylabusy przedmiotów.*

# Rekomendowany program studiów

Rekomendowane programy studiów trzy- oraz czterosemestralnych stanowią *Załącznik nr 2* i *Załącznik nr 3* do niniejszego dokumentu. Za główny uznawany jest program trzysemestralny. Poniżej opisano jego główne założenia.

Układ przedmiotów z omówionych powyżej planów ma swoje odzwierciedlenie w załączonych programach. Zastosowanie ma też uwaga z wcześniejszej sekcji o pewnej elastyczności w nazewnictwie przedmiotów. Oba programy studiów na wstępie zawierają listę efektów kształcenia, powiązaną z Polską Ramą Kwalifikacji, opracowaną na podstawie założeń programowych projektu *AI Tech* oraz programów studiów przygotowanych przez uczelnie partnerskie w ramach tego projektu. Programy zawierają wykaz przedmiotów obowiązkowych stanowiących minimum programowe na kierunku (bądź specjalności) *Cyberbezpieczeństwo*. Znaczna ilość przedmiotów do wyboru, szczególnie w programie studiów czterosemestralnych, pozostawia uczelni pewną swobodę w komponowaniu ostatecznego programu studiów.

Poniższa lista przedstawia przedmioty obowiązkowe w trzysemestralnej wersji programu:

* *Prawne aspekty cyberprzestrzeni,*
* *Matematyczne podstawy cyberbezpieczeństwa,*
* *Podstawy bezpieczeństwa danych cyfrowych,*
* *Budowa dużych sieci teleinformatycznych,*
* *Bezpieczeństwo systemów operacyjnych,*
* *Kryptologia,*
* *Wykrywanie ataków sieciowych,*
* *Testy penetracyjne,*
* *Socjotechnika i polityki cyberbezpieczeństwa.*

Pierwsze cztery przedmioty zawierają treści wprowadzające, dzięki którym studentom łatwiej będzie przyswoić koncepcje z późniejszych przedmiotów. Powinny być realizowane w pierwszym semestrze. Cała grupa wymienionych powyżej przedmiotów pozwala studentowi uzyskać bazową wiedzę i umiejętności niezbędne w pracy cyberspecjalisty.

Istotne dla pracodawców kompetencje miękkie rozwijane są na następujących, nie wymienionych powyżej, przedmiotach obowiązkowych:

* *Seminarium magisterskie,*
* *Warsztat kompetencji miękkich dla cyberspecjalisty,*
* *Język angielski,*
* *Przygotowanie do projektu badawczo-rozwojowego,*
* *Projekt badawczo-rozwojowy.*

*Seminarium magisterskie* trwa trzy semestry, co oznacza, że na studiach trzysemestralnych od razu na pierwszym semestrze student zobowiązany jest do wyboru tematyki. Rozważyć należy, czy przedmiot nie powinien rozpoczynać się z opóźnieniem w stosunku do pozostałych przedmiotów, nawet o pół semestru. Wybór grupy seminaryjnej powinien być poprzedzony otwartymi spotkaniami z prowadzącymi, którzy będą mieli okazję zaprezentować wiodącą w danym roku tematykę swoich zajęć. Ponadto dużą rolę w procesie wyboru pełnić będą konsultacje z tutorem.

Przedmioty *Warsztat kompetencji miękkich dla cyberspecjalisty* oraz *Socjotechnika i polityki cyberbezpieczeństwa* są przedmiotami na pograniczu nauk społecznych oraz informatyki, a ich łączne oszacowanie nakładu pracy to 5 punktów ECTS. Umieszczenie ich na ostatnim semestrze nie jest konieczne, jednakże jest to semestr na którym od studenta oczekuje się ukończenia dwóch dużych projektów: zespołowego badawczo-rozwojowego oraz indywidualnego projektu magisterskiego, więc dokładanie na ostatni semestr zbyt dużej liczby dużych przedmiotów może poskutkować trudnościami dotrzymaniu wszystkich terminów. Dlatego też dodatkowym zaleceniem jest zaplanowanie zakończenia dwusemestralnego *Projektu badawczo-rozwojowego* w połowie ostatniego semestru. Warto rozważyć zakończenie w postaci mini-konferencji na której studenci prezentować będą wyniki swoich prac i na którą zaproszeni zostaną przedstawiciele otoczenia gospodarczego uczelni.

W programie studiów przewidziano *Przedmiot ogólnouczelniany*, któremu przypisano 3 punkty ECTS. Jest to wyraz widocznej na uczelniach polskich tendencji do umożliwienia studentom poszerzenia wiedzy z obszaru kształcenia niezwiązanego ze studiowanym kierunkiem, a znajdującego się w sferze zainteresowań studenta. Ze względu na interdyscyplinarność uczenia maszynowego taka wiedza może być dla studenta cenna z punktu widzenia przyszłej pracy zawodowej. Jeżeli na uczelni taka oferta zajęć ogólnouczelnianych nie jest dostępna, można z tego przedmiotu zrezygnować i zastąpić go innym związanym z obszarem kształcenia.

Rozwój kompetencji językowych zawarto na przedmiocie *Język angielski*. Na studiach trzysemestralnych jest to przedmiot 45 godzinny na pierwszym semestrze, zaś na studiach czterosemestralnych przedmiot łącznie ma przypisanych 90 godzin i odbywa się zarówno na pierwszym jak i drugim semestrze. Uczelnia może zamienić kursy stricte językowe na inny przedmiot prowadzony w tym języku, który wymagać będzie od studentów rozwoju kompetencji językowych zarówno w warstwie prezentacyjnej, jak i przy tworzeniu rozbudowanych tekstów. Przykładem takiego przedmiotu jest *Pisanie prac naukowo-technicznych (Scientific & Technical Writing)* oferowany przez Politechnikę Poznańską.

W programie studiów czterosemestralnych występują dodatkowe przedmioty, których głównym celem jest wyrównanie ewentualnych nierówności w wiedzy świeżo zrekrutowanych studentów. Są to:

* *Administracja usługami sieciowymi,*
* *Programowanie sieciowe w języku C ,*
* *Zaawansowane algorytmy kombinatoryczne.*

Treści omawiane na dwóch pierwszych przedmiotach często pojawiają się w programach studiów inżynierskich na kierunku *Informatyka*, dlatego w sytuacji gdy nowo zrekrutowany student przedstawi potwierdzenie uzyskania odpowiednich kompetencji, powinien w miejsce odpowiednich przedmiotów wybrać taką ilość przedmiotów do wyboru, aby suma przypisanych im punktów ECTS była równa bądź większa od sumy punktów zastępowanych przedmiotów.

Oprócz przedmiotów wyrównujących, student studiów czterosemestralnych na drugim semestrze ma w programie dwa dodatkowe (nie występujące w programie studiów trzysemestralnych) obowiązkowe przedmioty, których celem jest pogłębienie wiedzy na temat architektury złośliwego oprogramowania (*Inżynieria wsteczna złośliwego oprogramowania*) oraz praktycznych zastosowań wiedzy na temat problematyki oraz metod pozyskiwania, zabezpieczania i analizy danych cyfrowych (*Kryminalistyka cyfrowa*). Przedmioty te mogą być również zamieszczone w ofercie kierunkowych przedmiotów do wyboru dla studiów trzysemestralnych.

Program studiów przewiduje umożliwienie studentowi (w porozumieniu z tutorem lub promotorem) swobodnego dobrania przedmiotów specjalizacyjnych. Przykładowa oferta takich przedmiotów została przedstawiona w następnej sekcji, poświęconej treściom nauczania. Ogólnie w proponowanych programach studiów liczba punktów ECTS przypisanych do przedmiotów zaliczanych do zajęć do wyboru wynosi: 38 dla studiów trzysemestralnych oraz 44 dla studiów czterosemestralnych. Uwaga: podczas dostosowywania planu i programu do konkretnej uczelni i jej warunków należy przeanalizować jeszcze raz faktyczny nakład pracy studenta na konkretnej realizacji przedmiotu oraz ile punktów ECTS będzie realizowanych w kontakcie z nauczycielem.

