

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Język angielski
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C010.1
Rok:	II
Semestr:	3
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	30
Wykład	
Ćwiczenia	30
Laboratorium	
Projekt	
Liczba punktów ECTS:	2
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Rozwinięcie umiejętności językowych w zakresie czterech sprawności: słuchania, czytania, mówienia i pisanie na poziomie B2 Europejskiego Systemu Opisu Kształcenia Językowego
C2	Nabywanie umiejętności posługiwania się językiem angielskim w zakresie podstawowego specjalistycznego języka potrzebnego w pracy inżyniera

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Znajomość języka angielskiego na poziomie B1

Efekty uczenia się	
	W zakresie umiejętności:
EK 1	potrafi posługiwać się słownictwem dotyczącym omawianych treści programowych
EK 2	umie posługiwać się strukturami gramatycznymi omawianymi w semestrze
EK3	potrafi wypowiadać się ustnie oraz pisemnie na tematy z zakresu inżynierii w tym związane ze studiowanym kierunkiem
EK4	potrafi zrozumieć i zinterpretować wypowiedzi pisemne i ustne na tematy inżynierskie z zakresu nauk technicznych
EK5	potrafi samodzielnie korzystać z materiałów dydaktycznych
EK6	potrafi pracować samodzielnie oraz w grupie, przyjmując w niej różne role
	W zakresie kompetencji społecznych:
EK7	jest gotów do krytycznej oceny swoich umiejętności językowych i podjęcia działań na rzecz ich doskonalenia, aby skuteczniej wspierać procesy wymiany wiedzy i rozwiązywania problemów w działalności zawodowej

Treści programowe przedmiotu	
Forma zajęć - ćwiczenia	
	Treści programowe
ĆW1	Słownictwo związane z uczelnią i studiowaniem
ĆW2	Opisywanie działania urządzeń, systemów, ich funkcje, zastosowania na przykładzie wybranego systemu
ĆW3	Zalety i wady działania systemów na przykładzie nowatorskich rozwiązań wybranej firmy
ĆW4	Rodzaje materiałów – metale, niemetale, pierwiastki, związki chemiczne, mieszaniny, stopy, kompozyty
ĆW5	Właściwości materiałów; opisywanie ich specyfiki, jakości oraz przydatności w różnych procesach
ĆW6	Architektura komputera
ĆW7	Powtórzenie zastosowania czasów w języku angielskim

Metody dydaktyczne	
1	Ćwiczenia językowe konwersacyjne
2	Ćwiczenia językowe leksykalno-gramatyczne
3	Praca z tekstem źródłowym lub innymi materiałami, w tym audio i audiowizualnymi
4	Praca wykonywana w grupach
5	Praca wykonywana indywidualnie

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	Ocena pracy pisemnej	51 %
O2	Ocena odpowiedzi ustnej	51 %

Literatura podstawowa	
1	Mark Ibbotson, Cambridge English for Engineering, Cambridge 2016.

Literatura uzupełniająca	
1	Beata Błaszczyk, English 4 IT. Praktyczny kurs języka angielskiego dla specjalistów IT i nie tylko, Helion 2017.
2	Noni Rizopoulou, Academic English for Computer Science, Disigma Publ. 2022.
3	Virginia Evans, Information technology (Career Paths), Express Publishing, 2022.
4	Foley Mark, Hall Diane, My GrammarLab, Pearson.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności

Godziny kontaktowe z wykładowcą, w tym:	30
Udział w ćwiczeniach:	30
Praca własna studenta, w tym:	20
Przygotowanie do ćwiczeń:	20
Łączny czas pracy studenta	50
Sumaryczna liczba punktów ECTS dla przedmiotu	2

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK1	CB1A_U02+++ CB1A_U03++	C1,C2	ĆW1 - ĆW7	1,2,3,4,5	O1, O2
EK2	CB1A_U02+++ CB1A_U03++	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1, O2
EK3	CB1A_U02+++ CB1A_U03++	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1, O2
EK4	CB1A_U02+++ CB1A_U03++	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1, O2
EK5	CB1A_U02+++ CB1A_U03++	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1, O2
EK6	CB1A_U02+++ CB1A_U03++	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1, O2
EK7	CB1A_K01+	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1, O2

Autor programu:	mgr Sławomir Kołtun
Adres e-mail:	s.koltun@pollub.pl
Jednostka organizacyjna:	Studium Języków Obcych

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Język niemiecki
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C010.2
Rok:	II
Semestr:	3
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	30
Wykład	
Ćwiczenia	30
Laboratorium	
Projekt	
Liczba punktów ECTS:	2
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Rozwinięcie umiejętności językowych w zakresie czterech sprawności: słuchania, czytania, mówienia i pisanie na poziomie B2 Europejskiego Systemu Opisu Kształcenia Językowego
C2	Nabywanie umiejętności posługiwania się językiem niemieckim w zakresie podstawowego specjalistycznego języka potrzebnego w pracy inżyniera

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Znajomość języka niemieckiego na poziomie B1

Efekty uczenia się	
	W zakresie umiejętności:
EK1	potrafi posługiwać się słownictwem dotyczącym omawianych treści programowych
EK2	umie posługiwać się strukturami gramatycznymi omawianymi w semestrze
EK3	potrafi wypowiadać się ustnie oraz pisemnie na tematy z zakresu inżynierii w tym związane ze studiowanym kierunkiem
EK4	potrafi zrozumieć i zinterpretować wypowiedzi pisemne i ustne na tematy inżynierskie z zakresu nauk technicznych
EK5	potrafi samodzielnie korzystać z materiałów dydaktycznych
EK6	potrafi pracować samodzielnie oraz w grupie, przyjmując w niej różne role
	W zakresie kompetencji społecznych:
EK7	jest gotów do krytycznej oceny swoich umiejętności językowych i podjęcia działań na rzecz ich doskonalenia, aby skuteczniej wspierać procesy wymiany wiedzy i rozwiązywania problemów w działalności zawodowej

Treści programowe przedmiotu	
Forma zajęć - ćwiczenia	
	Treści programowe
ĆW1	Analiza potrzeb programu technologicznego - rozszerzenie
ĆW2	Zakład przemysłowy - zagadnienia różne
ĆW3	Przepisy i regulacje dotyczące bezpieczeństwa w pracy
ĆW4	Oprogramowanie związane z cyberbezpieczeństwem
ĆW5	Cyberbezpieczeństwo - rozszerzenie i utrwalenie materiału leksykalnego
ĆW6	Różne obszary sztucznej inteligencji poświęcone algorytmom
ĆW7	Różne zagadnienia gramatyczne i syntaktyczne - powtórzenie i rozszerzenie

Metody dydaktyczne	
1	Ćwiczenia językowe konwersacyjne
2	Ćwiczenia językowe leksykalno-gramatyczne
3	Praca z tekstem źródłowym lub innymi materiałami, w tym audio i audiowizualnymi
4	Praca wykonywana w grupach
5	Praca wykonywana indywidualnie

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	Ocena pracy pisemnej	51%
O2	Ocena odpowiedzi ustnej	51%

Literatura podstawowa	
1	Sabrina Schmohl, Akademe Deutsch, Hueber Verlag 2018.
2	Monika Rolbiecka, Deutsch für Profis, Lektor Klett, 2017.

Literatura uzupełniająca	
1	Ilse Sander, Deutsch im Unternehmen, Ernst Klett Sprachen, 2016.
2	Grammatik, gramatyka języka niemieckiego z ćwiczeniami, WSiP 2018.
3	Internetowa baza danych.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	30
Udział w ćwiczeniach:	30
Praca własna studenta, w tym:	20
Przygotowanie do ćwiczeń:	20

Łączny czas pracy studenta	50
Sumaryczna liczba punktów ECTS dla przedmiotu	2

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_U02+++ CB1A_U03++	C1,C2	ĆW1 - ĆW7	1,2,3,4,5	O1,O2
EK 2	CB1A_U02+++ CB1A_U03++	C1,C2	ĆW1 - ĆW7	1,2,3,4,5	O1,O2
EK 3	CB1A_U02+++ CB1A_U03++	C1,C2	ĆW1 - ĆW7	1,2,3,4,5	O1,O2
EK 4	CB1A_U02+++ CB1A_U03++	C1,C2	ĆW1 - ĆW7	1,2,3,4,5	O1,O2
EK 5	CB1A_U02+++ CB1A_U03++	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1,O2
EK 6	CB1A_U02+++ CB1A_U03++	C1,C2	ĆW1 - ĆW7	1,2,3,4,5	O1,O2
EK 7	CB1A_K01+	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1,O2

Autor programu:	mgr Dominika Brodzka
Adres e-mail:	d.brodzka@pollub.pl
Jednostka organizacyjna:	Studium Języków Obcych

Karta (sylabus) modułu (przedmiotu)

Kierunek studiów: Cyberbezpieczeństwo

Studia pierwszego stopnia

Przedmiot:	Język angielski
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C011.1
Rok:	II
Semestr:	4
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	30
Wykład	
Ćwiczenia	30
Laboratorium	
Projekt	
Liczba punktów ECTS:	2
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu

C1	Rozwinięcie umiejętności językowych w zakresie czterech sprawności: słuchania, czytania, mówienia i pisanie na poziomie B2 Europejskiego Systemu Opisu Kształcenia Językowego
C2	Nabywanie umiejętności posługiwania się językiem angielskim w zakresie podstawowego specjalistycznego języka potrzebnego w pracy inżyniera

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1	Znajomość języka angielskiego na poziomie B1
----------	--

Efekty uczenia się

	W zakresie umiejętności:
EK 1	potrafi posługiwać się słownictwem dotyczącym omawianych treści programowych
EK 2	umie posługiwać się strukturami gramatycznymi omawianymi w semestrze
EK 3	potrafi wypowiadać się ustnie oraz pisemnie na tematy z zakresu inżynierii w tym związane ze studiowanym kierunkiem
EK4	potrafi zrozumieć i zinterpretować wypowiedzi pisemne i ustne na tematy inżynierskie z zakresu nauk technicznych
EK5	potrafi samodzielnie korzystać z materiałów dydaktycznych
EK6	potrafi pracować samodzielnie oraz w grupie, przyjmując w niej różne role
	W zakresie kompetencji społecznych:
EK7	jest gotów do krytycznej oceny swoich umiejętności językowych i podjęcia działań na rzecz ich doskonalenia, aby skuteczniej wspierać procesy wymiany wiedzy i rozwiązywania problemów w działalności zawodowej

Treści programowe przedmiotu	
Forma zajęć - ćwiczenia	
	Treści programowe
ĆW1	Projekt inżynierski: rodzaje rysunków technicznych, fazy powstawania projektu, problemy w projektowaniu oraz ich rozwiązywanie
ĆW2	Przyczyny powstawania problemów technicznych
ĆW3	Problemy techniczne: opisywanie wad, usterek, środki zapobiegawcze na wybranym przykładzie
ĆW4	Bazy danych
ĆW5	Rodzaje i zastosowanie podstawowych systemów operacyjnych
ĆW6	Sieci komputerowe
ĆW7	Strona bierna

Metody dydaktyczne	
1	Ćwiczenia językowe konwersacyjne
2	Ćwiczenia językowe leksykalno-gramatyczne
3	Praca z tekstem źródłowym lub innymi materiałami, w tym audio i audiowizualnymi
4	Praca wykonywana w grupach
5	Praca wykonywana indywidualnie

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	Ocena pracy pisemnej	51%
O2	Ocena odpowiedzi ustnej	51%

Literatura podstawowa	
1	Mark Ibbotson, Cambridge English for Engineering, Cambridge 2016.

Literatura uzupełniająca	
1	Beata Błaszczyk, English 4 IT. Praktyczny kurs języka angielskiego dla specjalistów IT i nie tylko, Helion 2017.
2	Noni Rizopoulou, Academic English for Computer Science, Disigma Publications, 2022.
3	Virginia Evans, Information technology (Career Paths), Express Publishing, 2022.
4	Foley Mark, Hall Diane, My GrammarLab, Pearson.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	30

Udział w ćwiczeniach:	30
Praca własna studenta, w tym:	20
Przygotowanie do ćwiczeń:	20
Łączny czas pracy studenta	50
Sumaryczna liczba punktów ECTS dla przedmiotu	2

Macierz efektów uczenia się					
Symbol przedmiotowe go efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_U02+++ CB1A_U03++	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1, O2
EK 2	CB1A_U02+++ CB1A_U03++	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1, O2
EK 3	CB1A_U02+++ CB1A_U03++	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1, O2
EK 4	CB1A_U02+++ CB1A_U03++	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1, O2
EK 5	CB1A_U02+++ CB1A_U03++	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1, O2
EK 6	CB1A_U02+++ CB1A_U03++	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1, O2
EK7	CB1A_K01+	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1, O2

Autor programu:	mgr Sławomir Kołtun
Adres e-mail:	s.koltun@pollub.pl
Jednostka organizacyjna:	Studium Języków Obcych

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Język niemiecki
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C011.2
Rok:	II
Semestr:	4
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	30
Wykład	
Ćwiczenia	30
Laboratorium	
Projekt	
Liczba punktów ECTS:	2
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Rozwinięcie umiejętności językowych w zakresie czterech sprawności: słuchania, czytania, mówienia i pisanie na poziomie B2 Europejskiego Systemu Opisu Kształcenia Językowego
C2	Nabywanie umiejętności posługiwania się językiem niemieckim w zakresie podstawowego specjalistycznego języka potrzebnego w pracy inżyniera

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Znajomość języka niemieckiego na poziomie B1

Efekty uczenia się	
	W zakresie umiejętności:
EK1	potrafi posługiwać się słownictwem dotyczącym omawianych treści programowych
EK2	umie posługiwać się strukturami gramatycznymi omawianymi w semestrze
EK3	potrafi wypowiadać się ustnie oraz pisemnie na tematy z zakresu inżynierii w tym związane ze studiowanym kierunkiem
EK4	potrafi zrozumieć i zinterpretować wypowiedzi pisemne i ustne na tematy inżynierskie z zakresu nauk technicznych
EK5	potrafi samodzielnie korzystać z materiałów dydaktycznych
EK6	potrafi pracować samodzielnie oraz w grupie, przyjmując w niej różne role
	W zakresie kompetencji społecznych:
EK7	jest gotów do krytycznej oceny swoich umiejętności językowych i podjęcia działań na rzecz ich doskonalenia, aby skuteczniej wspierać procesy wymiany wiedzy i rozwiązywania problemów w działalności zawodowej

Treści programowe przedmiotu	
Forma zajęć - ćwiczenia	
	Treści programowe
ĆW1	Projekt inżynierski, fazy powstawania projektu, problemy w projektowaniu oraz ich rozwiązywanie
ĆW2	Problemy techniczne i sposoby ich powstawania
ĆW3	Opisywanie wad, usterek, środki zapobiegawcze na wybranym przykładzie
ĆW4	Bazy danych
ĆW5	Systemy operacyjne: rodzaje i zastosowanie
ĆW6	Sieci komputerowe
ĆW7	Strona bierna, zdania podrzędnie złożone

Metody dydaktyczne	
1	Ćwiczenia językowe konwersacyjne
2	Ćwiczenia językowe leksykalno-gramatyczne
3	Praca z tekstem źródłowym lub innymi materiałami, w tym audio i audiowizualnymi
4	Praca wykonywana w grupach
5	Praca wykonywana indywidualnie

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	Ocena pracy pisemnej	51%
O2	Ocena odpowiedzi ustnej	51%

Literatura podstawowa	
1	Sabrina Schmohl, Akademe Deutsch, Hueber Verlag 2018.
2	Monika Rolbiecka, Deutsch für Profis, Lektor Klett, 2017.