Do przedmiotów tych zaliczane są:

* Przedmioty do wyboru *I, II, III, IV, V\*, VI\** – 3 punktów za każdy przedmiot,
* Przedmiot ogólnouczelniany *–* 2 punkty ECTS*,*
* Seminarium magisterskie *I*, *II*, *III* – 14 punktów ECTS*,*
* Projekt *badawczo-rozwojowy I i II* – 10 punktów ECTS*.*

Przedmioty oznaczone \* występują jedynie w programie studiów czterosemestralnych. Biorąc pod uwagę, że wspomniane wyżej przedmioty wyrównujące można zastąpić przedmiotami do wyboru, uczelnia powinna przygotować bogatą ofertę takich przedmiotów. Minimalna łączna suma punktów ECTS przypisanych do tych przedmiotów powinna wynosić 33. Przy założeniu, że byłyby to przedmioty 30 godzinne za 3 punkty ECTS oznacza to, że na liście powinno być minimum 11 przedmiotów nie uwzględniając przedmiotów wyrównujących wiedzę ze studiów czterosemestralnych. Przy wyliczaniu punktów kontaktowych z nauczycielem, każda uczelnia powinna kierować się wewnętrznymi regulacjami i ustaleniami oraz indywidualną organizacją pracy na tworzonych przedmiotach. Na potrzeby bieżącego modelu przyjęto następujące założenia:

* na przedmiotach 60h/6ECTS studenci uzyskują 4 punkty ECTS w kontakcie z nauczycielem,
* na przedmiotach 30h/3ECTS – odpowiednio 2 ECTS,
* blok seminaryjny daje 7 ECTS w kontakcie z nauczycielem,
* *Projekt badawczo-rozwojowy* daje 2 punkty ECTS.

Jednocześnie należy podkreślić, że te wyliczenia mogą się zmienić w zależności od konkretnej realizacji danego przedmiotu, co będzie szczególnie istotne przy wyliczaniu godzin dla Projektu badawczo-rozwojowego (uwzględniając takie aspekty jak wybór opiekuna grupy, częstotliwość jego kontaktu z grupą oraz formę ich współpracy). Rekomendacje w zakresie treści nauczania – sylabusy przedmiotów

W niniejszej sekcji po krótce przedstawione zostaną zalecenia do poszczególnych przedmiotów z ewentualnym wskazaniem na konkretny sylabus. Sylabusy stanowią *Załącznik nr 4.* do niniejszego dokumentu. W większości przypadków sylabus to dokument przygotowany na potrzeby specjalności *Cyberbezpieczeństwo* kierunku *Informatyka* na Uniwersytecie im. Adama Mickiewicza w Poznaniu. W pozostałych przypadkach załącznikami są dokumenty zawierające konkretne rekomendacje przygotowane przez autorów w zakresie treści dydaktycznych, jakie powinny być zawarte w opisywanym przedmiocie.

Poniższe przedmioty przedstawiono w kolejności alfabetycznej z podziałem na przedmioty obowiązkowe oraz rekomendowane przedmioty do wyboru. Trzecią grupę stanowią przedmioty ze studiów czterosemestralnych, które nie występują w programie trzysemestralnym, jednakże mogą być w nim rekomendowane jako przedmioty do wyboru.

Oznaczenia skrótowe zastosowane w tej sekcji to:

* w – wykład,
* ć – ćwiczenia,
* l – laboratoria,
* k – konwersatorium,
* s – seminarium
* p – projekt.

Po nazwie przedmiotu podano w nawiasie sugerowaną liczbę punktów ECTS oraz liczby godzin przypisanych do odpowiednich form zajęć. W przypadku, gdy do danego przedmiotu załączony jest gotowy sylabus, ale jego szczegóły różnią się od propozycji z niniejszego dokumentu, różnice są wyraźnie opisane.

Przedmioty obowiązkowe.

* ***Bezpieczeństwo systemów operacyjnych (6 ECTS, 30 w, 30 l)***

Celem przedmiotu jest zapoznanie studenta z mechanizmami zwiększającymi bezpieczeństwo systemów operacyjnych Windows, Linux oraz MacOS, czyli z technikami ,,utwardzania” (ang. Hardening) systemów operacyjnych. Należy zapoznać studenta z atakami na systemy operacyjne, polityką Zero Trust wspomagającą w walce z tymi atakami oraz zapoznać z wbudowanymi mechanizmami bezpieczeństwa w systemach operacyjny dostarczanych przez ich twórców oraz mechanizmami bezpieczeństwa, na które zarówno administrator jak i zwykły użytkownik mają wpływ.

Na ćwiczeniach student powinien nabyć umiejętności wykorzystywania istniejących mechanizmów zwiększających bezpieczeństwo systemu oraz jego użytkowników.

Zalecenia odnośnie treści przedmiotu znajdują się w dokumencie *Rekomendacja – Bezpieczeństwo systemów operacyjnych.*

* ***Budowa dużych sieci teleinformatycznych (6 ECTS, 30 w, 30 l)***

Celem przedmiotu jest zapoznanie studenta jak prawidłowo zaprojektować, wdrożyć i zabezpieczyć sieć teleinformatyczną w dużej firmie. Należy zapoznać studenta z tworzeniem sieci szkieletowej, połączeń między urządzeniami końcowymi a punktami dystrybucyjnymi, poprawnym rozmieszczaniem punktów dostępowych Wi-Fi. Należy również uwzględnić informacje jakiego sprzętu i okablowania używać, jak wyliczać moc punktów dystrybucyjnych, jakich kabli miedzianych lub światłowodowych używać.

Na laboratorium student powinien nabyć umiejętności wdrażania technologii VoIP, protokoły routingu, podział sieci na VLAN-y, wykorzystanie tunelowania, konfigurowanie firewalli.

Zalecenia odnośnie treści znajdują się w dokumencie *Rekomendacja – Budowa dużych sieci teleinformatycznych.*

* ***Język angielski I (3 ECTS, 45 ć)***

Celem przedmiotu jest rozwijanie i doskonalenie kompetencji językowych z uwzględnieniem słownictwa specjalistycznego związanego z kierunkiem studiów. W szczególności studenci powinni doskonalić umiejętności związane z komunikowaniem się w środowisku akademickim i zawodowym, czytaniem ze zrozumieniem tekstów akademickich oraz technicznych, a także z pisaniem różnorodnych tekstów (formalnych maili, opisów projektów, raportów z analizy danych).

* ***Kryptologia (6 ECTS, 30 w, 30 ć)***

Celem przedmiotu jest zapoznanie studenta ze współczesnymi algorytmami i protokołami kryptograficznymi, które pozwolą na budowanie bezpiecznego systemu informatycznego. Musi poznać współczesną terminologię kryptograficzną, wady i zalety różnych rozwiązań kryptograficznych, bezpieczeństwo protokołów kryptograficznych. Należy również zapoznać studenta z zagrożeniami wynikającymi z niewłaściwego stosowania technik kryptograficznych.

Na ćwiczeniach student powinien nabyć praktyczne umiejętności implementowania podstawowych systemów kryptograficznych oraz umiejętność wykorzystania bibliotek kryptograficznych wspierających bezpieczeństwo tworzonych aplikacji.

Przykładem realizacji takiego przedmiotu jest *Krytpologia* (UAM).

Do wykorzystania rekomenduje się sylabus przedmiotu *Kryptologia* (UAM).

* ***Matematyczne podstawy cyberbezpieczeństwa (6 ECTS, 30 w, 30 ć)***

Celem przedmiotu jest przedstawienie studentowi kluczowych pojęć matematycznych z algebry liniowej, rachunku prawdopodobieństwa, statystyki matematycznej oraz kryptografii. Omawiane zagadnienia powinny nauczyć studentów umiejętnego wykorzystania ich w rozwiązywaniu problemów informatycznych, zwłaszcza w kontekście zapewnienia bezpieczeństwa informacji w cyberprzestrzeni.

Na ćwiczeniach student powinien nauczyć się zastosowania algebry liniowej, rachunku prawdopodobieństwa, statystyki matematycznej ze szczególnym uwzględnieniem kryptografii w rozwiązywaniu problemów bezpieczeństwa informacji.

Przykładem realizacji takiego przedmiotu jest *Narzędzia matematyczne sztucznej inteligencji i cyberbezpieczeństwa* (UAM).

Do wykorzystania rekomenduje się sylabus przedmiotu *Narzędzia matematyczne sztucznej inteligencji i cyberbezpieczeństwa* (UAM) z dodatkowym uwzględnieniem kryptografii.

* ***Podstawy bezpieczeństwa danych cyfrowych (6 ECTS, 30 w, 30 l)***

Celem przedmiotu jest wykształcenie w studentach świadomości wyzwań związanych z zapewnieniem bezpieczeństwa danych cyfrowych w cyberprzestrzeni. Należy zapoznać studenta z szerokim zakresem potencjalnych zagrożeń i incydentów, które mogą się zdarzyć wraz z mechanizmami skutecznego zapobiegania ich występowania.

Na laboratorium należy umożliwić studentowi zdobycie wiedzy i doświadczenia w wykrywaniu rzeczywistych podatności w systemach informacyjnych z wykorzystaniem istniejących narzędzi wspierających zdobycie tej wiedzy.

Przykładem realizacji takiego przedmiotu jest *Podstawy bezpieczeństwa danych cyfrowych* (UAM).

Do wykorzystania rekomenduje się sylabus przedmiotu *Podstawy bezpieczeństwa danych cyfrowych* (UAM).

* ***Prawne aspekty cyberprzestrzeni (3 ECTS, 30 k)***

Celem przedmiotu jest zapoznanie studenta z zagrożeniami oraz wyzwaniami w cyberprzestrzeni wraz z regulacjami prawnymi, które pozwalają na reagowanie, zapobieganie oraz zwalczanie incydentów. Należy wprowadzić pojęcia związane z cyberprzestrzenią oraz cyberatakami. Należy zaznajomić studenta z kluczowymi podmiotami państwowymi w sektorze cyberbezpieczeństwa oraz z regulacjami prawnymi obowiązującymi w Polsce, Unii Europejskiej oraz z umowami międzynarodowymi pozwalającymi na ochronę w cyberprzestrzeni.

Zalecenia odnośnie treści przedmiotu znajdują się w dokumencie *Rekomendacja – Prawne aspekty cyberprzestrzeni.*

* ***Projekt badawczo-rozwojowy I (5 ECTS, 30 p)***

Celem przedmiotu jest zrealizowanie przez studenta projektu systemu informatycznego w zespole stawiając na kreatywność, innowacyjność, bezpieczeństwo oraz współpracę oraz na wdrożenia projektu w środowisku biznesowym. Projekt powinien zawierać specyfikację oraz harmonogram a następnie, zgodnie z tymi wytycznymi, powinien zostać zaimplementowany i wdrożony.

Przykładem realizacji takiego przedmiotu jest *Projekt badawczo-rozwojowy 1* (UAM).

Do wykorzystania rekomenduje się sylabus przedmiotu *Projekt badawczo-rozwojowy 1* (UAM).

* ***Projekt badawczo-rozwojowy II (5 ECTS, 30 p)***

Student kontynuuje pracę rozpoczętą na przedmiocie ***Projekt badawczo-rozwojowy I.***

Do wykorzystania rekomenduje się sylabus przedmiotu *Projekt badawczo-rozwojowy 2* (UAM).

* ***Przygotowanie do projektu badawczo-rozwojowego (2 ECTS, 30 k)***

Przedmiot ma na celu przygotowanie studenta do tworzenia projektów w zespole stawiając na kreatywność, innowacyjność oraz współpracę. Student powinien nabyć wiedzę, w jaki sposób pozyskiwać inwestorów dla projektów. Powinien nabyć umiejętność tworzenia systemu informatycznego spełniającego kryteria funkcjonalności oraz użyteczności a następnie zdobyć wiedzę w jaki sposób wdrażać gotowe projekty w środowisku biznesowym.

Przykładem realizacji takiego przedmiotu jest *Przygotowanie do projektu badawczo-rozwojowego* (UAM).

Do wykorzystania rekomenduje się sylabus przedmiotu *Przygotowanie do projektu badawczo-rozwojowego* (UAM).

* ***Seminarium magisterskie I (3 ECTS, 30 s)***

Na seminariach magisterskich studenci pod opieką promotora referują wybrane zagadnienia z literatury przedmiotu. Wybierane wspólnie przez studentów i prowadzących seminarium tematy referatów mają ukierunkowywać studenta do napisania ciekawej i wartościowej pracy magisterskiej w zakresie cyberbezpieczeństwa. Od studentów oczekuje się samodzielności w opracowywaniu zakresu tematu oraz w przygotowywaniu prezentacji a następnie przygotowanie praktycznego lub teoretycznego projektu wykorzystującego zdobytą wiedzę na kierunku.

Przykładem realizacji takiego przedmiotu jest *Seminarium magisterskie 1* (UAM).

Do wykorzystania rekomenduje się sylabus przedmiotu *Seminarium magisterskie 1* (UAM).

* ***Seminarium magisterskie II (3 ECTS, 30 s)***

Student kontynuuje pracę rozpoczętą na przedmiocie ***Seminarium magisterskie I.***

Do wykorzystania rekomenduje się sylabus przedmiotu *Seminarium magisterskie 2* (UAM).

* ***Seminarium magisterskie III (8 ECTS, 30 s)***

Student kontynuuje pracę rozpoczętą na przedmiocie ***Seminarium magisterskie I*** oraz ***Seminarium magisterskie II.***

Praca powinna zakończyć się napisaniem pracy magisterskiej w zakresie cyberbezpieczeństwa.

Do wykorzystania rekomenduje się sylabus przedmiotu *Seminarium magisterskie 3* (UAM).

* ***Socjotechnika i polityki cyberbezpieczeństwa (3 ECTS, 30 k)***

Celem przedmiotu jest zapoznanie studenta ze źródłem, tendencjami oraz znaczeniem rewolucji informatycznej oraz nabycie umiejętności identyfikowania kluczowych wyzwań oraz zagrożeń ,,miękkich’’ i ,,twardych’’ dotyczących cyberbezpieczeństwa oraz ich zwalczaniu. Dodatkowo należy zapoznać studenta z szerokim wachlarzem ataków socjotechnicznych i ich wpływem na politykę bezpieczeństwa systemów informacyjnych oraz użytkowników przeciw którym te ataki w głównej mierze są stosowane.

Przykładem realizacji takiego przedmiotu jest *Polityka cyberbezpieczeństwa* (UAM).

Do wykorzystania rekomenduje się sylabus przedmiotu *Polityka cyberbezpieczeństwa* (UAM) z dodatkowym uwzględnieniem ataków socjotechnicznych.

* ***Testy penetracyjne (3 ECTS, 30 l)***

Celem przedmiotu jest zapoznanie studenta z metodykami prowadzenia testów penetracyjnych w systemach Windows i Linux oraz w aplikacjach webowych. Należy zapoznać studenta z etycznymi i prawnymi aspektami przeprowadzania takich testów. Student powinien poznać pasywne i aktywne metody pozyskiwania danych o danym celu (osobie, domenie, firmie czy sieci). Powinien umieć wykrywać podatności w systemach operacyjnych, sieciach oraz aplikacjach webowych, poznać narzędzia pomagające wykrywać podatności, umieć napisać własne proste narzędzia automatyzujące pracę podczas testów.

Przykładem realizacji takiego przedmiotu jest *Testy penetracyjne* (UAM).

Do wykorzystania rekomenduje się sylabus przedmiotu *Testy penetracyjne* (UAM).

* ***Warsztat kompetencji miękkich dla cyberspecjalisty (2 ECTS, 30 k)***

Celem przedmiotu jest rozbudowanie u studenta kompetencji miękkich, które będą mu potrzebne zarówno w trakcie pracy jako specjalisty od cyberbezpieczeństwa ale także w życiu osobistym. Student m.in. będzie mógł przeanalizować swój styl funkcjonowania i jego wpływ na zachowanie innych osób. Będzie też mógł rozpoznać własne silne i słabe strony wpływające na potencjalne ryzyko w budowaniu dobrych relacji społecznych i odpowiednie przekazywanie informacji zawodowych.

Przykładem realizacji takiego przedmiotu jest *Warsztat kompetencji miękkich dla cyberspecjalisty* (UAM).

Do wykorzystania rekomenduje się sylabus przedmiotu *Warsztat kompetencji miękkich dla cyberspecjalisty* (UAM).

* ***Wykrywanie ataków sieciowych (6 ECTS, 30 w, 30 l)***

Celem przedmiotu jest podniesienie świadomości studenta nt. bezpieczeństwa sieci i problemów z tym związanych. Należy przypomnieć studentowi podstawową wiedzę z zakresu sieci komputerowych i protokołów sieciowych oraz przedstawić szeroki wachlarz potencjalnych ataków i incydentów, które mogą się pojawić. Należy zapoznać studenta z systemami pasywnymi i aktywnymi pozwalającymi wykrywać i reagować na incydenty.

Na laboratorium student powinien nauczyć się wykorzystywać narzędzia wspomagające wykrywanie i przeciwdziałanie atakom sieciowym oraz poznać mechanizmy wspomagające analizę ruchu sieciowego.