Literatura uzupełniająca	
1	Ilse Sander, Deutsch im Unternehmen, Ernst Klett Sprachen, 2016.
2	Grammatik, gramatyka języka niemieckiego z ćwiczeniami, WSiP 2018.
3	Internetowa baza danych.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	30
Udział w ćwiczeniach:	30
Praca własna studenta, w tym:	20
Przygotowanie do ćwiczeń:	20

Łączny czas pracy studenta	50
Sumaryczna liczba punktów ECTS dla przedmiotu	2

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_U02+++ CB1A_U03++	C1,C2	ĆW1 - ĆW7	1,2,3,4,5	O1,O2
EK 2	CB1A_U02+++ CB1A_U03++	C1,C2	ĆW1 - ĆW7	1,2,3,4,5	O1,O2
EK 3	CB1A_U02+++ CB1A_U03++	C1,C2	ĆW1 - ĆW7	1,2,3,4,5	O1,O2
EK 4	CB1A_U02+++ CB1A_U03++	C1,C2	ĆW1 - ĆW7	1,2,3,4,5	O1,O2
EK 5	CB1A_U02+++ CB1A_U03++	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1,O2
EK6	CB1A_U02+++ CB1A_U03++	C1,C2	ĆW1 - ĆW7	1,2,3,4,5	O1,O2
EK7	CB1A_K01+	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1,O2

Autor programu:	mgr Dominika Brodzka
Adres e-mail:	d.brodzka@pollub.pl
Jednostka organizacyjna:	Studium Języków Obcych

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Język angielski
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C012.1
Rok:	III
Semestr:	5
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	30
Wykład	
Ćwiczenia	30
Laboratorium	
Projekt	
Liczba punktów ECTS:	2
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Rozwinięcie umiejętności językowych w zakresie czterech sprawności: słuchania, czytania, mówienia i pisanie na poziomie B2 Europejskiego Systemu Opisu Kształcenia Językowego
C2	Nabywanie umiejętności posługiwania się językiem angielskim w zakresie podstawowego specjalistycznego języka potrzebnego w pracy inżyniera

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Znajomość języka angielskiego na poziomie B1

Efekty uczenia się	
	W zakresie umiejętności:
EK 1	potrafi posługiwać się słownictwem dotyczącym omawianych treści programowych
EK 2	umie posługiwać się strukturami gramatycznymi omawianymi w semestrze
EK 3	potrafi wypowiadać się ustnie oraz pisemnie na tematy z zakresu inżynierii w tym związane ze studiowanym kierunkiem
EK4	potrafi zrozumieć i zinterpretować wypowiedzi pisemne i ustne na tematy inżynierskie z zakresu nauk technicznych
EK5	potrafi samodzielnie korzystać z materiałów dydaktycznych
EK 6	potrafi pracować samodzielnie oraz w grupie, przyjmując w niej różne role
	W zakresie kompetencji społecznych:
EK 7	jest gotów do krytycznej oceny swoich umiejętności językowych i podjęcia działań na rzecz ich doskonalenia, aby skuteczniej wspierać procesy wymiany wiedzy i rozwiązywania problemów w działalności zawodowej

Treści programowe przedmiotu	
Forma zajęć - ćwiczenia	
	Treści programowe
ĆW1	Proces technologiczny: analiza potrzeb, wymagania, ocena stopnia wykonalności, proponowane rozwiązania
ĆW2	Rodzaje zagrożeń w zakładach przemysłowych; procedury i środki bezpieczeństwa
ĆW3	Przepisy BHP- standardowe środki zapobiegawcze, przepisy, regulacje, oznaczenia maszyn i urządzeń
ĆW4	Złośliwe oprogramowanie
ĆW5	Uczenie maszynowe
ĆW6	Cyberbezpieczeństwo
ĆW7	Czasowniki modalne

Metody dydaktyczne	
1	Ćwiczenia językowe konwersacyjne
2	Ćwiczenia językowe leksykalno-gramatyczne
3	Praca z tekstem źródłowym lub innymi materiałami, w tym audio i audiowizualnymi
4	Praca wykonywana w grupach
5	Praca wykonywana indywidualnie

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	Ocena pracy pisemnej	51%
O2	Ocena odpowiedzi ustnej	51%

Literatura podstawowa	
1	Mark Ibbotson, Cambridge English for Engineering, Cambridge 2016.

Literatura uzupełniająca	
1	Noni Rizopoulou, Academic English for Computer Science, Disigma Publications, 2022.
2	Virginia Evans, Information technology (Career Paths), Express Publishing, 2022.
3	Foley Mark, Hall Diane, My GrammarLab, Pearson.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	30
Udział w ćwiczeniach:	30
Praca własna studenta, w tym:	20
Przygotowanie do ćwiczeń:	20

Łączny czas pracy studenta	50
Sumaryczna liczba punktów ECTS dla przedmiotu	2

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_U02+++ CB1A_U03++	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1, O2
EK 2	CB1A_U02+++ CB1A_U03++	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1, O2
EK 3	CB1A_U02+++ CB1A_U03++	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1, O2
EK 4	CB1A_U02+++ CB1A_U03++	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1, O2
EK 5	CB1A_U02+++ CB1A_U03++	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1, O2
EK 6	CB1A_U02+++ CB1A_U03++	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1, O2
EK 7	CB1A_K01+	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1, O2

Autor programu:	mgr Sławomir Kołtun
Adres e-mail:	s.koltun@pollub.pl
Jednostka organizacyjna:	Studium Języków Obcych

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
 Studia pierwszego stopnia

Przedmiot:	Język niemiecki
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C012.2
Rok:	III
Semestr:	5
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	30
Wykład	
Ćwiczenia	30
Laboratorium	
Projekt	
Liczba punktów ECTS:	2
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Rozwinięcie umiejętności językowych w zakresie czterech sprawności: słuchania, czytania, mówienia i pisanie na poziomie B2 Europejskiego Systemu Opisu Kształcenia Językowego
C2	Nabywanie umiejętności posługiwania się językiem niemieckim w zakresie podstawowego specjalistycznego języka potrzebnego w pracy inżyniera

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Znajomość języka niemieckiego na poziomie B1

Efekty uczenia się	
	W zakresie umiejętności:
EK1	potrafi posługiwać się słownictwem dotyczącym omawianych treści programowych
EK2	umie posługiwać się strukturami gramatycznymi omawianymi w semestrze
EK3	potrafi wypowiadać się ustnie oraz pisemnie na tematy z zakresu inżynierii w tym związane ze studiowanym kierunkiem
EK4	potrafi zrozumieć i zinterpretować wypowiedzi pisemne i ustne na tematy inżynierskie z zakresu nauk technicznych
EK5	potrafi samodzielnie korzystać z materiałów dydaktycznych
EK6	potrafi pracować samodzielnie oraz w grupie, przyjmując w niej różne role
	W zakresie kompetencji społecznych:
EK7	jest gotów do krytycznej oceny swoich umiejętności językowych i podjęcia działań na rzecz ich doskonalenia, aby skuteczniej wspierać procesy wymiany wiedzy i rozwiązywania problemów w działalności zawodowej

Treści programowe przedmiotu	
Forma zajęć - ćwiczenia	
	Treści programowe
ĆW1	Proces technologiczny: analiza potrzeb, wymagania, ocena
ĆW2	Rodzaje zagrożeń w zakładach przemysłowych
ĆW3	Przepisy BHP- standardowe środki zapobiegawcze, przepisy, regulacje, oznaczenia maszyn i urządzeń
ĆW4	Złośliwe oprogramowanie
ĆW5	Uczenie maszynowe
ĆW6	Cyberbezpieczeństwo
ĆW7	Czasowniki modalne, czasowniki rozdzielnie i nierozdzielnie złożone

Metody dydaktyczne	
1	Ćwiczenia językowe konwersacyjne
2	Ćwiczenia językowe leksykalno-gramatyczne
3	Praca z tekstem źródłowym lub innymi materiałami, w tym audio i audiowizualnymi
4	Praca wykonywana w grupach
5	Praca wykonywana indywidualnie

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	Ocena pracy pisemnej	51%
O2	Ocena odpowiedzi ustnej	51%

Literatura podstawowa	
1	Sabrina Schmohl, Akademe Deutsch, Hueber Verlag 2018.
2	Monika Rolbiecka, Deutsch für Profis, Lektor Klett, 2017.

Literatura uzupełniająca	
1	Ilse Sander, Deutsch im Unternehmen, Ernst Klett Sprachen, 2016.
2	Grammatik, gramatyka języka niemieckiego z ćwiczeniami, WSiP 2018.
3	Internetowa baza danych.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	30
Udział w ćwiczeniach:	30
Praca własna studenta, w tym:	20
Przygotowanie do ćwiczeń:	20

Łączny czas pracy studenta	50
Sumaryczna liczba punktów ECTS dla przedmiotu	2

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_U02+++ CB1A_U03++	C1,C2	ĆW1 - ĆW7	1,2,3,4,5	O1,O2
EK 2	CB1A_U02+++ CB1A_U03++	C1,C2	ĆW1 - ĆW7	1,2,3,4,5	O1,O2
EK 3	CB1A_U02+++ CB1A_U03++	C1,C2	ĆW1 - ĆW7	1,2,3,4,5	O1,O2
EK 4	CB1A_U02+++ CB1A_U03++	C1,C2	ĆW1 - ĆW7	1,2,3,4,5	O1,O2
EK 5	CB1A_U02+++ CB1A_U03++	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1,O2
EK6	CB1A_U02+++ CB1A_U03++	C1,C2	ĆW1 - ĆW7	1,2,3,4,5	O1,O2
EK7	CB1A_K01+	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1,O2

Autor programu:	mgr Dominika Brodzka
Adres e-mail:	d.brodzka@pollub.pl
Jednostka organizacyjna:	Studium Języków Obcych

Karta (sylabus) modułu (przedmiotu)

Kierunek studiów: Cyberbezpieczeństwo

Studia pierwszego stopnia

Przedmiot:	Język angielski
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C013.1
Rok:	III
Semestr:	6
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	30
Wykład	
Ćwiczenia	30
Laboratorium	
Projekt	
Liczba punktów ECTS:	2
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu

C1	Rozwinięcie umiejętności językowych w zakresie czterech sprawności: słuchania, czytania, mówienia i pisanie na poziomie B2 Europejskiego Systemu Opisu Kształcenia Językowego
C2	Nabywanie umiejętności posługiwania się językiem angielskim w zakresie podstawowego specjalistycznego języka potrzebnego w pracy inżyniera

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1	Znajomość języka angielskiego na poziomie B1
----------	--

Efekty uczenia się

	W zakresie umiejętności:
EK 1	potrafi posługiwać się słownictwem dotyczącym omawianych treści programowych
EK 2	umie posługiwać się strukturami gramatycznymi omawianymi w semestrze
EK 3	potrafi wypowiadać się ustnie oraz pisemnie na tematy z zakresu inżynierii w tym związane ze studiowanym kierunkiem
EK 4	potrafi zrozumieć i zinterpretować wypowiedzi pisemne i ustne na tematy inżynierskie z zakresu nauk technicznych
EK 5	potrafi samodzielnie korzystać z materiałów dydaktycznych
EK 6	potrafi pracować samodzielnie oraz w grupie, przyjmując w niej różne role
	W zakresie kompetencji społecznych:
EK 7	jest gotów do krytycznej oceny swoich umiejętności językowych i podjęcia działań na rzecz ich doskonalenia, aby skuteczniej wspierać procesy wymiany wiedzy i rozwiązywania problemów w działalności zawodowej

Treści programowe przedmiotu	
Forma zajęć - ćwiczenia	
	Treści programowe
ĆW1	Proces monitoringu- różnice pomiędzy systemem automatycznym a systemem ręcznym, parametry
ĆW2	Odczyty, przybliżone dane, wykresy i ich interpretacja oraz ocena
ĆW3	Sztuczna inteligencja
ĆW4	Programowanie - podstawowe języki, etapy pisania programu komputerowego
ĆW5	Zarządzanie danymi
ĆW6	Big data
ĆW7	Zdania podrzędne

Metody dydaktyczne	
1	Ćwiczenia językowe konwersacyjne
2	Ćwiczenia językowe leksykalno-gramatyczne
3	Praca z tekstem źródłowym lub innymi materiałami, w tym audio i audiowizualnymi
4	Praca wykonywana w grupach
5	Praca wykonywana indywidualnie

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	Ocena pracy pisemnej	51%
O2	Ocena odpowiedzi ustnej	51%

Literatura podstawowa	
1	Mark Ibbotson, Cambridge English for Engineering, Cambridge 2016.

Literatura uzupełniająca	
1	Beata Błaszczuk, English 4 IT. Praktyczny kurs języka angielskiego dla specjalistów IT i nie tylko, Helion 2017.
2	Noni Rizopoulou, Academic English for Computer Science, Disigma Publications, 2022.
3	Virginia Evans, Information technology (Career Paths), Express Publishing, 2022.
4	Foley Mark, Hall Diane, My GrammarLab, Pearson.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	30
Udział w ćwiczeniach:	30

Praca własna studenta, w tym:	20
Przygotowanie do ćwiczeń:	20
Łączny czas pracy studenta	50
Sumaryczna liczba punktów ECTS dla przedmiotu	2

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_U02+++ CB1A_U03++	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1, O2
EK 2	CB1A_U02+++ CB1A_U03++	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1, O2
EK 3	CB1A_U02+++ CB1A_U03++	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1, O2
EK 4	CB1A_U02+++ CB1A_U03++	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1, O2
EK 5	CB1A_U02+++ CB1A_U03++	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1, O2
EK6	CB1A_U02+++ CB1A_U03++	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1, O2
EK7	CB1A_K01+	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1, O2

Autor programu:	mgr Sławomir Koltun
Adres e-mail:	s.koltun@pollub.pl
Jednostka organizacyjna:	Studium Języków Obcych

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
 Studia pierwszego stopnia

Przedmiot:	Język niemiecki
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C013.2
Rok:	III
Semestr:	6
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	30
Wykład	
Ćwiczenia	30
Laboratorium	
Projekt	
Liczba punktów ECTS:	2
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Rozwinięcie umiejętności językowych w zakresie czterech sprawności: słuchania, czytania, mówienia i pisanie na poziomie B2 Europejskiego Systemu Opisu Kształcenia Językowego
C2	Nabywanie umiejętności posługiwania się językiem niemieckim w zakresie podstawowego specjalistycznego języka potrzebnego w pracy inżyniera

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Znajomość języka niemieckiego na poziomie B1

Efekty uczenia się	
	W zakresie umiejętności:
EK1	potrafi posługiwać się słownictwem dotyczącym omawianych treści programowych
EK2	umie posługiwać się strukturami gramatycznymi omawianymi w semestrze
EK3	potrafi wypowiadać się ustnie oraz pisemnie na tematy z zakresu inżynierii w tym związane ze studiowanym kierunkiem
EK4	potrafi zrozumieć i zinterpretować wypowiedzi pisemne i ustne na tematy inżynierskie z zakresu nauk technicznych
EK5	potrafi samodzielnie korzystać z materiałów dydaktycznych
EK6	potrafi pracować samodzielnie oraz w grupie, przyjmując w niej różne role
	W zakresie kompetencji społecznych:
EK7	jest gotów do krytycznej oceny swoich umiejętności językowych i podjęcia działań na rzecz ich doskonalenia, aby skuteczniej wspierać procesy wymiany wiedzy i rozwiązywania problemów w działalności zawodowej

Treści programowe przedmiotu	
Forma zajęć - ćwiczenia	
	Treści programowe
ĆW1	Proces monitoringu- różnice i parametry
ĆW2	Odczyty, przybliżone dane, wykresy
ĆW3	Sztuczna inteligencja
ĆW4	Programowanie - podstawowe języki, etapy pisania programu komputerowego
ĆW5	Zarządzanie danymi
ĆW6	Big data
ĆW7	Relativ- und Finalsätze

Metody dydaktyczne	
1	Ćwiczenia językowe konwersacyjne
2	Ćwiczenia językowe leksykalno-gramatyczne
3	Praca z tekstem źródłowym lub innymi materiałami, w tym audio i audiowizualnymi
4	Praca wykonywana w grupach
5	Praca wykonywana indywidualnie

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	Ocena pracy pisemnej	51 %
O2	Ocena odpowiedzi ustnej	51 %

Literatura podstawowa	
1	Sabrina Schmohl, Akademie Deutsch, Hueber Verlag 2018.
2	Monika Rolbiecka, Deutsch für Profis, Lektor Klett, 2017.

Literatura uzupełniająca	
1	Ilse Sander, Deutsch im Unternehmen, Ernst Klett Sprachen, 2016.
2	Grammatik, gramatyka języka niemieckiego z ćwiczeniami, WSiP 2018.
3	Internetowa baza danych.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	30
Udział w ćwiczeniach:	30
Praca własna studenta, w tym:	20
Przygotowanie do ćwiczeń:	20

Łączny czas pracy studenta	50
Sumaryczna liczba punktów ECTS dla przedmiotu	2

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_U02+++ CB1A_U03++	C1,C2	ĆW1 - ĆW7	1,2,3,4,5	O1,O2
EK 2	CB1A_U02+++ CB1A_U03++	C1,C2	ĆW1 - ĆW7	1,2,3,4,5	O1,O2
EK 3	CB1A_U02+++ CB1A_U03++	C1,C2	ĆW1 - ĆW7	1,2,3,4,5	O1,O2
EK 4	CB1A_U02+++ CB1A_U03++	C1,C2	ĆW1 - ĆW7	1,2,3,4,5	O1,O2
EK 5	CB1A_U02+++ CB1A_U03++	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1,O2
EK6	CB1A_U02+++ CB1A_U03++	C1,C2	ĆW1 - ĆW7	1,2,3,4,5	O1,O2
EK7	CB1A_K01+	C1, C2	ĆW1 - ĆW7	1,2,3,4,5	O1,O2

Autor programu:	mgr Dominika Brodzka
Adres e-mail:	d.brodzka@pollub.pl
Jednostka organizacyjna:	Studium Języków Obcych

Karta (sylabus) modułu (przedmiotu)

Kierunek studiów: Cyberbezpieczeństwo

Studia pierwszego stopnia

Przedmiot:	Bezpieczeństwo i higiena pracy
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C101
Rok:	I
Semestr:	1
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	5
Wykład	5
Ćwiczenia	
Laboratorium	
Projekt	
Liczba punktów ECTS:	0
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu

C1	Zapoznanie z podstawami prawnymi BHP
C2	Zrozumienie zagrożeń w pracy z technologiami informatycznymi
C3	Dostarczenie wiedzy na temat zasad pierwszej pomocy oraz sposobów postępowania w sytuacjach awaryjnych

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1	Ogólna wiedza dotycząca zasad bezpieczeństwa
----------	--

Efekty uczenia się

	W zakresie wiedzy:
EK 1	zna podstawowe pojęcia związane z bezpieczeństwem i higieną pracy oraz ergonomią stanowiska pracy
EK 2	rozumie przepisy prawne oraz zasady ochrony zdrowia i bezpieczeństwa w pracy
	W zakresie kompetencji społecznych:
EK3	jest gotów do świadomego przestrzegania zasad bezpieczeństwa i higieny pracy

Treści programowe przedmiotu

Forma zajęć - wykłady

	Treści programowe
W1	Definicja i istota bezpieczeństwa i higieny pracy. Podstawowe akty prawne z zakresu BHP
W2	Zagrożenia w środowisku pracy w branży IT i cyberbezpieczeństwie
W3	Postępowanie w sytuacjach awaryjnych i pierwsza pomoc w miejscu pracy

Metody dydaktyczne	
1	wykład informacyjny
2	analiza przypadków

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%

Literatura podstawowa	
1	Ustawa z dnia 16 maja 2019 r. – Kodeks pracy. Dziennik Ustaw, poz. 1043, 2019.
2	Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 26 września 1997 r. w sprawie ogólnych przepisów bezpieczeństwa i higieny pracy. Dziennik Ustaw, nr 129, poz. 844, 1997.
3	Goniewicz, Mariusz, i in. Pierwsza pomoc : podręcznik dla studentów. Wyd. 1, 6 dodr., Wyd. Lekarskie PZWL, 2016.

Literatura uzupełniająca	
1	Rączkowski, Bogdan, i in. BHP w praktyce. Wydanie XVIII, stan Prawny na dzień 1 marca 2020 r., ODDK, 2020.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	5
Udział w wykładach:	5
Praca własna studenta, w tym:	0
Łączny czas pracy studenta	5
Sumaryczna liczba punktów ECTS dla przedmiotu	0

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W20+++	C1	W1-W3	1,2	O1
EK 2	CB1A_W20+++	C2	W1-W3	1,2	O1

EK 3	CB1A_K05++	C1-C3	W1-W3	1,2	O1
------	------------	-------	-------	-----	----

Autor programu:	mgr inż. Aleksandra Prus
Adres e-mail:	a.prus@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Technicznej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Ochrona własności intelektualnej
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C102
Rok:	I
Semestr:	1
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	15
Wykład	15
Ćwiczenia	
Laboratorium	
Projekt	
Liczba punktów ECTS:	1
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	zapoznanie z rodzajami dóbr własności intelektualnej, z możliwościami oraz zasadami eksploataowania i komercjalizacji przedmiotów własności intelektualnej
C2	przekazanie wiedzy na temat charakteru norm prawa własności intelektualnej oraz procedur i narzędzi pozwalających na ochronę przedmiotów własności intelektualnej
C3	uwrażliwienie na etyczne zachowania przy ochronie praw własności intelektualnej i związane z tym, poczucie odpowiedzialności budujące postawę prospołeczną

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	wiedza z zakresu działań organów ustawodawczych w kraju
2	znajomość obsługi wyszukiwarek internetowych
3	zdolność logicznego myślenia

Efekty uczenia się	
	W zakresie wiedzy:
EK 1	zna i rozumie wagę przestrzegania praw ochrony własności intelektualnej w tym przestrzegania praw autorskich, praw własności przemysłowej oraz know-how firmy
EK 2	zna pojęcia prawa autorskiego osobistego i prawa autorskiego majątkowego; pojęcia: własność przemysłowa, wynalazek, patent, wzór użytkowy, wzór przemysłowy, znak towarowy, topografia układu scalonego, oznaczenie geograficzne, dobro niematerialne
EK 3	ma wiedzę na temat posługiwania się aktami prawnymi dotyczącymi ochrony własności intelektualnej obowiązującymi w kraju, z uwzględnieniem aktów wynikających z porozumień międzynarodowych

EK 4	ma wiedzę na temat źródeł pozyskiwania informacji z zakresu ochrony własności intelektualnej
	W zakresie kompetencji społecznych:
EK 5	jest gotów do krytycznej oceny posiadanej wiedzy i krytycznej weryfikacji własnych wyników poszukiwań najnowszych rozwiązań technicznych i technologicznych, uzyskanych w procesie wyszukiwania w naukowych bazach literatury światowej, w bazach patentowych oraz literaturze patentowej
EK 6	jest gotów do odpowiedzialnego pełnienia ról zawodowych wykazując zdolność do identyfikowania nieprawnych i nieetycznych działań związanych z ochroną własności intelektualnej

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W 1	podstawy prawne własności intelektualnej oraz przybliżenie pojęć własności intelektualnej wraz z charakterystyką dóbr takich jak.: utwór, wynalazek, wzór użytkowy, wzór przemysłowy, znak towarowy, oznaczenie geograficzne, topografia układu scalonego, oznaczenia przedsiębiorstwa, know-how, nowe odmiany roślin
W 2	przedmiot i podmiot autorskich praw majątkowych i praw pokrewnych; ochrona autorskich praw osobistych i majątkowych, dozwolony użytek osobisty i publiczny; przenoszenie praw (umowy licencyjne); wolne licencje i zasoby Open Access oraz bazy literatury naukowej; regulamin zarządzania prawami autorskimi i prawami pokrewnymi oraz prawami własności przemysłowej; zasady komercjalizacji w Politechnice Lubelskiej – w części dotyczącej praw autorskich i praw pokrewnych
W 3	przesłanki zdolności patentowej wynalazku, pojęcie czystości patentowej; zakres prawa patentowego; rozwiązania wyłączone spod ochrony patentowej; wygaśnięcie i unieważnienie patentu, dodatkowe prawo ochronne (SPC)
W 4	ochrona wynalazków: krajowe, regionalne i międzynarodowe systemy ochrony patentowej (UPRP, EPO, PCT); regulamin zarządzania prawami autorskimi i prawami pokrewnymi oraz prawami własności przemysłowej; zasady komercjalizacji w Politechnice Lubelskiej – w części dotyczącej praw własności przemysłowej
W 5	klasyfikacje stosowane dla własności przemysłowej: Międzynarodowa Klasyfikacja Patentowa (klasyfikacja MKP), Wspólna Klasyfikacja Patentowa (CPC), Międzynarodowa Klasyfikacja Towarów i Usług (klasyfikacja nicejska), Międzynarodowa Klasyfikacja Elementów Obrazowych Znaków Towarowych (klasyfikacja wiedeńska), Międzynarodowa Klasyfikacja Wzorów Przemysłowych (klasyfikacja lokarneńska), Międzynarodowa Klasyfikacja Wzorów Przemysłowych (klasyfikacja Euro Locarno)
W 6	przesłanki uzyskania prawa ochronnego na wzór użytkowy; systemy uzyskiwania ochrony wzoru użytkowego; bazy danych wzorów użytkowych
W 7	zdolność rejestrowa wzoru przemysłowego; zakres i ograniczenia prawa z rejestracji na wzór przemysłowy; ulga w nowości; systemy ochrony wzorów przemysłowych: krajowe (UPRP), regionalne – wspólnotowy wzór przemysłowy (EUIPO), międzynarodowe (Porozumienie Haskie); unieważnienie i wygaśnięcie prawa z rejestracji wzoru przemysłowego; bazy danych wzorów przemysłowych