Przykładem realizacji takiego przedmiotu jest *Wykrywanie ataków sieciowych* (UAM).

Do wykorzystania rekomenduje się sylabus przedmiotu W*ykrywanie Ataków Sieciowych* (UAM).

Zalecane przedmioty do wyboru.

* ***Administracja usługami sieciowymi (6 ECTS, 30 w, 30 l)***

Celem przedmiotu jest zapoznanie studentów z zagadnieniami administrowania systemami, kontroli procesów sieciowych, instalacji i konfiguracji serwerowych usług sieciowych oraz doboru i odpowiedniej instalacji systemu operacyjnego w zależności od sprzętu i przeznaczenia. W trakcie przedmiotu student nauczy się budować proste sieci komputerowe, pozna podstawowe narzędzia administracyjne oraz dowie się jak w sposób bezpieczny konfigurować i udostępniać różne usługi sieciowe.

Przedmiot jest często organizowany jako obowiązkowy na studiach informatycznych I stopnia. W przypadku, gdy student realizował zadane treści we wcześniejszych etapach edukacyjnych, powinien w miejsce tego przedmiotu zrealizować odpowiednią (pod kątem punktów ECTS) ilość przedmiotów do wyboru.

W przypadku konieczności budowy nowego przedmiotu o tej tematyce, zalecenia odnośnie treści znajdują się w pliku *Rekomendacja – Administracja usługami sieciowymi*.

* ***Cybernetyczne działania wojenne (3 ECTS, 30 k)***

Celem przedmiotu jest uświadomienie studentowi wzrostu znaczenia cyberbezpieczeństwa w sferze aktywności współczesnych sił zbrojnych oraz służb specjalnych na całym świecie, a w szczególności podkreślenie nowych możliwości działania w konfliktach zbrojnych, ale również w dobie spokoju. W tym celu należy pokazać studentowi militaryzację i sekurytyzację domeny cyber, przyczyniające się do budowania potencjału zarówno defensywnego, jak i ofensywnego we współczesnych siłach zbrojnych. Dodatkowo należy uświadomić studentom możliwość spotkania się z wrogą aktywnością w cyberprzestrzeni, która może być pochodną cyberszpiegostwa lub cyberuderzeń wynikających z przyczyn politycznych, wojskowych, szpiegowskich oraz gospodarczych.

Przykładem realizacji takiego przedmiotu jest *Cybernetyczne działanie wojenne* (UAM).

Do wykorzystania rekomenduje się sylabus przedmiotu *Cybernetyczne działanie wojenne* (UAM).

* ***Inżynieria wsteczna złośliwego oprogramowania (3 ECTS, 30 l)***

Celem przedmiotu jest zapoznanie studenta z różnymi typami, zasadami działania oraz sposobami analizy złośliwego oprogramowania. Powinno się pokazać studentowi w jaki sposób analizować pliki binarne, zrzut pamięci, złośliwe skrypty, pliki dokumentów pakietu Office, pliki pdf. Student powinien poznać podstawy analizy kodu, umieć korzystać z deasemblera, rozumieć kod napisany w asemblerze.

Przykładem realizacji takiego przedmiotu jest *Inżynieria wsteczna złośliwego oprogramowania* (UAM).

Do wykorzystania rekomenduje się sylabus przedmiotu *Inżynieria wsteczna złośliwego oprogramowania* (UAM).

* ***Kryminalistyka cyfrowa (3 ECTS, 30 l)***

Celem przedmiotu jest zapoznanie studenta z metodami pozyskiwania, zabezpieczania i analizy danych cyfrowych. W tym celu student powinien zostać zaznajomiony z podstawowymi pojęciami związanymi z kryminalistyką cyfrową, metodami pozyskiwania oraz zabezpieczania danych, aby miały wartość dowodową z różnych nośników danych i różnych źródeł, metodami analizy danych oraz prawidłowym raportowaniem wykonanej analizy.

Student powinien poznać różne narzędzia wspierające pracę pozyskiwania i analizowania danych cyfrowych.

Zalecenia odnośnie treści przedmiotu znajdują się w dokumencie *Rekomendacje – Kryminalistyka cyfrowa.*

* ***Kryptografia post-kwantowa (3 ECTS, 30 l)***

Celem przedmiotu jest zapoznanie studentów z matematycznymi konceptami oraz algorytmami, stosowanymi do budowy systemów trudnych do złamania nawet dla komputerów kwantowych. W odróżnieniu od kryptografii kwantowej, kryptografia postkwantowa nie wymaga wykorzystania zjawisk kwantowych w celu osiągnięcia tajności danych.

W ramach przedmiotu student rozwija umiejętności analizowania bezpieczeństwa systemu informatycznego oraz wykorzystania aparatu matematycznego w procesie analizy i tworzenia systemu informatycznego. Ponadto student zapoznaje się z algorytmami i protokołami kryptologicznymi odpornymi na ataki z wykorzystaniem komputera kwantowego.

W celu weryfikacji nabytych kompetencji wśród form weryfikacyjnych powinien znaleźć się projekt indywidualny.

Przykładem realizacji takiego przedmiotu jest *Kryptografia post-kwantowa* (UAM).

Do wykorzystania rekomenduje się sylabus przedmiotu *Kryptografia post-kwantowa* (UAM)*.*

* ***Programowanie sieciowe w języku C (6 ECTS, 30 w, 30 l)***

Celem przedmiotu jest przekazanie studentowi wiedzy nt. mechanizmów wymiany wiadomości w sieciach komputerowych oraz zasad projektowania architektury klient-serwer. Student nabywa praktyczne umiejętności tworzenia oprogramowania realizującego komunikację sieciową na poziomie warstw 4 – 7 modelu OSI.

Alternatywnie można realizować przedmiot w innych językach, itp. Java.

Zalecenia odnośnie treści przedmiotu znajdują się w dokumencie *Rekomendacje – Programowanie sieciowe w języku C.*

* ***Sztuczna inteligencja w cyberbezpieczeństwie (3 ECTS, 30 k)***

Celem przedmiotu jest zapoznanie studenta z możliwościami wykorzystania sztucznej inteligencji w zwiększaniu bezpieczeństwa systemów informacyjnych, ale również uświadomienie zagrożeń wynikających z powstających narzędzi opartych o AI w cyberprzestrzeni. Student powinien poznać możliwości tworzenia automatycznych narzędzi do wykrywania i analizy incydentów występujących w cyberprzestrzeni, monitorowania ruchu sieciowego, wykrywania wiadomości phishingowych czy wykrywania złośliwego oprogramowania. Student musi również mieć świadomość jak AI może zostać wykorzystana do siania zagrożenia w cyberprzestrzeni poprzez itp. generowanie fake newsów, fałszywych tożsamości, wizerunków, wiadomości phishingowych, wysyłania spamu czy ataków kryptograficznych.

Zalecenia odnośnie treści przedmiotu znajdują się w dokumencie *Rekomendacje – Sztuczna inteligencja w cyberbezpieczeństwie.*

* ***Wykrywanie incydentów (3 ECTS, 30 l)***

Celem przedmiotu jest zapoznanie studenta z szerokim wachlarzem incydentów, które mogą mieć miejsce w cyberprzestrzeni, metodami ich wykrywania oraz sposobami ich obsługi. W tym celu student powinien poznać środowisko, technologie i narzędzia wykorzystywane do wykrywania i zarządzania incydentami, znać różnice pomiędzy narzędziami typu SIEM/IDS/IPS. Student powinien rozumieć i identyfikować różne zagrożenia typu phishing, eskalacja uprawnień, ataki na zewnętrzne usługi sieciowe.

Przykładem realizacji takiego przedmiotu jest *Wykrywanie incydentów* (UAM).

Do wykorzystania rekomenduje się sylabus przedmiotu *Wykrywanie incydentów* (UAM).

* ***Zaawansowane algorytmy kombinatorycznych (3 ECTS, 30 ć)***

Celem przedmiotu jest zapoznanie studenta z praktycznym zastosowaniem algorytmów kombinatorycznych. Powinno się zapoznać z algorytmami generowania, kodowania i rozkodowywania podstawowych obiektów kombinatorycznych, zapoznać z metodami dokładnego i przybliżonego rozwiązywania trudnych obliczeniowo problemów optymalizacyjnych. Student powinien nabyć umiejętność oceniania i porównywania tych algorytmów.

Przykładem realizacji takiego przedmiotu jest *Zaawansowane algorytmy kryptograficzne* (UAM).