W 8	rodzaje znaków towarowych; zdolność odróżniająca znaku towarowego, bezwzględne przeszkody rejestracji znaku towarowego; zakres i ograniczenia prawa ochronnego na znak towarowy; systemy ochrony znaków towarowych: krajowe (UPRP), regionalne – unijny znak towarowy (EUIPO), międzynarodowe (Porozumienie Madryckie i Protokół do Porozumienia Madryckiego); unieważnienie i wygaśnięcie prawa ochronnego na znak towarowy; bazy danych znaków towarowych
W 9	zdolność rejestracyjna oznaczenia geograficznego; procedury ochrony oznaczenia geograficznego w trybie krajowym (UPRP), wspólnotowym: Chroniona Nazwa Pochodzenia, Chronione Oznaczenie Geograficzne oraz Gwarantowana Tradycyjna Specjalność; bazy danych chronionych oznaczeń geograficznych
W 10	topografia układu scalonego – przesłanki zdolności rejestrowej topografii układu scalonego; systemy ochrony krajowej (UPRP); ulga w oryginalności; unieważnienie i wygaśnięcie prawa z rejestracji na topografię układu scalonego; bazy danych topografii układów scalonych
W 11	zwalczanie nieuczciwej konkurencji (tajemnica przedsiębiorstwa, oznaczenia przedsiębiorstwa, oznaczenia informacyjne); regulamin zarządzania prawami autorskimi i prawami pokrewnymi oraz prawami własności przemysłowej, zasady komercjalizacji w Politechnice Lubelskiej – w części zasad komercjalizacji obejmującej zwalczanie nieuczciwej konkurencji
W 12	korzystanie z informacji patentowej; metodologia poszukiwań prowadzonych w profesjonalnych bazach patentowych i wyszukiwarkach zawierających informacje patentową

Metody dydaktyczne	
1	wykład informacyjny
2	pokaz z objaśnieniami
3	wykład konwersatoryjny
4	dyskusja dydaktyczna

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%

Literatura podstawowa	
1	zbiór aktualnych podstawowych przepisów prawnych: Ustawa z dnia 30 czerwca 2000 r. Prawo własności przemysłowej, z późn. zmianami Ustawa z dnia 4 lutego 1994 r. O prawie autorskim i prawach pokrewnych, z późn. zmianami Ustawa z dnia 16 kwietnia 1993 r. O zwalczaniu nieuczciwej konkurencji, z późn. zmianami Ustawa z dnia 16 lutego 2007 r. O ochronie konkurencji i konsumentów, z późn. zmianami.
2	aktualne akty prawne: Rozporządzenie Prezesa Rady Ministrów w sprawie dokonywania i rozpatrywania zgłoszeń wynalazków i wzorów użytkowych Rozporządzenie Prezesa Rady Ministrów w sprawie dokonywania i rozpatrywania

	zgłoszeń topografii układów scalonych Rozporządzenie Prezesa Rady Ministrów w sprawie dokonywania i rozpatrywania zgłoszeń wzorów przemysłowych Rozporządzenie Prezesa Rady Ministrów w sprawie składania i rozpatrywania wniosków o udzielenie dodatkowego prawa ochronnego dla produktów leczniczych i produktów ochrony roślin Rozporządzenie Prezesa Rady Ministrów w sprawie dokonywania i rozpatrywania zgłoszeń znaków towarowych Rozporządzenie Prezesa Rady Ministrów w sprawie rejestrów prowadzonych przez Urząd Patentowy Rzeczypospolitej Polskiej.
3	aktualne Zarządzenie Rektora Politechniki Lubelskiej w sprawie wprowadzenia w Politechnice Lubelskiej Regulaminu funkcjonowania systemu antyplagiatowego aktualna Uchwała Senatu Politechniki Lubelskiej w sprawie uchwalenia Regulaminu zarządzania prawami autorskimi i prawami pokrewnymi oraz prawami własności przemysłowej, a także zasad komercjalizacji w Politechnice Lubelskiej.

Literatura uzupełniająca	
1	Barta, Janusz, i in. Prawo autorskie i prawa pokrewne, Wyd. 10, stan prawny na 20 września 2024 r., Wolters Kluwer Polska, 2024.
2	Michniewicz, G. Ochrona własności intelektualnej, Wyd. 5, C. H. Beck, 2022.
3	Prawo własności przemysłowej Wyd. 18, stan prawny: 22 stycznia 2024 r., C. H. Beck, 2024.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	15
Udział w wykładach:	15
Praca własna studenta, w tym:	10
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	10
Łączny czas pracy studenta	25
Sumaryczna liczba punktów ECTS dla przedmiotu	1

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W16+++	C1, C3	W1-W3,W6-W8	1, 2, 4	O1

EK 2	CB1A_W20+ CB1A_W16+++	C1, C2	W1, W2, W12	2, 3, 4	O1
EK 3	CB1A_W16+++	C1, C2, C3	W1-W3, W6-W8	2, 3, 4	O1
EK 4	CB1A_W16+++	C2, C3	W1, W4, W6-W9	2, 3, 4	O1
EK 5	CB1A_K01+	C1, C2	W1 - W12	1 - 4	O1
EK 6	CB1A_K05+++	C3	W1 - W12	1, 4	O1

Autor programu:	mgr Małgorzata Jaworowska
Adres e-mail:	m.jaworowska@pollub.pl
Jednostka organizacyjna:	Katedra Metod i Technik Nauczania

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Przysposobienie biblioteczne
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C103
Rok:	I
Semestr:	1
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	2
Wykład	
Ćwiczenia	2
Laboratorium	
Projekt	
Liczba punktów ECTS:	0
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Poznanie usług świadczonych przez Bibliotekę PL
C2	Uzyskanie podstawowej wiedzy o specyfice, charakterze i rozmieszczeniu zbiorów udostępnianych przez Bibliotekę PL
C3	Poznanie praw i obowiązków czytelników, określonych w regulaminie udostępniania zasobów oraz działalności Biblioteki w Centrum Informacji Naukowo-Technicznej Politechniki Lubelskiej
C4	Nabycie umiejętności korzystania z bibliotecznego katalogu komputerowego, multiwyszukiwarki oraz wybranych zasobów elektronicznych
C5	Wykształcenie potrzeby ciągłego zdobywania wiedzy poprzez korzystanie z zasobów bibliotecznego katalogu komputerowego oraz innych źródeł

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Podstawowa znajomość obsługi komputera
2	Znajomość podstawowych technik informacyjnych

Efekty uczenia się	
	W zakresie umiejętności:
EK 2	potrafi korzystać z licencjonowanych zasobów elektronicznych udostępnianych poprzez stronę WWW CINT oraz dokumentów specjalistycznych

Treści programowe przedmiotu	
Forma zajęć - ćwiczenia	
	Treści programowe

ĆW1	Poznanie usług świadczonych przez Centrum Informacji Naukowo-Technicznej. Zapoznanie z regulaminem udostępniania zasobów oraz działalności Biblioteki w Centrum Informacji Naukowo-Technicznej Politechniki Lubelskiej. Charakterystyka zbiorów bibliotecznych. Poznanie strony domowej CINT PL stanowiącej pomoc w dotarciu do poszukiwanej informacji. Prezentacja na temat narzędzi wyszukiwawczych: posługiwanie się bibliotecznym katalogiem komputerowym i multiwyszukiwarką. Prezentacja wybranych zasobów elektronicznych – Biblioteka Cyfrowa PL, Czytelnia – IBUK, inne dokumenty specjalistyczne. Wykorzystanie zasobów bibliotecznych zgodnie z zasadami etyki i przepisami prawa autorskiego
ĆW2	Złożenie zamówienia na książkę i czasopismo przez biblioteczny katalog komputerowy. Wyszukiwanie zasobów w Bibliotece Cyfrowej PL i Czytelni IBUK

Metody dydaktyczne	
1	ćwiczenia przedmiotowe

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena wykonanych ćwiczeń przedmiotowych	100%

Literatura podstawowa	
1	Strona domowa CINT https://cint.pollub.pl – lokalizacja, godziny otwarcia, inne informacje praktyczne.
2	Aktualny regulamin udostępniania zbiorów bibliotecznych oraz zasad działalności usługowej w Centrum Informacji Naukowo-Technicznej.

Literatura uzupełniająca	
1	Poradniki i instrukcje dostępne na stronie CINT https://cint.pollub.pl .

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	2
Udział w ćwiczeniach:	2
Praca własna studenta:	0
Łączny czas pracy studenta	2
Sumaryczna liczba punktów ECTS dla przedmiotu	0

Macierz efektów uczenia się					
Symbol przedmiotowe	Odniesienie przedmiotowego efektu uczenia się	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny

go efektu uczenia się	do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania				
EK 1	CB1A_U01++	C1-C5	ĆW1-ĆW2	1	O1

Autor programu:	mgr Stanisława Pietrzyk-Leonowicz; mgr Łukasz Tomczak
Adres e-mail:	s.pietrzyk@pollub.pl; l.tomczak@pollub.pl
Jednostka organizacyjna:	Centrum Informacji Naukowo-Technicznej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Matematyka
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C104
Rok:	I
Semestr:	1
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	75
Wykład	30
Ćwiczenia	45
Laboratorium	
Projekt	
Liczba punktów ECTS:	5
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zaznajomienie z rachunkiem różniczkowym i całkowym w zakresie funkcji jednej zmiennej
C2	Zaznajomienie z podstawowymi zagadnieniami z zakresu algebry liniowej
C3	Wyszkolenie nawyku systematycznego podnoszenia poziomu swojej wiedzy i umiejętności oraz zdobywania nowych kompetencji

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Znajomość matematyki na poziomie szkoły średniej

Efekty uczenia się	
	W zakresie wiedzy:
EK 1	rozpoznaje i opisuje podstawowe metody rachunku różniczkowego w zakresie funkcji jednej zmiennej
EK 2	rozpoznaje i opisuje podstawowe metody rachunku całkowego w zakresie funkcji jednej zmiennej
EK 3	rozpoznaje i opisuje podstawowe metody algebry liniowej
	W zakresie umiejętności:
EK 4	posługuje się rachunkiem różniczkowym w zakresie funkcji jednej zmiennej
EK 5	posługuje się rachunkiem całkowym w zakresie funkcji jednej zmiennej
EK 6	posługuje się metodami algebry liniowej
	W zakresie kompetencji społecznych:

EK 7	jest gotów do krytycznej oceny własnej wiedzy i systematycznego zdobywania nowych kompetencji zawodowych w sposób samodzielny oraz poprzez zasięgnięcie opinii ekspertów
-------------	--

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Ciągi liczbowe i ich granice
W2	Granica funkcji i ciągłość funkcji. Asymptoty wykresu funkcji
W3	Pochodna funkcji. Podstawowe wzory na pochodne
W4	Przedziały monotoniczności i ekstrema lokalne funkcji
W5	Ekstrema globalne funkcji. Przedziały wklęsłości i wypukłości funkcji
W6	Twierdzenie de l'Hospitala
W7	Badanie przebiegu zmienności funkcji
W8	Całka nieoznaczona i jej własności
W9	Całka oznaczona i jej zastosowania
W10	Algebra macierzy
W11	Wyznacznik macierzy kwadratowej i metody jego obliczania
W12	Układy równań liniowych
Forma zajęć - ćwiczenia	
	Treści programowe
ĆW1	Obliczanie granic ciągów liczbowych
ĆW2	Obliczanie granic funkcji. Badanie ciągłości funkcji. Wyznaczanie asymptot wykresu funkcji
ĆW3	Wyznaczanie pochodnych funkcji
ĆW4	Wyznaczanie przedziałów monotoniczności i oraz ekstremów lokalnych funkcji
ĆW5	Wyznaczanie ekstremów globalnych funkcji. Wyznaczanie przedziałów wklęsłości i wypukłości funkcji
ĆW6	Obliczanie granic funkcji z wykorzystaniem twierdzenia de l'Hospitala
ĆW7	Sporządzanie wykresów funkcji
ĆW8	Obliczanie całek nieoznaczonych
ĆW9	Rozwiązywanie zadań dotyczących zastosowania całek oznaczonych
ĆW10	Wykonywanie działań na macierzach
ĆW11	Obliczanie wyznacznika macierzy kwadratowej
ĆW12	Rozwiązywanie układów równań liniowych

Metody dydaktyczne	
1	Wykład informacyjny
2	Wykład konwersatoryjny
3	Ćwiczenia rachunkowe

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	Ocena pracy pisemnej	51%
O2	Ocena aktywności w trakcie zajęć	ocena formująca bez progu zaliczeniowego

Literatura podstawowa	
1	Krysicki, Włodzimierz, i in. Analiza matematyczna w zadaniach. Wyd. Naukowe PWN SA, 2024.
2	Gewert, Marian, i in. Analiza matematyczna 1 : przykłady i zadania. Oficyna Wydawnicza GiS, 2018.
3	Jurlewicz, Teresa, i in. Algebra liniowa 1 : przykłady i zadania. Oficyna Wydawnicza GiS, 2005.

Literatura uzupełniająca	
1	Stankiewicz Włodzimierz, Zadania z matematyki dla wyższych uczelni technicznych, cz.1, PWN, 2001.
2	Gewert Marian, Skoczylas Zbigniew, Analiza matematyczna 1, Definicje, twierdzenia, wzory, Oficyna Wydawnicza GiS, 2019.
3	Jurlewicz Teresa, Skoczylas Zbigniew, Algebra liniowa 1, Definicje, twierdzenia, wzory, Oficyna Wydawnicza GiS, 2005.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	75
Udział w wykładach:	30
Udział w ćwiczeniach:	45
Praca własna studenta, w tym:	50
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	20
Przygotowanie do ćwiczeń:	30
Łączny czas pracy studenta	125
Sumaryczna liczba punktów ECTS dla przedmiotu	5

Macierz efektów uczenia się					
Symbol przedmiotowe go efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny

	zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania				
EK 1	CB1A_W01+++	C1	W1-W7	1, 2	O1
EK 2	CB1A_W01+++	C1	W8-W9	1, 2	O1
EK 3	CB1A_W01+++	C2	W10-W12	1, 2	O1
EK 4	CB1A_U15+++ CB1A_U12++	C1	ĆW1-ĆW7	3	O1, O2
EK 5	CB1A_U15+++ CB1A_U12++	C1	ĆW8-ĆW9	3	O1, O2
EK 6	CB1A_U15+++ CB1A_U12++	C2	ĆW10-ĆW12	3	O1, O2
EK 7	CB1A_K01+	C3	W1-W12 ĆW1-ĆW12	1, 2, 3	O1, O2

Autor programu:	dr Izolda Gorgol; dr Ewa Łazuka, profesor uczelni; dr Paweł Właz
Adres e-mail:	i.gorgol@pollub.pl; e.lazuka@pollub.pl; p.wlaz@pollub.pl
Jednostka organizacyjna:	Katedra Matematyki Stosowanej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Fizyka
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C105
Rok:	I
Semestr:	1
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	60
Wykład	30
Ćwiczenia	30
Laboratorium	
Projekt	
Liczba punktów ECTS:	4
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Poznanie i zrozumienie podstawowych praw fizyki
C2	Nabycie umiejętności rachunkowych z zakresu rozwiązywania zadań z fizyki
C3	Poznanie i zrozumienie podstaw mechaniki kwantowej w kontekście informacji kwantowej

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	znajomość matematyki z zakresu programu nauczania szkoły średniej
2	znajomość fizyki z zakresu programu nauczania szkoły średniej

Efekty uczenia się	
	W zakresie wiedzy:
EK1	zna podstawowe prawa fizyki
EK2	zna podstawy mechaniki kwantowej potrzebne do zrozumienia zagadnień z zakresu informacji kwantowej
	W zakresie umiejętności:
EK3	rozwiązuje typowe zadania rachunkowe z fizyki
EK4	wyszukuje i stosuje informacje z literatury w temacie fizyki, a w szczególności mechaniki kwantowej i informacji kwantowej
EK5	szacuje dokładność pomiarową wielkości fizycznych
	W zakresie kompetencji społecznych:
EK6	jest gotów do krytycznej oceny posiadanej wiedzy i odbieranych treści z obszaru fizyki, rozumiejąc potrzebę ciągłego jej uzupełniania oraz weryfikacji, aby rzetelnie i

	odpowiedzialnie wykorzystywać zdobytą wiedzę w rozwiązywaniu problemów związanych z bezpieczeństwem cyfrowym
--	--

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Rachunek wektorowy, elementy rachunku różniczkowego i całkowego, układ jednostek SI
W2	Kinematyka punktu materialnego
W3	Dynamika punktu materialnego i bryły sztywnej, zasady zachowania w fizyce, praca i moc
W4	Prawo powszechnego ciążenia, prawa Keplera
W5	Drgania i fale, oscylator harmoniczny, wahadło matematyczne i fizyczne
W6	Sprężystość ciał stałych, hydrostatyka i elementy dynamiki płynów
W7	Termodynamika: równanie stanu gazu doskonałego, przemiany gazowe, zasady termodynamiki, sprawność silnika Carnota, przejścia fazowe
W8	Elektrostatyka, elektryczność, magnetyzm, fale elektromagnetyczne
W9	Optyka geometryczna i falowa
W10	Fizyka współczesna: fizyka atomowa i jądrowa oraz fizyka ciała stałego
W11	Elementy mechaniki kwantowej
W12	Informacja kwantowa i komputery kwantowe
W13	Pomiar i analiza danych pomiarowych oraz rola symulacji komputerowych w fizyce
Forma zajęć - ćwiczenia	
	Treści programowe
ĆW1	Rozwiązywanie zadań z zakresu rachunku wektorowego, rachunku różniczkowego i całkowego
ĆW2	Rozwiązywanie zadań z kinematyki i dynamiki punktu materialnego oraz bryły sztywnej
ĆW3	Rozwiązywanie zadań z dynamiki oscylatora harmonicznego, wahadła matematycznego i fizycznego
ĆW4	Rozwiązywanie zadań z hydrostatyki i termodynamiki
ĆW5	Rozwiązywanie zadań z elektrostatyki, elektryczności i magnetyzmu
ĆW6	Rozwiązywanie zadań z optyki geometrycznej i falowej
ĆW7	Rozwiązywanie zadań z zakresu fizyki współczesnej
ĆW8	Rozwiązywanie zadań z mechaniki kwantowej
ĆW9	Planowanie i analiza eksperymentów fizycznych na podstawie danych pomiarowych (syntetyczne)

Metody dydaktyczne	
1	wykład informacyjny
2	ćwiczenia rachunkowe
3	analiza przypadków

4	dyskusja dydaktyczna
---	----------------------

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena aktywności w trakcie zajęć	51%

Literatura podstawowa	
1	Orear J., Fizyka, tomy 1-2, Wyd. Naukowo-Techniczne, Warszawa 2015.
2	Halliday D., Resnick R., Walker J., Podstawy fizyki, t. 1,2,3,4 i 5, PWN, Warszawa (wszystkie roczniki).
3	Jędrzejewski J., Kruczek W., Kujawski A., Zbiór zadań z fizyki, tomy 1-2, Wyd. Naukowo-Techniczne, Warszawa (wszystkie roczniki).
4	D.J. Griffiths, D.F. Schroeter. Wstęp do mechaniki kwantowej. 1. wyd. Wyd. Naukowe PWN, 2021.

Literatura uzupełniająca	
1	Richard P. Feynman, Leighton Robert B., Matthew Sands, Feynmana wykłady z fizyki, t. 1.1, 1.2, 2.1, 2.2, 3, PWN, Warszawa (wszystkie roczniki).
2	Taylor J.R.: Wstęp do analizy błęd pomiarowego. Warszawa: PWN, 1999.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	60
Udział w wykładach:	30
Udział w ćwiczeniach:	30
Praca własna studenta, w tym:	40
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	20
Przygotowanie do ćwiczeń:	20
Łączny czas pracy studenta	100
Sumaryczna liczba punktów ECTS dla przedmiotu	4

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny

	kierunku studiów wraz z określeniem stopnia powiązania				
EK1	CB1A_W01+++	C1	W1-W12	1	O1
EK2	CB1A_W01+++	C3	W11-W12	1	O1
EK3	CB1A_U15+++	C1, C2	ĆW1-ĆW8	1	O1, O2
EK4	CB1A_U08++	C1, C2, C3	ĆW1-ĆW9	2, 3, 4	O1, O2
EK5	CB1A_U14++	C1, C2	ĆW9	2, 3, 4	O1, O2
EK6	CB1A_K01+	C1, C2, C3	W1-W13 ĆW1-ĆW9	1, 2, 3, 4	O2

Autor programu:	dr Maciej Czarnacki; dr Marcin Bogucki
Adres e-mail:	m.czarnacki@pollub.pl; m.bogucki@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Technicznej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Podstawy programowania
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C106
Rok:	I
Semestr:	1
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	75
Wykład	30
Ćwiczenia	
Laboratorium	45
Projekt	
Liczba punktów ECTS:	6
Sposób zaliczenia:	egzamin
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zapoznanie z podstawowymi pojęciami i technikami programowania
C2	Rozwinięcie umiejętności analitycznego myślenia i rozwiązywania problemów za pomocą algorytmów
C3	Praktyczne wprowadzenie do jednego z języków programowania wysokiego poziomu

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Podstawowa znajomość matematyki i logiki
2	Podstawowa znajomość obsługi komputerów

Efekty uczenia się	
	W zakresie wiedzy:
EK 1	zna podstawowe konstrukcje programistyczne
EK 2	rozumie podstawowe zasady pisania czytelnego i efektywnego kodu
	W zakresie umiejętności:
EK3	potrafi analizować i rozwiązywać proste problemy programistyczne
EK4	umie tworzyć, testować i debugować proste programy
	W zakresie kompetencji społecznych:
EK5	jest gotów do podejmowania wyzwań związanych z programowaniem i ich krytycznej oceny

Treści programowe przedmiotu
Forma zajęć - wykłady

	Treści programowe
W1	Wprowadzenie do programowania. Algorytm, program, kompilator, interpreter. Wybór i konfiguracja środowiska programistycznego
W2	Podstawy składni. Zmienne i typy danych. Operatory arytmetyczne i logiczne
W3	Instrukcje sterujące. Podstawowe operacje wejścia/wyjścia. Debugowanie
W4	Funkcje i modularność programu. Definiowanie i wywoływanie funkcji. Parametry i wartości zwracane
W5	Rekurencja
W6	Podstawowe struktury danych. Tablice. Listy
W7	Podstawy programowania obiektowego. Klasy, obiekty, właściwości, metody
W8	Dziedziczenie i polimorfizm
W9	Zdarzenia i wyjątki
W10	Podstawy budowy interfejsu użytkownika

Forma zajęć - laboratoria

	Treści programowe
L1	Wprowadzenie do programowania. Instalacja środowiska, konfiguracja IDE i tworzenie pierwszych programów konsolowych. Zmienne i typy danych
L2	Instrukcje sterujące. Operacje wejścia/wyjścia
L3	Debugowanie. Identyfikacja błędów i wykorzystanie debuggerów do analizy kodu
L4	Definiowanie i wywoływanie funkcji, parametry, wartości zwracane. Organizacja kodu w moduły
L5	Implementacja funkcji rekurencyjnych. Rozwiązywanie prostych problemów algorytmicznych
L6	Tablice jedno- i wielowymiarowe. Listy
L7	Podstawy programowania obiektowego. Tworzenie klas i obiektów, definiowanie właściwości i metod
L8	Dziedziczenie. Polimorfizm
L9	Obsługa wyjątków. Zarządzanie błędami w kodzie
L10	Tworzenie aplikacji z graficznym interfejsem użytkownika oraz obsługa zdarzeń

Metody dydaktyczne

1	wykład informacyjny
2	ćwiczenia laboratoryjne
3	metoda programowania z użyciem komputera

Metody i kryteria oceny

Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena wykonanych programów komputerowych	51%

Literatura podstawowa

1	Lis, Marcin, C#. Praktyczny kurs, Helion. Gliwice 2016.
---	---

Literatura uzupełniająca	
1	Michaelis, Mark, C# 8.0 : kompletny przewodnik dla praktyków, Helion, Gliwice 2021.
2	Alls, Jason, Czysty kod w C# : techniki refaktoryzacji i najlepsze praktyki, Helion, Gliwice 2021.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	75
Udział w wykładach:	30
Udział w zajęciach laboratoryjnych:	45
Praca własna studenta, w tym:	75
Studiowanie tematyki wykładów, przygotowanie do egzaminu:	35
Przygotowanie do zajęć laboratoryjnych:	40
Łączny czas pracy studenta	150
Sumaryczna liczba punktów ECTS dla przedmiotu	6

Macierz efektów uczenia się					
Symbol przedmiotowe go efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W06+++	C1, C2, C3	W1-W10	1	O1
EK 2	CB1A_W06+++	C1, C2, C3	W1-W10	1	O1
EK 3	CB1A_U06+ CB1A_U24+++	C1, C2, C3	L1-L10	2, 3	O2
EK 4	CB1A_U06+ CB1A_U24+++	C1, C2, C3	L1-L10	2, 3	O2
EK 5	CB1A_K01+ CB1A_K05++	C1, C2, C3	W1-W10	1	O1

Autor programu:	dr hab. Paweł Karczmarek, profesor uczelni; mgr Krystyna Kiersztyn; mgr Patrycja Miazek; mgr Alicja Żmudzińska; dr inż. Łukasz Gałka
Adres e-mail:	p.karczmarek@pollub.pl; k.kiersztyn@pollub.pl; p.miazek@pollub.pl; a.zmudzinska@pollub.pl; l.galka@pollub.pl

Jednostka organizacyjna:	Katedra Inteligencji Obliczeniowej
--------------------------	------------------------------------

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Podstawy systemów operacyjnych
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C107
Rok:	I
Semestr:	1
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	45
Wykład	15
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	3
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu

C1	Przekazanie podstawowej wiedzy na temat funkcjonowania systemów operacyjnych, ich roli, zadań systemów operacyjnych, problemów związanymi z ich realizacją i metodami ich rozwiązywania
C2	Zapoznanie z programami i narzędziami używanymi w systemach operacyjnych
C3	Zapoznanie z podstawowymi kwestiami zarządzania pakietami oprogramowania

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1	Umiejętność samodzielnej obsługi interfejsu użytkownika systemu operacyjnego oraz wykonywania podstawowych operacji na plikach i katalogach
----------	---

Efekty uczenia się

	W zakresie wiedzy:
EK 1	zna i rozumie architektury systemów operacyjnych oraz ich znaczenie w kontekście bezpieczeństwa informatycznego
EK 2	ma podstawową wiedzę o zadaniach systemu operacyjnego, problemach współbieżności, procesach i wątkach
EK 3	zna zasady funkcjonowania pamięci, systemów plików i operacji wejścia-wyjścia
	W zakresie umiejętności:
EK4	potrafi w stopniu podstawowym zarządzać i administrować systemami operacyjnymi w sposób zapewniający ich bezpieczeństwo
EK5	potrafi ocenić i wybrać właściwe metody i narzędzia potrzebne do zbudowania zgodnej z danymi założeniami aplikacji
	W zakresie kompetencji społecznych:

EK6	jest gotów do odpowiedzialnego pełnienia ról zawodowych wykazując dbałość o bezpieczeństwo, integralność i niezawodność systemów operacyjnych
------------	---

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Zadania systemów operacyjnych, struktura systemu, architektury systemów operacyjnych, jądro i jego znaczenie oraz architektura
W2	Powłoki oraz jej podstawowe typy, dostęp do systemu plików oraz struktura katalogów w systemach POSIX i Windows. Rola architektury systemu w zapewnianiu izolacji procesów, zarządzaniu uprawnieniami i integralnością systemu.
W3	Podstawowe operacje w systemie i narzędzia
W4	Koncepcja procesu i harmonogramu procesów w systemie operacyjnym
W5	Proces startu systemu i alokacji zasobów
W6	Zarządzanie pakietami oprogramowania i procesem instalacji i przygotowania oprogramowania
Forma zajęć - laboratoria	
	Treści programowe
L1	Wirtualizacja środowisk oraz tworzenie maszyn wirtualnych
L2	Powłoki systemów operacyjnych, podstawowa obsługa systemów plików oraz operacje na plikach i katalogach
L3	Przetwarzanie potokowe i zastosowanie filtrów w systemach operacyjnych, mechanizmy wejścia i wyjścia oraz manipulacja strumieniami danych
L4	Edycja plików tekstowych i binarnych
L5	Podstawy zarządzania i konfiguracji usług w systemie
L6	Zarządzanie oprogramowaniem i menedżerami pakietów
L7	Kompilacja oprogramowania dostarczanego w postaci źródłowej
L8	Zarządzanie kontami użytkowników i grup, nadawanie uprawnień oraz konfiguracja polityk bezpieczeństwa. Monitorowanie procesów, rejestrów zdarzeń i logów systemowych

Metody dydaktyczne	
1	wykład informacyjny
2	ćwiczenia laboratoryjne

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena wykonanych programów komputerowych	51%

Literatura podstawowa

1	Stallings W.: Systemy operacyjne : struktura i zasady budowy, Wyd. Naukowe PWN, 2006.
2	Tanenbaum A. S.: Systemy operacyjne. Wydanie IV, Helion, 2015.
3	Silbershatz A., Galvin P. B., Gagne G.: Podstawy systemów operacyjnych, Wydanie 7, WNT 2006.
4	Ebrahim M., Mallett A.: Skrypty powłoki systemu Linux. Zagadnienia zaawansowane, Wydanie II, Helion 2019.