Do wykorzystania rekomenduje się sylabus przedmiotu z pliku *Zaawansowane algorytmy kryptograficzne* (UAM).

* ***Zabezpieczenia protokołów sieciowych (3 ECTS, 30 l)***

Celem przedmiotu jest zapoznanie studenta z konfiguracją urządzeń sieciowych pozwalających obsługiwać średniej wielkości sieć lokalną oraz zabezpieczenie jej w kontekście bezpiecznego przesyłania informacji. Student musi zostać zaznajomiony z możliwymi atakami na infrastrukturę sieciową oraz przesyłane treści, metodami ich wykrywania oraz technikami wykorzystania bezpiecznych protokół do komunikacji i przesyłania informacji.

Przykładem realizacji takiego przedmiotu jest *Zabezpieczenia protokołów sieciowych* (UAM).

Do wykorzystania rekomenduje się sylabus przedmiotu *Zabezpieczenia protokołów sieciowych* (UAM)*.*

Obowiązkowe przedmioty dodatkowe dla studiów czterosemestralnych.

Przedmiot z tej grupy mogą być również rekomendowane studentom studiów trzysemestralnych do dodatkowego zaliczenia w ramach uzupełnienia braków z wcześniejszych etapów edukacji:

* ***Administracja usługami sieciowymi (6 ECTS, 30 w, 30 l)***

Opis przedmiotu powyżej w sekcji *Zalecane przedmioty do wyboru* dla studiów trzysemestralnych.

* ***Inżynieria wsteczna złośliwego oprogramowania (3 ECTS, 30 l)***

Opis przedmiotu powyżej w sekcji *Zalecane przedmioty do wyboru* dla studiów trzysemestralnych.

* ***Kryminalistyka cyfrowa (3 ECTS, 30 l)***

Opis przedmiotu powyżej w sekcji *Zalecane przedmioty do wyboru* dla studiów trzysemestralnych.

* ***Programowanie sieciowe w języku C (6 ECTS, 30 w, 30 l)***

Opis przedmiotu powyżej w sekcji *Zalecane przedmioty do wyboru* dla studiów trzysemestralnych.

* ***Zaawansowane algorytmy kombinatorycznych (3 ECTS, 30l)***

Opis przedmiotu powyżej w sekcji *Zalecane przedmioty do wyboru* dla studiów trzysemestralnych.

# Rekomendacje w zakresie dodatkowych form kształcenia

W ramach projektu *AI Tech*, oprócz standardowych form kształcenia, wprowadzono szereg dodatkowych form uzupełniających i wzbogacających ścieżkę edukacyjną. Kluczowe formy to: projekty badawczo-rozwojowe bądź projekty informatyczne (wdrożeniowe), oferty płatnych staży oraz krótkich wizyt studyjnych u pracodawców, finansowany ze środków uczelni udział studentów w konferencjach zarówno krajowych, jak i międzynarodowych, szkoły letnie oraz indywidualne wsparcie dla studenta w formie tutoringu. Za wyjątkiem staży wszystkie powyższe formy realizowane były na wszystkich uczelniach partnerskich projektu *AI Tech*. Zgromadzone doświadczenia pozwalają stwierdzić, że te dodatkowe formy kształcenia sprzyjają aktywnemu i wszechstronnemu rozwojowi studenta, porządkując wiedzę teoretyczną i nadając jej praktyczny wymiar odpowiednio umieszczonej w najnowszym kontekście dynamicznie rozwijającej się problematyki cyberzagrożeń, bezpieczeństwa oraz analiz ryzyka i skutków podatności.

Poniżej przedstawiono rekomendacje odnośnie ww. form.

## Staże i wizyty studyjne

Jednym z istotnych elementów kształcenia jest przekazanie studentom wiedzy na temat funkcjonowania rynku pracy oraz realiów pracy na stanowiskach powiązanych z cyberbezpieczeństwem. Ten cel realizują formy dydaktyczne tj. praktyki, staże oraz wizyty studyjne. Każda z tych form wymaga, by uczelnia aktywnie prowadziła politykę współpracy z otoczeniem społeczno-gospodarczym.

### Praktyki

Zgodnie z rozwiązaniami przyjętymi w analizowanych programach studiów, rekomendowany model wzorcowy nie przewiduje praktyk (w ich miejsce proponując staże i wizyty studyjne). Jednak to od uczelni zależy, czy zdecyduje się ona na wprowadzenie praktyk jako obowiązkowych do programu studiów. Jeśli tak, to powinny im zostać przypisane punkty ECTS (domyślnie 6) oraz liczba wymaganych godzin do zrealizowania (min. 160). Obowiązkowe praktyki mogą wówczas zastąpić jeden z przedmiotów obieralnych wymienionych w rekomendowanym programie studiów. Uczelnie zazwyczaj organizują praktyki zgodnie z wewnętrznymi regulaminami praktyk na podstawie umów trójstronnych z pracodawcą oraz studentem i do nadzorowania ich realizacji mają powołanego opiekuna praktyk. Należy zwrócić uwagę na to, by zapewnić studentom możliwość realizacji praktyk w firmach, które mają istotne aspekty cyberbezpieczeństwa w profilu swojej działalności lub posiadają rozbudowane działy informatyczne skupione wokół zabezpieczenia danych, komunikacji bądź stabilności działania systemów. Uczelnia powinna także określić program takich praktyk. Ustawą z dnia 1 grudnia 2022 r. o zmianie ustawy Prawo o szkolnictwie wyższym i nauce oraz niektórych innych ustępów art. 67 dodano ust. 7., który umożliwia zaliczenie na poczet praktyki zawodowej czynności wykonywanych przez studenta w ramach m.in. zatrudnienia, stażu lub wolontariatu, jeżeli umożliwiły one uzyskanie efektów uczenia się określonych w programie studiów dla praktyk zawodowych.

### Staże

Rekomendowaną formą dydaktyczną są staże organizowane są we współpracy uczelni z partnerami gospodarczymi, naukowymi, ośrodkami badawczo-rozwojowymi lub innymi podmiotami, które oferują możliwość zdobycia doświadczenia w szeroko pojętym obszarze cyberbezpieczeństwa. Staże, w odróżnieniu od praktyk są nieobowiązkowe oraz wiążą się z wynagrodzeniem dla studenta i dłuższym okresem zatrudnienia. Odbywają się na podstawie dwustronnej umowy pomiędzy firmą a studentem. Rekomendowany okres stażu to 1-2 miesięcy, zatem powinny być organizowane w wakacyjnym okresie wolnym od obowiązkowych zajęć dydaktycznych.

Niektóre uczelnie w Polsce prowadzą (zwykle poprzez uczelniane Biura Karier) wykazy firm oferujących staże oraz oferują studentom wsparcie od strony organizacyjnej (pisanie CV, kierowanie do odpowiednich placówek na badania lekarskie, itp.).

Staże oraz wizyty studyjne powinny być koordynowane odgórnie przez specjalnie powołaną komisję. Komisja ta w pierwszej kolejności powinna skompletować ofertę staży prowadząc odpowiednie rozmowy z potencjalnymi pracodawcami. Aby usprawnić ten proces uczelnia mogłaby stworzyć sieć partnerstwa z firmami technologicznymi z najbliższego otoczenia gospodarczego w celu utworzenia stabilnego rdzenia oferty stażowej. Jednocześnie komisja powinna poszukiwać kontaktów również w dalszej odległości, w szczególności wśród firm międzynarodowych.

### Wizyty studyjne

Kolejną rekomendowaną dodatkową formą dydaktyczną są wizyty studyjne u pracodawców. Zalecane jest, aby wizyty te odbywały się stacjonarnie w siedzibie zapraszającej firmy, jednakże w szczególnych przypadkach mogą to być wizyty zdalne (np. w firmach z siedzibą za granicą, bądź w przypadku, gdy firma z powodu wewnętrznych regulaminów nie może wpuszczać osób postronnych na swój teren).

Wizyty studyjne stanowią istotny element kształcenia na kierunku *Cyberbezpieczeństwo*. Są one zaprojektowane tak, aby umożliwić studentom zapoznanie się z praktycznymi zastosowaniami teorii, które omawiane są na wykładach oraz stworzyć pole do interakcji z praktykami. Każde spotkanie obejmuje prezentację firmy, jej działalności, wykorzystywanych narzędzi IT, a także otwiera przestrzeń dla interakcji, takich jak dyskusje czy zadania dla uczestników. Na podstawie doświadczeń zebranych w trakcie trwania projektu *AI Tech* zbudowano następujące rekomendacje dla wizyt studyjnych:

* optymalny czas trwania pojedynczej wizyty to ok. 3 dni,
* rozmiar wizytującej grupy powinien być niewielki, od 5 do 8 studentów,
* każdy student zobowiązany jest do odbycia minimum jednej wizyty studyjnej, a zalecane jest odbycie co najmniej dwóch wizyt,
* po wizycie każdy student zobowiązany jest do zdania pisemnego sprawozdania,
* powinna być powołana komisja (np. ta sama co w przypadku staży) gromadząca oferty staży i budująca listy rankingowe uwzględniającej aktywność studentów (średnią ocen, obecność na zajęciach itp.), ale jednocześnie pozwalającą na objęcie tą formą wsparcia możliwie szerokiej grupy studentów (ilość już realizowanych wizyt, pierwsza wizyta jest obowiązkowa),
* uczelnia określa czytelne i przejrzyste zasady finansowania wyjazdu; rekomendowane jest finansowanie kosztów pobytu ze środków uczelni.

Dodatkowo, warto zachęcić opiekuna i studentów do przygotowania i przedstawienia relacji z realizowanej wizyty w celach promocyjnych w mediach społecznościowych i Internecie, z poszanowaniem uzgodnień z wizytowanym podmiotem i uczelnią.

## Współpraca krajowa w tym ze środowiskiem biznesowym

Współpraca krajowa ma na celu twórcze zintegrowanie środowisk akademickich i biznesowych. Jej elementami są wymiana doświadczeń oraz transfer wiedzy. Głównymi formami współpracy krajowej, w szczególności ze środowiskiem biznesowym, w ramach tworzonego kierunku studiów będą: projekty badawczo-rozwojowe, staże bądź praktyki, wizyty studyjne, szkoły letnie oraz krajowe konferencje naukowe i branżowe.

Rekomendujemy organizację cyklicznych wykładów, spotkań i warsztatów z udziałem przedstawicieli firm technologicznych, w tym w ramach szkół letnich. Daje to studentom kolejną możliwość poznania najnowszych trendów i rozwiązań stosowanych w praktyce, a biznesowi możliwość prezentacji ścieżek kariery oraz wymagań stawianych przyszłym pracownikom.

### 

### Udział w konferencjach

Zaleca się wprowadzenie szczegółowej i klarownej procedury aktywnego udziału studentów w konferencjach naukowych. Udział studentów w konferencjach, nawet w trybie zwykłego słuchacza, daje szanse na znaczne poszerzenie horyzontów naukowych, rozwój kompetencji osobistych oraz budowanie sieci kontaktów. Jest zatem bardzo istotnym narzędziem dydaktycznym i powinien być oferowany studentom, jeżeli tylko pozwala na to sytuacja finansowa uczelni. Lista potencjalnie interesujących konferencji z zakresu *Cyberbezpieczeństwa* powinna być tworzona i publikowana przez specjalnie powołaną komisję oceniającą. Udział najlepszych studentów w rekomendowanej konferencji powinien być refundowany ze środków uczelni. Studenci tacy powinni być wytypowani na podstawie listy rankingowej stworzonej przez ww. komisję na podstawie: osiągnięć studenta na polu dydaktycznym, aktywności w dodatkowych formach edukacyjnych (np. kołach), ilości konferencji na jakich już student uczestniczył. Stworzona procedura powinna pozwalać na objęcie tą formą dydaktyczną jak najszerszej grupy studentów, przy jednoczesnej zachęcie do bardziej intensywnego udzielania się studenta na polu dydaktycznym. Na daną konferencję nie powinna być kierowana jednorazowo zbyt duża grupa studentów i powinna w trakcie konferencji mieć opiekę ze strony przydzielonego opiekuna naukowego, któremu po zakończeniu konferencji studenci będą musieli zdać raport z wysłuchanych wystąpień.

### 

### Szkoły letnie

Przez szkołę letnią rozumie się kilkudniowy kurs dla studentów organizowany najczęściej w czasie wolnym od zajęć dydaktycznych. Celem szkoły letniej ma być pogłębienie wiedzy i umiejętności studentów w zakresie zagadnień merytorycznych i praktycznych poprzez kontakt z wybitnymi przedstawicielami nauki i biznesu, ale także nawiązanie kontaktów naukowych i zawodowych. Podobnie jak w przypadku wizyt studyjnych bądź konferencji, zaleca się by uczelnia prowadziła wykaz rekomendowanych szkół na jakie mogą samodzielnie aplikować studenci. W przypadku chęci samodzielnej organizacji takiej szkoły, uczelnia powinna rozważyć przede wszystkim współpracę z inną uczelnią bądź ośrodkiem badawczym oraz zapraszać do wystąpienia przedstawicieli otoczenia społeczno-gospodarczego (w szczególności dużych firm międzynarodowych) oraz cenionych nauczycieli akademickich z innych ośrodków, w tym zagranicznych. Warto rozważyć uatrakcyjnienie takiej szkoły przez różnego rodzaju panele, krótkie projekty kilkuosobowe oraz konkursy i hackathony.

## Współpraca międzynarodowa

Rekomendujemy, aby studia były realizowane we współpracy międzynarodowej, z położeniem nacisku na rozwijanie międzynarodowych relacji naukowych i umożliwienie studentom zdobywania umiejętności pozwalających na pracę w zglobalizowanym świecie technologii. Studenci mają wówczas możliwość współpracy zarówno z naukowcami jak i praktykami z całego świata.

Uczelnia powinna zadbać o nawiązanie i wzmocnienie współpracy międzynarodowej, włączając w to pozyskanie naukowców. Należy kłaść nacisk na to, by przewidziane w planie wizyty studyjne, staże oraz udział konferencjach czy szkołach letnich, realizowane były w środowisku międzynarodowym, zarówno w krajach w UE, jak i w krajach spoza UE. Zabiegi te mają służyć rozwinięciu umiejętności akademickich studentów kierunku, ale pozwoli to też na zdobycie praktycznego doświadczenia w budowaniu międzynarodowych sieci kontaktów zawodowych i naukowych.

## Projekty informatyczne

W niniejszej koncepcji modelu systemowego kształcenia na kierunku lub specjalności *Cyberbezpieczeństwo* projekty informatyczne są rozumiane szerzej – jako projekty badawczo-rozwojowe.

Głównym celem projektów badawczo-rozwojowych jest realizacja przez studentów ambitnych przedsięwzięć o charakterze naukowym lub praktycznym z zakresu cyberbezpieczeństwa. Te projekty stanowią platformę pozwalającą studentom na konkretne zastosowanie zdobytej wiedzy i umiejętności w rozwiązywaniu realnych wyzwań, wdrażaniu technik cyberbezpieczeństwa oraz ocenie ich efektywności.

Przewiduje się, że tematyka projektów będzie dokładnie określona i realizowana w ścisłej współpracy z partnerami społeczno-gospodarczymi uczelni lub pracownikami uczelni prowadzącymi interdyscyplinarne badania, w których cyberbezpieczeństwo pełni istotną rolę.

Rekomenduje się, aby realizacji projektów badawczo-rozwojowych towarzyszyły następujące działania:

* Powołanie koordynatora lub zespołu ds. koordynacji projektów, odpowiedzialnego za selekcję projektów, opiniowanie potencjalnych opiekunów oraz nadzór nad współpracą studentów z interesariuszami i prawidłowość realizacji przedmiotu, w tym zaliczanie semestru I.
* Stworzenie systemu zgłaszania tematów projektów, otwartego dla pracowników uczelni i podmiotów z otoczenia społeczno-gospodarczego. Warto zbierać pomysły na tematy projektów w trakcie wizyt studyjnych u podmiotów partnerskich.
* Wyznaczenie opiekuna projektu ze strony zgłaszającego temat, który będzie odpowiadał za określenie problematyki projektu oraz ocenę rozwiązań. Może to być przedstawiciel firmy z otoczenia gospodarczego (opiekun techniczny), bądź przedstawiciel kadry naukowej uczelni (opiekun naukowy), niekoniecznie z wydziału prowadzącego kierunek *Cyberbezpieczeństwo*.
* Zapewnienie studentom wsparcia merytorycznego przez doświadczonych pracowników wydziału podczas realizacji projektów (na przykład poprzez rolę tutora, bądź osób wyznaczonych do zespołu koordynującego przedmiot).
* Zapewnienie, że projekty badawczo-rozwojowe będą realizowane przez zespoły składające się z 3-5 studentów. Daje to sposobność do rozwijania umiejętności pracy grupowej. Przewiduje się dwusemestralny cykl realizacji projektów, z około 30 godzinami zajęć dydaktycznych w każdym semestrze. Projekt badawczo-rozwojowy jest planowany jako obowiązkowa forma kształcenia dla wszystkich studentów.
* Należy szczegółowo określić prawa autorskie i majątkowe studentów w odniesieniu do wyników ich pracy, szczególnie w przypadku projektów realizowanych we współpracy z otoczeniem społeczno-gospodarczym.
* Należy również umożliwić studentom prezentację i dyskusję wyników projektów badawczo-rozwojowych, w tym publiczne prezentacje na forum społeczności wydziału oraz zaproszonych przedstawicieli otoczenia gospodarczego uczelni. W zależności od charakteru projektu i ewentualnych ograniczeń narzuconych przez zleceniodawcę projektu, można rozważyć także publikację wyników projektu w formie naukowej, zgłoszenia patentowego, raportu technicznego lub publikacji.