Literatura uzupełniająca	
1	Nemeth E., i in.: Unix i Linux. Przewodnik administratora systemów. Wydanie V, Helion 2018.
2	Love R.: Linux programowanie systemowe, Helion 2008.
3	Bar M.: Linux : systemy plików, Wyd. RM, 2002.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	45
Udział w wykładach:	15
Udział w zajęciach laboratoryjnych:	30
Praca własna studenta, w tym:	30
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	10
Przygotowanie do zajęć laboratoryjnych:	20
Łączny czas pracy studenta	75
Sumaryczna liczba punktów ECTS dla przedmiotu	3

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W05+++	C1,C2	W1 - W6	1	O1
EK 2	CB1A_W05+++	C1,C2,C3	W1 - W6	1	O1
EK 3	CB1A_W05+++ CB1A_W06+	C1,C2	W1 - W6	1	O1
EK 4	CB1A_U10+++	C1,C2	L1 - L8	2	O1, O2
EK 5	CB1A_U10+++ CB1A_U12++	C1,C2,C3	L1 - L8	2	O1, O2

EK 6	CB1A_K05+	C1,C2,C3	W1 - W6 L1 - L8	1,2	O1, O2
------	-----------	----------	--------------------	-----	--------

Autor programu:	mgr inż. Albert Rachwał; dr Rafał Stęgiński
Adres e-mail:	a.rachwal@pollub.pl; r.stegierski@pollub.pl
Jednostka organizacyjna:	Katedra Inteligencji Obliczeniowej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Wstęp do sieci komputerowych
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C108
Rok:	I
Semestr:	1
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	60
Wykład	30
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	4
Sposób zaliczenia:	egzamin
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zapoznanie z podstawami działania sieci komputerowych, w tym ich architekturą, protokołami i standardami
C2	Zapoznanie z podstawową konfiguracją urządzeń sieciowych
C3	Rozwinięcie umiejętności diagnozowania i rozwiązywania problemów sieciowych
C4	Przygotowanie do dalszej nauki zaawansowanych technologii sieciowych w kontekście cyberbezpieczeństwa

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Podstawowa znajomość obsługi komputera
2	Znajomość podstawowych pojęć z zakresu systemów operacyjnych

Efekty uczenia się	
	W zakresie wiedzy:
EK1	zna podstawowe modele sieciowe oraz ich zastosowanie w komunikacji sieciowej
EK2	rozumie działanie i funkcje protokołów sieciowych, takich jak IP, TCP, UDP, DHCP, DNS
EK3	zna zasady adresacji IP oraz podziału na podsieci
EK4	zna i rozumie zasady zarządzania cyklem życia zasobów sieciowych, w tym uwzględniające bezpieczeństwo oraz ochronę prywatności, na wszystkich etapach: projektowania, wdrażania, eksploatacji i wycofywania infrastruktury sieciowej
	W zakresie umiejętności:
EK5	potrafi skonfigurować podstawowe urządzenia sieciowe, takie jak przełączniki i routery

EK6	potrafi analizować ruch sieciowy za pomocą wybranych narzędzi
EK7	potrafi diagnozować i rozwiązywać podstawowe problemy w sieciach komputerowych
EK8	potrafi zaprojektować podstawową sieć komputerową, uwzględniając topologię, adresację IP oraz odpowiedni dobór urządzeń sieciowych
	W zakresie kompetencji społecznych:
EK9	jest gotów do odpowiedzialnego pełnienia ról zawodowych w sektorze bezpieczeństwa cyfrowego, w szczególności w obszarze utrzymania i zabezpieczania sieci komputerowych, uwzględniając wymagania techniczne, organizacyjne i etyczne

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Definicje i podstawowe pojęcia z obszaru sieci komputerowych. Historia rozwoju sieci komputerowych. Typy oraz topologia sieci komputerowych
W2	Modele sieciowe: model TCP/IP, model OSI. Warstwy i ich funkcje. Przykłady protokołów w różnych warstwach (np. HTTP, TCP, IP, Ethernet)
W3	Adresacja IP i podstawy podsieci. Struktura adresów IPv4: klasy adresów, sieci prywatne i publiczne. Podstawy IPv6: format, struktura i zastosowania. Koncepcja maski podsieci i obliczanie zakresów adresów. Podział na podsieci (subnetting) – metody i przykłady
W4	Urządzenia sieciowe. Routery: funkcje i zastosowanie w przesyłaniu danych między sieciami. przełączniki: działanie, różnice między hubem a przełącznikiem. Punkty dostępu bezprzewodowego (AP): zastosowanie i konfiguracja. Inne urządzenia sieciowe
W5	Protokoły sieciowe. Protokół IP: funkcje, różnice między IPv4 a IPv6. Protokoły transportowe: TCP i UDP – różnice i zastosowania. Protokoły sieciowe: DHCP (przydzielanie adresów IP), DNS (tłumaczenie nazw na adresy IP). Protokoły aplikacyjne: HTTP/HTTPS, FTP, SMTP, POP3, IMAP. Protokół ARP i ICMP: mechanizmy działania i zastosowania
W6	Komunikacja w sieciach lokalnych i bezprzewodowych. Media transmisyjne w sieciach LAN: przewodowe (Ethernet) i światłowodowe. Podstawy działania Ethernetu. Standardy Wi-Fi: 802.11, działanie i konfiguracja. Zabezpieczenia sieci bezprzewodowych: szyfrowanie
W7	Analiza ruchu sieciowego. Narzędzia do analizy: Wireshark, tcpdump – podstawowe zastosowania. Diagnostyka połączeń: ping, traceroute, netstat. Identyfikacja i rozwiązywanie problemów sieciowych
W8	Podstawy bezpieczeństwa sieci komputerowych. Typowe zagrożenia sieciowe: sniffing, spoofing, ataki DoS, phishing. Rola firewalli i systemów IDS/IPS w ochronie sieci. Podstawy szyfrowania danych w sieci (SSL/TLS). Dobre praktyki w konfiguracji urządzeń sieciowych
Forma zajęć - laboratoria	
	Treści programowe

L1	Wprowadzenie do środowiska pracy i podstawowe komendy sieciowe. Wprowadzenie do symulatorów sieciowych (np. Cisco Packet Tracer, GNS3). Omówienie narzędzi sieciowych dostępnych w systemach operacyjnych
L2	Podstawy konfiguracji urządzeń sieciowych. Podstawowa konfiguracja routera (nazwa urządzenia, hasła dostępu). Konfiguracja interfejsów sieciowych. Tworzenie i testowanie połączeń między urządzeniami
L3	Adresacja IP. Przypisywanie statycznych adresów IPv4 urządzeniom w sieci. Ćwiczenia z obliczania i przypisywania adresów IP dla różnych podsieci. Testowanie komunikacji między urządzeniami w ramach jednej podsieci. Wprowadzenie do adresacji IPv6: przypisywanie adresów IPv6 w urządzeniach. Diagnostyka poprawności konfiguracji adresów IP
L4	Wprowadzenie do przełączników i ich funkcji w sieciach LAN. Konfiguracja VLAN (Virtual Local Area Network): tworzenie i przypisywanie VLAN-ów do portów przełącznika, testowanie izolacji ruchu między VLAN-ami. Ćwiczenia z konfiguracją połączeń typu trunk między przełącznikami
L5	Konfiguracja protokołów sieciowych. Konfiguracja serwera DHCP na routerze: przydzielanie dynamicznych adresów IP klientom w sieci, testowanie poprawności działania DHCP. Konfiguracja serwera DNS. Diagnostyka i rozwiązywanie problemów z protokołami DHCP i DNS
L6	Analiza ruchu sieciowego. Instalacja i konfiguracja narzędzia Wireshark. Analiza pakietów sieciowych: identyfikacja protokołów (DHCP, DNS, TCP, UDP, HTTP), analiza struktury ramki Ethernet i pakietów IP. Monitorowanie ruchu w lokalnej sieci: identyfikacja problemów i anomalii
L7	Rozwiązywanie problemów sieciowych. Symulacja problemów sieciowych: brak połączenia z internetem, błędy w konfiguracji adresacji IP, niewłaściwa konfiguracja VLAN-ów. Diagnostyka i naprawa problemów przy użyciu narzędzi sieciowych: ping, tracert, netstat. Dokumentowanie i raportowanie wyników diagnozy oraz podjętych działań
L8	Podstawy bezpieczeństwa sieci. Konfiguracja podstawowego firewalla na routerze. Tworzenie i testowanie reguł ACL (Access Control List) na routerach. Podstawowe techniki ochrony przełączników (np. zabezpieczenie dostępu do portów)
L9	Praktyczne zastosowanie zdobytej wiedzy w ramach projektu sieciowego. Zaprojektowanie i skonfigurowanie małej sieci komputerowej. Uwzględnienie adresacji IP, VLAN-ów i protokołów DHCP/DNS. Testowanie i weryfikacja działania zaprojektowanej sieci

Metody dydaktyczne	
1	wykład informacyjny
2	ćwiczenia laboratoryjne
3	metoda projektu

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy

O1	ocena pracy pisemnej	51%
O2	ocena wykonanych ćwiczeń laboratoryjnych	51%
O3	ocena przygotowanego projektu	51%

Literatura podstawowa		
1	Kurose, James, i in. Sieci komputerowe : ujęcie całościowe. Wyd. Helion, 2019.	
2	Jakub Kubica, i in., Podstawy sieci dla technika i studenta - Część 1. Wyd. ITStart, 2021.	
3	Marek Retinger, i in.i. Sieci komputerowe. Laboratorium. Wyd. Politechniki Poznańskiej, 2020.	

Literatura uzupełniająca		
1	Serafin, Marek, Bezpieczeństwo sieci firmowej : kontrola ruchu wychodzącego. Wyd. Helion, 2023.	
2	White, Russ, i in. Sieci komputerowe : najczęstsze problemy i ich rozwiązania : innowacyjne podejście do budowania odpornych, nowoczesnych sieci. Wyd. Helion, 2019.	
3	Stallings, William i in. Bezpieczeństwo systemów informatycznych : zasady i praktyka. T. 1 i 2. Wyd. Helion, 2019.	