W tej sugerowanej koncepcji systemu edukacyjnego projektom badawczo-rozwojowym przypisuje się łącznie 10 punktów ECTS w ciągu dwóch semestrów, co przekłada się na 150-300 godzin pracy każdego studenta nad projektem.

Oprócz obowiązkowych projektów badawczo-rozwojowych, zaleca się zaangażowanie studentów w jak największą liczbę projektów realizowanych na uczelni, włączając w to także projekty grantowe.

## Tutoring

Tutoring to zorganizowana zindywidualizowana praca, szczególnie z wybitnymi i zmagającymi się z trudnościami studentami (1:1, w małych grupach, rzadziej w większych grupach) w ramach programów/zajęć na uczelni (lub online), uwzględniająca różnorodność doświadczeń studentów, dyscyplin, umiejętności akademickich, specjalizacji, potrzeb, oczekiwań itp. i umożliwiająca studentom osiągnięcie celów akademickich i rozwojowych (definicja MNiSW na potrzeby projektu *Mistrzowie dydaktyki*).

Wśród celów prowadzenia tutoringu w uczelni wyższej za główny należy uznać przestawienie studenta z pasywnego na aktywnego odbiorcę usługi edukacyjnej, co prowadzi do zwiększenia efektów kształcenia oraz może przeciwdziałać zjawisku przedwczesnego opuszczania systemu kształcenia (rezygnacja ze studiów w trakcie ich trwania, tzw. zjawisko *drop-out* – [https://radon.nauka.gov.pl/analizy/dropout,](about:blank) dostęp z dnia 27.10.2023). Tutoring może także ułatwić funkcjonowanie studentom z zagranicy, którzy muszą odnaleźć się w nowym dla nich środowisku.

Uczelniom, które mają odpowiednie możliwości kadrowe i finansowe, rekomenduje się objęcie tutoringiem wszystkich studentów. W przypadku braku takich możliwości wsparciem tego typu należy objąć przede wszystkim studentów, którzy wyrażą chęć przystąpienia do programu tutoringowego, zwłaszcza wybitnie uzdolnionych oraz zmagających się z trudnościami (w tym niepełnosprawnością).

Rekomendacje odnośnie organizacji tutoringu zakładają szerokie podejście do wsparcia udzielanego studentom przez pracowników akademickich w sprawach akademickich i osobistych. Obejmuje to również informacje na temat procesów występujących w szkolnictwie wyższym, procedur i oczekiwań, informacji zwrotnych i rozwoju akademickiego oraz wsparcia opieki społecznej (Gray & Osborne, 2018). Brak zainteresowania przedmiotem studiów oraz problemy osobiste zostały zidentyfikowane jako główne przyczyny rezygnacji ze studiów przed uzyskaniem dyplomu ([https://radon.nauka.gov.pl/analizy/dropout,](about:blank) dostęp z dnia 27.10.2023).

W kontekście studiów na kierunku/specjalności *Cyberbezpieczeństwo*, głównym zadaniem tutora jest wspieranie rozwoju akademickiego studenta. Obejmuje to sugerowanie przedmiotów obieralnych, lektur uzupełniających, konsultowanie tematyki projektu, pomoc w wyborze, miejsca stażu, wizyty studyjnej, konferencji oraz inne konsultacje dotyczące naukowego i osobistego rozwoju studenta, w tym pomoc w doborze publikacji do przeczytania oraz sposobu ewentualnego spisania wyników projektu badawczo-rozwojowego w formie publikacji bądź raportu technicznego. Tutor również powinien wspierać studenta w pozyskiwaniu informacji nt. wsparcia socjalnego i wsparcia rozwoju osobistego ze strony uczelni.

Najbardziej efektywnym modelem jest tutoring indywidualny (1:1), który był realizowany na Uniwersytecie Warszawskim i Politechnice Gdańskiej. Student powinien mieć możliwość wyboru tutora spośród osób wskazanych przez uczelnię lub także osób z zewnątrz, zależnie od ustaleń wewnętrznych uczelni. Wstępną listę rekomendowanych tutorów powinna sporządzać specjalna komisja co najmniej dwa tygodnie przed rozpoczęciem każdego semestru. Ta sama komisja powinna mieć możliwość weryfikacji i zatwierdzania kandydatury tutora spoza listy. Studenci powinni mieć możliwość skorzystania z przynajmniej dwóch godzin tutoringu w każdym pierwszym miesiącu semestru oraz po minimum jednej godzinie w pozostałych miesiącach, zgodnie z harmonogramem spotkań ustalonym z tutorami. Po każdym spotkaniu studenci powinni sporządzić krótką notatkę i przesłać ją tutorowi, co służy podkreśleniu odpowiedzialności studenta za proces tutoringu oraz pozwala na kontrolowanie czy rozmowy i ustalenia w trakcie spotkań zostały dobrze zrozumiane. Bardzo ważna jest też co semestralna ewaluacja procesu tutoringu, na przykład poprzez ankiety oraz co semestralne studenckie raporty podsumowujące.

Rekomendacje odnośnie tutorów skupiają się na wyborze odpowiednich osób do pełnienia tej roli. Tutor powinien być nauczycielem akademickim lub inną osobą, która posiada wiedzę i doświadczenie związane z procesem kształcenia ekspertów z dziedziny cyberbezpieczeństwa oraz komunikuje się sprawnie, w tym ma umiejętność słuchania, zadawania pytań i aktywnego wyjaśniania. Tutorzy powinni być przeszkoleni w zakresie zadań oraz metod tutoringu, a także zakresu wsparcia socjalnego i wsparcia rozwoju osobistego oferowanego przez uczelnię. Ważne jest także, aby tutorzy mieli ograniczoną liczbę studentów pod swoją opieką jednocześnie, co pozwala na efektywną pracę. Łączna liczba podopiecznych u danego tutora nie powinna przekroczyć 5 osób. Uczelnia powinna jasno określić zasady rozliczania pracy tutorów, włączając w to zasady wynagradzania za tę pracę. Dla tutorów zewnętrznych powinien zostać przygotowany pakiet informacyjny zawierający m.in. wskazówki i procedury odnoszące się do oferowanych przez uczelnię form wsparcia (stypendia socjalne, opcje wyjazdów na wymiany studenckie itp.).

Wskazówki odnośnie realizacji procesu tutoringu w szkole wyższej uczelnie mogą znaleźć w publikacji J. Brdulak, J. Gotlib, R. Koziołek, J. Uriasz: *Model tutoringu* (2019) powstałej w ramach projektu MNiSW *Mistrzowie dydaktyki*

([https://www.gov.pl/attachment/8fd3a897-d990-4034-b216-b0f669d1e102,](about:blank) dostęp z dnia 27.10.2023).

Jeśli możliwości uczelni na to pozwalają, studentom można również oferować wzięcie udziału w programie mentoringowym, który jest nastawiony na odkrywanie cech wewnętrznych, indywidualnych predyspozycji i celów życiowych studentów (Dr. Beverly J. Irby (2018) *Editor’s Overview: Differences and Similarities with Mentoring, Tutoring, and Coaching*, Mentoring & Tutoring: Partnership in Learning, 26:2, 115-121,

<https://doi.org/10.1080/13611267.2018.1489237,> dostęp z dnia 27.10.2023)

# Materiały dydaktyczne

Rekomendujemy, aby studia były prowadzone w oparciu o rzetelnie przygotowane materiały dydaktyczne, zarówno pod względem treści, jak i formy. Warto ustalić sugerowany wzorzec materiałów i dbać o ich jednolitą postać. Kluczowa jest jednak weryfikacja merytoryczna, dlatego materiały dydaktyczne powinny być przygotowywane zespołowo. Dobrą praktyką jest powołanie zespołu koordynacyjnego i przygotowanie procedury zapewnienia jakości i poprawności merytorycznej materiałów dydaktycznych.

Materiały wykładowe zwyczajowo mają formę slajdów w formacie pdf. W przypadku, gdy materiały oferowane są w formatach docx/odt bądź pptx/odp zalecane jest dodatkowe udostępnienie plików skonwertowanych do pdf. Jest to podyktowane koniecznością odczytywania materiałów na rozmaitych systemach operacyjnych (w tym Android) jakimi mogą dysponować studenci. Ponadto do każdego przedmiotu powinny być rekomendowane bądź udostępniane materiały uzupełniające. W zależności od tematyki przedmiotu mogą to być przykładowe kody i konfiguracje czy też nagrania wideo tj. zweryfikowane tutoriale online, nagrania wykładów, fragmenty nagrań z wizyt studyjnych, wideo-raporty z eksperymentów dużych agencji, itp. Ponadto student powinien być zachęcany do zapoznawania się z najnowszymi, bądź najistotniejszymi publikacjami naukowymi z danego obszaru. Takie materiały warto zamieszczać na dedykowanych platformach e-learningowych hostowanych przez uczelnię. Przykładem takiego oprogramowania jest otwarto-źródłowy Moodle.

Materiały do zajęć laboratoryjnych powinny zawierać w sobie elementy interaktywności. Jednym z aktualnych rozwiązań, chętnie wykorzystywanym w badanych cyklach kształcenia, są notatniki interaktywne w formacie Jupyter Notebook. Pomimo, iż kojarzone są przede wszystkim z wykorzystaniem języka Python w obszarze eksploracji danych, notatniki Jupyter można z powodzeniem wykorzystać do nauki szerokiej gamy języków, w tym języka C w zastosowaniach sieciowych. Można je też wykorzystać na laboratoriach poświęconych algorytmice, kryptografii, programowaniu usług sieciowych, a nawet testowaniu podatności systemów. Dla wielu laboratoriów na studiach z cyberbezpieczeństwa wartościowe byłoby przygotowane wirtualne laboratoriów, które student mógłby wykorzystywać zarówno w trakcie zajęć na uczelni, ale również mógłby je pobrać i pracować z nimi w domu. Przykładami takich rozwiązań są gotowych kontenery typu docker czy obrazy systemów wirtualnych. Zaletą kontenerów jest prostota w ich instalacji, przenaszalność pomiędzy różnymi systemami operacyjnymi i możliwość mało kłopotliwego stworzenia dowolnej konfiguracji oprogramowania. Natomiast trudne jest zachowanie zmian i wyeksportowanie ich do dalszej pracy w domu. Z drugiej strony można także przygotowywać obrazy wirtualnych maszyn, które są mocno rozbudowane, można zapisywać i przenosić ich stan (pod warunkiem posiadania obszernej pamięci USB), ale są też mocno obciążające dla systemu podstawowego (hostującego).

Należy też pamiętać o jednym z celów dydaktycznych, jakim jest pogłębienie u studentów świadomości konieczności stałego samodoskonalenia i pozyskiwania nowej wiedzy. Dlatego należy w procesie dydaktycznym zawrzeć elementy wymagające od studentów poszukiwania wiedzy w publikacjach naukowych i raportach głównych agencji CERT.

# Dodatkowe rekomendacje

**Wykładowy język angielski**

Proponowany model kształcenia warto rozszerzyć przez zmianę dla części (lub wszystkich) przedmiotów języka wykładowego na język angielski. Większa liczba przedmiotów prowadzonych w języku angielskim ułatwi absolwentom wzorcowego kierunku późniejsze samodoskonalenie i zrozumienie najświeższych wyników badań w zakresie cyberbezpieczeństwa. Dodatkowo, propozycja taka otworzy prowadzone studia zarówno na kandydatów zagranicznych jak i ułatwi rekrutację kadry spośród ekspertów w danej dziedzinie.

# Podsumowanie

Niniejsze opracowanie opisuje koncepcję oraz rekomendacje dla modelu systemowego kształcenia na kierunku *Cyberbezpieczeństwo*. Powstało ono jako efekt analiz materiałów przygotowanych w trakcie realizacji projektu *AI Tech*. Do tych materiałów należy zaliczyć opracowania ankiet wśród pracodawców, studentów oraz kandydatów na studia, założenia programowe opracowane przez Radę Programową projektu oraz materiały i doświadczenia wypracowane przez pięć uczelni partnerskich projektu. Kluczowymi dla niniejszego opracowania były materiały opracowane przez Uniwersytet im. Adama Mickiewicza w Poznaniu dla specjalności *Cyberbezpieczeństwo* na kierunku *Informatyka*.

Zaprezentowane zostały dwie koncepcje. Wiodącą jest koncepcja studiów trzysemestralnych na kierunku *Cyberbezpieczeństwo*, ale przygotowana została również koncepcja studiów czterosemestralnych. Studia te są przypisane w 100% do dyscypliny *Informatyka* w dziedzinie nauk ścisłych i przyrodniczych, ale można je też z powodzeniem przypisać do dyscypliny informatyka techniczna i telekomunikacja w dziedzinie nauk inżynieryjno-technicznych.

W dokumencie opisano cele kształcenia na kierunku *Cyberbezpieczeństwo* oraz przedstawiono sylwetkę absolwenta. W skrócie omówiono plany i programy studiów, których pełne wersje stanowią załączniki do niniejszego dokumentu. Opisano też proponowane przedmioty, którymi można uzupełnić program kształcenia w formie przedmiotów do wyboru. Do każdego omówionego przedmiotu załączony został albo sylabus przygotowany w ramach projektu *AI Tech* przez UAM, albo dokument rekomendacji treści dla sugerowanego, nie istniejącego jeszcze przedmiotu. W zależności od zasobów uczelni wdrażającej opracowane koncepcje, rekomendacje treści oraz sylabusy można odpowiednio dostosowywać do własnych potrzeb pod warunkiem realizacji odpowiednich efektów kształcenia. W bieżącym dokumencie znajdują się również rekomendacje odnośnie konstrukcji materiałów dydaktycznych.

Istotnym elementem projektu *AI Tech* oraz realizowanych w jego ramach pilotażowych cyklów kształcenia było zastosowanie innowacyjnych form kształcenia. Zebrane doświadczenia posłużyły przygotowaniu w ramach tego dokumentu rekomendacji w tym zakresie. Głównymi celami wprowadzenia tych metod jest nie tylko zwiększenie zaangażowania studentów i szerokie wsparcie ich rozwoju, ale również przeciwdziałanie zjawisku *drop-out*, powszechnemu w przypadku studiów informatycznych. Istotnymi elementem proponowanego modelu jest objęcie jak największej liczby studentów programem tutoringowym oraz oferowanie studentom szerokiej gamy dodatkowych form dydaktycznych tj. staże, wizyty studyjne, udział studentów w konferencjach oraz szkołach letnich. Dla tych form opisano istotne aspekty, jakie należy uwzględnić planując ich realizację.

Podsumowując, przeanalizowane efekty realizacji projektu *AI Tech* są wartościowe i zawierają istotne wskazówki dla uczelni chcących otwierać nowe kierunki studiów, w szczególności studia II stopnia na kierunku *Cyberbezpieczeństwo*. Programy i doświadczenia uczelni nabyte w ramach projektu *AI Tech* pozwoliły na przygotowanie koncepcji planu i programu studiów, które mogą być uznane za standard kształcenia specjalistów z zakresu cyberbezpieczeństwa.

# Spis aneksów i załączników

1. **Załącznik nr 1.** *C – AI TECH – Rekomendowany Plan studiów.xlsx* – rekomendowany plan studiów 3- i 4-semestralnych.
2. **Załącznik nr 2**. *C – AI TECH – Rekomendowany program studiów 3 sem.docx* – Rekomendowany program studiów 3-semestralnych
3. **Załącznik nr 3**. *C – AI TECH – Rekomendowany program studiów 4 sem.docx* – rekomendowany program studiów 4-semestralnych
4. **Załącznik nr 4.** C – AI TECH – Sylabusy – rekomendowane sylabusy przedmiotów (w folderze)