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	60
Udział w wykładach:	30
Udział w zajęciach laboratoryjnych:	30
Praca własna studenta, w tym:	40
Studiowanie tematyki wykładów, przygotowanie do egzaminu:	25
Przygotowanie do zajęć laboratoryjnych:	15
Łączny czas pracy studenta	100
Sumaryczna liczba punktów ECTS dla przedmiotu	4

Macierz efektów uczenia się					
Symbol przedmiotowe go efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W09+++	C1, C2, C4	W1, W2, W6	1	O1

EK 2	CB1A_W09+++	C1, C2, C4	W2, W5, W6	1	O1
EK 3	CB1A_W09+++	C1, C2, C4	W3, W5, W6	1	O1
EK 4	CB1A_W09+++ CB1A_W21++	C1 - C4	W1, W4, W7, W8	1	O1
EK 5	CB1A_U16+++ CB1A_U10+++	C2, C4	L1 - L5, L9	2, 3	O2, O3
EK 6	CB1A_U16+++ CB1A_U10+++	C1, C3, C4	L6, L7	2	O2
EK 7	CB1A_U10+++	C1, C3, C4	L5, L7, L8	2	O2
EK 8	CB1A_U17++	C1 - C4	L9	3	O3
EK 9	CB1A_K05+	C1 - C4	W1 - W9, L1 - L9	1 - 3	O1 - O3

Autor programu:	mgr inż. Jacek Zaburko; dr hab. Arkadiusz Syta, profesor uczelni
Adres e-mail:	j.zaburko@pollub.pl; a.syta@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Technicznej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Wprowadzenie do cyberbezpieczeństwa
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C109
Rok:	I
Semestr:	1
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	45
Wykład	30
Ćwiczenia	
Laboratorium	15
Projekt	
Liczba punktów ECTS:	3
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zrozumienie podstawowych pojęć i zasad z zakresu cyberbezpieczeństwa
C2	Uzyskanie wiedzy o podstawowych podatnościach i zagrożeniach systemów informatycznych
C3	Uzyskanie podstawowych umiejętności z zakresu ochrony systemów informatycznych

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Podstawowe kompetencje cyfrowe
2	Umiejętność posługiwania się systemem operacyjnym komputera
2	Wiedza z zakresu podstawowych usług w sieciach komputerowych

Efekty uczenia się	
	W zakresie wiedzy:
EK 1	identyfikuje fundamentalne dylematy dotyczące zagrożeń w cyberprzestrzeni oraz funkcjonowania człowieka w społeczeństwie cyfrowym
EK 2	rozpoznaje metody oraz mechanizmy zapewniające bezpieczeństwo w systemach informatycznych
EK 3	wyszukuje przepisy prawne, normy i standardy określające wytyczne i wymagania w zakresie zapewniania bezpieczeństwa informatycznego, w tym dotyczące kształtowania polityki cyberbezpieczeństwa w przedsiębiorstwie
	W zakresie umiejętności:
EK 4	potrafi dokonać oceny istniejących rozwiązań w zakresie cyberbezpieczeństwa
EK 5	analizuje działanie systemów zabezpieczeń, identyfikując i reagując na zagrożenia

EK 6	planuje własne uczenie się przez całe życie, m.in. w celu podnoszenia swoich kompetencji zawodowych w obszarze cyberbezpieczeństwa
	W zakresie kompetencji społecznych:
EK 7	jest gotów do przestrzegania zasad etyki zawodowej, rozumiejąc znaczenie etycznych standardów specjalisty ds. cyberbezpieczeństwa

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Podstawowe pojęcia z zakresu cyberbezpieczeństwa. Podstawowe zasady bezpieczeństwa
W2	Najważniejsze normy i wymagania prawne, m.in. Dyrektywa NIS 2, ISO/IEC 27001, Ustawa o krajowym systemie cyberbezpieczeństwa
W3	Narodowe Standardy Cyberbezpieczeństwa
W4	Podstawy działania zespołów Red, Blue i Purple Team
W5	Rodzaje ataków
W6	Złośliwe oprogramowanie
W7	Podatności i zagrożenia
W8	Zarządzanie ryzykiem
W9	Bezpieczeństwo fizyczne urządzeń, kontrola dostępu
Forma zajęć - laboratoria	
	Treści programowe
L1	Uprawnienia systemu plików
L2	Zasady dotyczące haseł, ochrona haseł
L3	Zastosowania szyfrowania
L4	Bezpieczeństwo sieci bezprzewodowej
L5	Bezpieczeństwo przeglądarki i stron internetowych
L6	Identyfikacja ataków za pośrednictwem poczty elektronicznej, ochrona poczty elektronicznej
L7	Rozpoznawanie socjotechniki i reagowanie na jej wykrycie

Metody dydaktyczne	
1	wykład informacyjny
2	ćwiczenia laboratoryjne
3	metoda doświadczeń

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena przygotowanego referatu	51%
O2	ocena wykonanych ćwiczeń laboratoryjnych	51%
O3	obserwacja pracy studenta	51%

Literatura podstawowa	
1	Bravo, Cesar. Cyberbezpieczeństwo dla zaawansowanych. Skuteczne zabezpieczenia systemu Windows, Linux, IoT i infrastruktury w chmurze. Helion, 2023.
2	Parasram, Shiva V. N. Informatyka śledcza i Kali Linux. Przeprowadź analizy nośników pamięci, ruchu sieciowego i zawartości RAM-u za pomocą narzędzi systemu Kali Linux 2022.x. Helion, 2024.
3	Diogenes, Yuri, Ozkaya, Erdal. Cyberbezpieczeństwo - strategię ataku i obrony. Jak osiągnąć najwyższy możliwy stan zabezpieczeń systemu informatycznego. Helion, 2023.

Literatura uzupełniająca	
1	Krawiec, Jerzy. Cyberbezpieczeństwo. Podejście systemowe. Oficyna Wydawnicza Politechniki Warszawskiej, 2020.
2	Hubbard, Douglas W., Seiersen, Richard. Ryzyko w cyberbezpieczeństwie. Metody modelowania, pomiaru i szacowania ryzyka. Helion, 2024.
3	DiMaggio, Jon. Sztuka wojny cyfrowej. Przewodnik dla śledczego po szpiegostwie, oprogramowaniu ransomware i cyberprzestępczości zorganizowanej. Helion, 2023.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	45
Udział w wykładach:	30
Udział w zajęciach laboratoryjnych:	15
Praca własna studenta, w tym:	30
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	20
Przygotowanie do zajęć laboratoryjnych:	10
Łączny czas pracy studenta	75
Sumaryczna liczba punktów ECTS dla przedmiotu	3

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W02++	C1, C2	W1-W8	1	O1
EK 2	CB1A_W12++	C1, C2	W1-W8	1	O1

EK 3	CB1A_W13++	C1, C2	W1-W8	1	O1
EK 4	CB1A_U13+++	C1 - C3	L1-L9	2, 3	O2, O3
EK 5	CB1A_U18+++	C1 - C3	L1-L9	2, 3	O2, O3
EK 6	CB1A_U08++	C1 - C3	L1-L9	2, 3	O2, O3
EK 7	CB1A_K05++	C1 - C3	W1-W8, L1-L9	1 - 3	O1 - O3

Autor programu:	dr inż. Michał Charlak
Adres e-mail:	m.charlak@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Stosowanej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Bazy danych
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C110
Rok:	I
Semestr:	1
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	60
Wykład	30
Ćwiczenia	
Laboratorium	
Projekt	30
Liczba punktów ECTS:	4
Sposób zaliczenia:	egzamin
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zrozumienie podstaw teorii baz danych i modelu relacyjnego
C2	Rozwijanie praktycznych umiejętności w zakresie projektowania i zarządzania bazami danych
C3	Nabywanie umiejętności posługiwania się językiem SQL
C4	Zapoznanie z nowoczesnymi technologiami i zastosowaniami baz danych

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Umiejętność posługiwania się systemem operacyjnym komputera
2	Ogólna umiejętność posługiwania się narzędziami i programami w systemach komputerowych

Efekty uczenia się	
	W zakresie wiedzy:
EK 1	zna zasady tworzenia diagramów projektowania baz danych
EK 2	rozumie strukturę i elementy systemu bazodanowego oraz potrafi je obsługiwać i konfigurować
EK3	zna język SQL w zakresie przetwarzania danych, w tym pisanie zapytań, operacji na danych i zarządzania strukturą bazy danych
EK4	zna pełny cykl życia systemu bazodanowego, w tym etapy projektowania, implementacji, eksploatacji, optymalizacji oraz utrzymania, a także procesy związane z migracją i archiwizacją danych
	W zakresie umiejętności:

EK5	potrafi przełożyć wybrany obszar rzeczywistości na model ERD, tworząc relacje między encjami, oraz stosuje zasady normalizacji, aby zapewnić efektywną i optymalną strukturę bazy danych
EK6	posługuje się językiem SQL do przetwarzania i pobierania danych, tworząc zapytania odpowiadające specyficznym potrzebom oraz wymaganiom problemowym i potrafi budować zapytania, które dokładnie odpowiadają zadanym kryteriom
EK7	potrafi planować i realizować zadania projektowe związane z bazami danych, zarówno indywidualnie, jak i w zespole, efektywnie komunikując się z członkami grupy projektowej przy użyciu właściwej terminologii
	W zakresie kompetencji społecznych:
EK8	jest gotów do zasięgania opinii u specjalistów w przypadku trudności z samodzielnym rozwiązaniem problemów związanych z bazami danych, doceniając znaczenie ciągłego doskonalenia umiejętności w zakresie technologii bazodanowych jako kluczowych elementów rozwiązywania problemów w obszarze cyberbezpieczeństwa

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Pojęcie i historia baz danych
W2	Rodzaje baz danych: hierarchiczne, sieciowe, relacyjne, NoSQL
W3	Podstawy modelu relacyjnego: tabele, wiersze, kolumny
W4	Klucz podstawowy, klucz obcy, więzy integralności
W5	Relacje i ich typy: jeden-do-jednego, jeden-do-wielu, wiele-do-wielu
W6	Proces modelowania danych
W7	Normalizacja i denormalizacja: formy normalne
W8	Tworzenie, modyfikacja i usuwanie struktur bazy danych (DDL)
W9	Operacje na danych: wstawianie, usuwanie, aktualizacja i selekcja (DML)
W10	Flirty i sortowanie danych (WHERE, ORDER BY, GROUP BY, HAVING)
W11	Funkcje agregujące: COUNT, SUM, AVG, MAX, MIN i operacje na zbiorach: UNION, INTERSECT, EXCEPT
W12	Widoki (views) i ich zastosowania
W13	Procedury składowane i funkcje użytkownika (procedural SQL)
W14	Obsługa transakcji: ACID, COMMIT, ROLLBACK
W15	Zarządzanie użytkownikami i uprawnieniami, kopie zapasowe i odtwarzanie danych
Forma zajęć - projekt	
	Treści programowe
P1	Wprowadzenie do podstawowych zasad działania i organizacji baz danych relacyjnych. Definiowanie encji i związków między nimi
P2	Tworzenie diagramu bazy danych i jego normalizacja
P3	Podstawy języka SQL: polecenia DDL i DML
P4	Wybrane polecenia języka SQL: Filtry, unie, funkcje agregujące, łączenie tabel, operacje na datach

P5	Pisanie kwerend wykorzystujących podzapytania nieskorelowane oraz skorelowane w celu uzyskania specyficznych informacji z bazy danych
P6	Tworzenie wyzwalaczy automatyzujących operacje oraz widoków ułatwiających dostęp do danych. Tworzenie i zarządzanie procedurami w bazie danych uwzględniając wymagania bezpieczeństwa danych, filtrowania i zapewnienia kontroli dostępu do nich
P7	Zarządzanie użytkownikami, przydzielanie uprawnień i zarządzanie dostępem do bazy danych. Kopia zapasowa, import i eksport danych

Metody dydaktyczne	
1	wykład informacyjny
2	metoda projektu
3	praca wykonywana w grupach

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena przygotowanego projektu	51%
O3	ocena obrony projektu	51%

Literatura podstawowa	
1	Elmasri, Ramez A., i in. Wprowadzenie do systemów baz danych. Helion SA, 2019.
2	Mazur, Zygmunt, i in. Bazy danych. Oficyna Wyd. PW, 2000.
3	Krótkiewicz, Marek, i in. Asocjacyjny metamodel baz danych : definicja formalna oraz analiza porównawcza metamodeli baz danych. Oficyna Wydawnicza Politechniki Opolskiej, 2016.
4	Karwin, Bill, i in. Antywzorce języka SQL : jak uniknąć pułapek podczas programowania baz danych. Wyd. Helion, 2012.

Literatura uzupełniająca	
1	Sheldon, Robert, and Geoff Moes. Beginning MySQL. Wiley Pub., 2005.
2	Góźdź, Rafał, and Maria Skublewska-Paszkowska. Analysis of the Possibility of Managing the Database Stored in the Cloud. Journal of Computer Sciences Institute, vol. 2, no. 2, 2016, pp. 127-132.
3	Delobel, Claude, i in. Relacyjne bazy danych. Wydawnictwa Naukowo-Techniczne, 1989.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	60
Udział w wykładach:	30

Udział w zajęciach projektowych:	30
Praca własna studenta, w tym:	40
Studiowanie tematyki wykładów, przygotowanie do egzaminu:	25
Przygotowanie projektu:	15
Łączny czas pracy studenta	100
Sumaryczna liczba punktów ECTS dla przedmiotu	4

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W06+++	C1	W1 - W15	1	O1
EK 2	CB1A_W06+++	C1, C4	W1 - W15	1	O1
EK 3	CB1A_W06+++	C1, C4	W1 - W15	1	O1
EK 4	CB1A_W21++	C1, C4	W1 - W15	1	O1
EK 5	CB1A_U17+++ CB1A_U24++	C1, C2, C3	P1 - P7	2, 3	O2, O3
EK 6	CB1A_U17+++	C1, C3	P1 - P7	2, 3	O2, O3
EK 7	CB1A_U03++	C2	P1 - P7	2, 3	O2, O3
EK 8	CB1A_K02+	C1, C2, C3, C4	W1 - W15, P1 - P7	1, 2, 3	O1, O2, O3

Autor programu:	dr Rafał Stęgierski; mgr inż. Albert Rachwał; mgr Alicja Żmudzińska
Adres e-mail:	r.stegierski@pollub.pl; a.rachwal@pollub.pl; a.zmudzinska@pollub.pl
Jednostka organizacyjna:	Katedra Inteligencji Obliczeniowej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Matematyka dyskretna z elementami teorii liczb
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C201
Rok:	I
Semestr:	2
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	90
Wykład	45
Ćwiczenia	45
Laboratorium	
Projekt	
Liczba punktów ECTS:	6
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu

C1	Zapoznanie z podstawowymi pojęciami i technikami matematyki dyskretnej
C2	Wykształcenie umiejętności stosowania metod matematyki dyskretnej w rozwiązywaniu problemów z dziedziny informatyki i nauk technicznych
C3	Rozwinięcie zdolności analitycznego myślenia i rozumowania formalnego

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1	Znajomość podstaw matematyki
----------	------------------------------

Efekty uczenia się

	W zakresie wiedzy:
EK 1	definiuje podstawowe pojęcia matematyki dyskretnej, takie jak zbiory, relacje, funkcje, grafy i kombinatoryka
EK 2	objaśnia zastosowanie teorii grafów, logiki matematycznej i kombinatoryki w praktycznych problemach
	W zakresie umiejętności:
EK3	sporządza dowody matematyczne, w tym indukcyjne
EK4	posługuje się strukturami matematyki dyskretnej do modelowania i rozwiązywania problemów
	W zakresie kompetencji społecznych:
EK5	jest gotów do podejmowania wyzwań związanych z wykorzystaniem technik matematyki dyskretnej i ich krytycznej oceny

Treści programowe przedmiotu

Forma zajęć - wykłady	
	Treści programowe
W1	Operacje na zbiorach. Diagramy Venna. Podstawy algebry zbiorów. Indukcja matematyczna
W2	Wybrane zagadnienia z zakresu relacji
W3	Wybrane zagadnienia z zakresu funkcji, algorytmów i złożoności obliczeniowej
W4	Podstawy logiki i rachunku zdań. Tabele decyzyjne
W5	Wybrane zagadnienia kombinatoryki. Permutacje. Kombinacje. Wariacje. Diagramy drzewkowe
W6	Rekurencja
W7	Wybrane zagadnienia z zakresu prawdopodobieństwa. Prawdopodobieństwo warunkowe. Zmienne losowe. Prawo wielkich liczb
W8	Wybrane zagadnienia z teorii grafów. Reprezentacja grafów. Grafy etykietowane. Problem komiwojażera
W9	Drzewa binarne
W10	Wybrane zagadnienia zaawansowanej matematyki dyskretnej
W11	Podstawowe pojęcia z teorii liczb. Podzielność. Liczby pierwsze i faktoryzacja
W12	Kongruencje i teoria reszt. Arytmetyka modularna. Twierdzenie Eulera. Równania kongruencyjne
W13	Kwadraty i reszty kwadratowe. Krzywe eliptyczne. Hipoteza Riemanna i otwarte problemy teorii liczb
Forma zajęć - ćwiczenia	
	Treści programowe
ĆW1	Operacje na zbiorach i algebra zbiorów. Indukcja matematyczna
ĆW2	Relacje i ich własności
ĆW3	Badanie własności funkcji. Analiza złożoności algorytmów.
ĆW4	Implementacja tabel prawdy i przekształcanie wyrażeń logicznych. Weryfikacja tautologii i kontrtautologii. Analiza tabel decyzyjnych i ich zastosowanie
ĆW5	Algorytmy generowania permutacji, kombinacji i wariacji. Implementacja i wizualizacja diagramów drzewkowych
ĆW6	Implementacja i analiza algorytmów rekurencyjnych
ĆW7	Prawdopodobieństwo klasyczne i geometryczne, prawdopodobieństwo warunkowe i całkowite. Dyskretne zmienne losowe. Zastosowanie prawa wielkich liczb
ĆW8	Reprezentacja grafów: listy sąsiedztwa, macierz incydencji. Implementacja i analiza algorytmów przeszukiwania grafów. Rozwiązanie problemu komiwojażera
ĆW9	Implementacja drzew binarnych i operacji na nich. Eksperymentalna analiza różnych metod wyszukiwania
ĆW10	Implementacja i analiza struktur matematycznych. Eksperymentalna weryfikacja twierdzeń matematyki dyskretnej
ĆW11	Algorytmy podzielności i testowania pierwszości. Implementacja metod faktoryzacji liczb. Eksperymentalna analiza podzielności liczb

ĆW12	Operacje modularne i ich zastosowanie. Implementacja twierdzenia Eulera i rozwiązywanie równań kongruencyjnych. Algorytmy obliczania odwrotności modularnej
ĆW13	Znajdowanie reszt kwadratowych i ich zastosowania. Implementacja krzywych eliptycznych w kryptografii

Metody dydaktyczne	
1	wykład informacyjny
2	ćwiczenia laboratoryjne

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena wykonanych ćwiczeń laboratoryjnych	51%

Literatura podstawowa	
1	Fałda, Beata, i in. Wstęp do matematyki dyskretnej. Wyd. KUL, 2010.
2	Kordecki, Wojciech, i in. Matematyka dyskretna dla informatyków. Helion, 2018.
3	Marzantowicz, Wojciech, Zarzycki, Piotr, Elementarna teoria liczb. PWN. 2012.
Literatura uzupełniająca	
1	Pusz, Piotr, Elementy matematyki dyskretnej, Wyd. UR, Rzeszów 2018.
2	Kacprzak, Magdalena, Elementy matematyki dyskretnej : zbiór zadań, Wyd. PJWSTK, Warszawa 2008.
3	Rębowski, Ryszard, Płaskonka-Fietkowska, Janina, Zbiór zadań z matematyki dyskretnej dla informatyków, Wyd. PWST im Witelona, Legnica 2009.
4	Zakrzewski, Marek, Matematyka dyskretna, Oficyna Wydawnicza GIS, Wrocław 2014.
5	Ross, Kenneth A., Wright, Charles R. B., Matematyka dyskretna, Wyd. Naukowe PWN, Warszawa 2006.
6	Biegańska, Teresa, Górnicka, Anetta, Matematyka dyskretna : zbiór zadań, Wyd. im. Stanisława Podobińskiego, Częstochowa 2008.
7	Lewis, Harry R., Matematyka dyskretna : niezbędnik dla informatyków, Wyd. Naukowe PWN, Warszawa 2021.
8	Chojnacki, Andrzej, Jak to rozwiązać? Matematyka dyskretna. Część I, Wyd. WAT, Warszawa 2021.
9	Chojnacki, Andrzej, Jak to rozwiązać? Matematyka dyskretna. Część II, Wyd. WAT, Warszawa 2021.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności

Godziny kontaktowe z wykładowcą, w tym:	90
Udział w wykładach:	45
Udział w ćwiczeniach:	45
Praca własna studenta, w tym:	60
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	30
Przygotowanie do ćwiczeń:	30
Łączny czas pracy studenta	150
Sumaryczna liczba punktów ECTS dla przedmiotu	6

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W01+++	C1, C2, C3	W1-W13	1	O1
EK 2	CB1A_W01+++	C1, C2, C3	W1-W13	1	O1
EK 3	CB1A_U15+++	C1, C2, C3	ĆW1 - ĆW7	2	O2
EK 4	CB1A_U19++	C1, C2, C3	ĆW5 - ĆW10	2	O2
EK 5	CB1A_K01+	C1, C2, C3	W1-W13 ĆW1 -ĆW10	1, 2	O1,O2

Autor programu:	dr hab. Paweł Karczmarek, profesor uczelni; dr Adam Kiersztyn; mgr Krystyna Kiersztyn; dr inż. Łukasz Gałka
Adres e-mail:	p.karczmarek@pollub.pl; a.kiersztyn@pollub.pl; k.kiersztyn@pollub.pl; l.galka@pollub.pl
Jednostka organizacyjna:	Katedra Inteligencji Obliczeniowej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Podstawy inżynierii oprogramowania i zarządzania projektami IT
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C202
Rok:	I
Semestr:	2
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	60
Wykład	30
Ćwiczenia	
Laboratorium	
Projekt	30
Liczba punktów ECTS:	4
Sposób zaliczenia:	egzamin
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zapoznanie z metodami inżynierii oprogramowania
C2	Nabycie praktycznej wiedzy z zakresu inżynierii oprogramowania, jej metodyk i stosowania w każdej fazie cyklu życia oprogramowania

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Podstawowa wiedza z zakresu baz danych
2	Znajomość zasad programowania obiektowego

Efekty uczenia się	
	W zakresie wiedzy:
EK 1	ma wiedzę dotyczącą właściwości metod inżynierii oprogramowania
EK 2	ma podstawową wiedzę dotyczącą stosowania podstawowych metodyk wytwarzania oprogramowania
	W zakresie umiejętności:
EK3	potrafi stosować wybrane techniki inżynierii oprogramowania
EK4	potrafi umiejętnie stosować wybrane metodyki wytwórcze w zależności od uwarunkowań projektowych
	W zakresie kompetencji społecznych:
EK5	jest gotów do podejmowania wyzwań związanych z wykorzystaniem nowoczesnych metodyk inżynierii oprogramowania i ich krytycznej oceny

Treści programowe przedmiotu

Forma zajęć - wykłady	
	Treści programowe
W1	Cykle życia i procesy wytwarzania oprogramowania
W2	Inżynieria wymagań. Pozyskiwanie wymagań
W3	Metody strukturalne analizy i projektowania oprogramowania. Diagramy encji, przepływu danych
W4	Metody obiektowe analizy i projektowania oprogramowania. Diagramy przypadków użycia. Przypadki użycia i ich scenariusze. Diagramy klas i obiektów
W5	Jakość kodu. Przeglądy kodu
W6	Testowanie aplikacji
W7	Tworzenie dokumentacji oprogramowania
W8	Konserwacja oprogramowania
W9	Systemy krytyczne
W10	Wybrane wzorce projektowe i ich implementacja
W11	Zarządzanie projektem informatycznym. Cechy projektu. Wybrane aspekty zarządzania projektem. Wybrane narzędzia do zarządzania projektami
W12	Metodyki zwinne. Diagram spalania
W13	Systemy kontroli wersji
W14	Sztuczna inteligencja w tworzeniu oprogramowania

Forma zajęć - projekt	
	Treści programowe
P1	Wprowadzenie do zarządzania projektem informatycznym. Tworzenie harmonogramów projektów
P2	Metody oceny czasochłonności i pracochłonności zadań
P3	Planowanie i analiza wymagań
P4	Wybrane diagramy wykorzystujące metody obiektowe i strukturalne, stosowane do zaprojektowania systemu informatycznego, w tym diagramy przypadków użycia, klas, obiektów i czynności
P5	Tworzenie wybranych diagramów opisujących przepływ procesów i obiektów w systemie, w tym diagramów modelowania procesów biznesowych
P6	Omówienie wybranych wzorców projektowych i ich zastosowania
P7	Techniki analizy jakości kodu i refaktoryzacja, wprowadzenie do testowania
P8	Konserwacja oprogramowania i zarządzanie zmianami
P9	Systemy krytyczne i optymalizacja

Metody dydaktyczne	
1	wykład informacyjny
2	metoda projektu
3	ćwiczenia laboratoryjne

Metody i kryteria oceny

Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena przygotowanego projektu	51%
O3	ocena obrony projektu	51%

Literatura podstawowa	
1	Sacha K.: Inżynieria oprogramowania, Warszawa: PWN, 2023 (2010).
2	UML 2.1. Ćwiczenia. Pod red. St. Wryczy, Helion, 2007.
3	Jaszkiewicz A.: Inżynieria oprogramowania. Helion, Gliwice 1997.

Literatura uzupełniająca	
1	Martin R. C.: Czysty kod : podręcznik dobrego programisty, Helion, Gliwice 2014.
2	Wiegers K. E., Beatty J. A.: Specyfikacja oprogramowania : inżynieria wymagań, Helion, Gliwice 2014.
3	Bruegge B., Dutoit A.: Inżynieria oprogramowania w ujęciu obiektowym : UML, wzorce projektowe i Java, Helion, Gliwice 2011.
4	Sutherland J. J.: SCRUM w praktyce, PWN, Warszawa 2020.
5	Koszlańda A.: Zarządzanie projektami IT : przewodnik po metodykach, Helion, Gliwice 2010.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	60
Udział w wykładach:	30
Udział w zajęciach projektowych:	30
Praca własna studenta, w tym:	40
Studiowanie tematyki wykładów, przygotowanie do egzaminu:	25
Przygotowanie projektu:	15
Łączny czas pracy studenta	100
Sumaryczna liczba punktów ECTS dla przedmiotu	4

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny

	wraz z określeniem stopnia powiązania				
EK 1	CB1A_W10+++	C1	W1-W12	1	O1
EK 2	CB1A_W17++	C2	W1-W12	1	O1
EK 3	CB1A_U17++	C1, C2	P1 - P9	2, 3	O2, O3
EK 4	CB1A_U12++ CB1A_U24+++ CB1A_U17+	C1, C2	P1 - P9	2, 3	O2, O3
EK 5	CB1A_K01+	C1, C2	W11, W12 P1 - P9	1, 2, 3	O1, O2, O3

Autor programu:	dr hab. Paweł Karczmarek, profesor uczelni; mgr Patrycja Miazek; mgr inż. Albert Rachwał; dr inż. Łukasz Gałka
Adres e-mail:	p.karczmarek@pollub.pl; p.miazek@pollub.pl; a.rachwal@pollub.pl; l.galka@pollub.pl
Jednostka organizacyjna:	Katedra Inteligencji Obliczeniowej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Algorytmy i struktury danych
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C203
Rok:	I
Semestr:	2
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	60
Wykład	30
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	4
Sposób zaliczenia:	egzamin
Język wykładowy:	język polski

Cele przedmiotu

C1	Zapoznanie z podstawowymi pojęciami dotyczącymi algorytmów i struktur danych
C2	Opanowanie umiejętności implementacji i analizy algorytmów

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1	Znajomość podstaw programowania
2	Znajomość podstaw analizy matematycznej

Efekty uczenia się

	W zakresie wiedzy:
EK 1	zna i rozumie klasyczne algorytmy (sortujące, tekstowe) oraz podstawowe i złożone struktury danych, w tym ich zastosowania w rozwiązywaniu problemów obliczeniowych
EK 2	zna metody projektowania algorytmów oraz wylicza ich złożoność obliczeniową
	W zakresie umiejętności:
EK3	oblicza złożoność algorytmów
EK4	stosuje podstawowe i złożone struktury danych
EK5	analizuje postawiony problem oraz projektuje odpowiedni algorytm jego rozwiązania
	W zakresie kompetencji społecznych:
EK6	jest gotów do zasięgania opinii oraz wsparcia podczas rozwiązywania złożonych problemów

Treści programowe przedmiotu

Forma zajęć - wykłady	
	Treści programowe
W1	Poprawność i złożoność obliczeniowa algorytmów
W2	Metody projektowania algorytmów
W3	Wyszukiwanie i sortowanie
W4	Algorytmy rekurencyjne. Rozwiązywanie niektórych równań rekurencyjnych
W5	Podstawowe struktury danych i abstrakcyjne struktury danych
W6	Kolejka priorytetowa, słownik
W7	Podstawowe algorytmy grafowe
W8	Wybrane algorytmy tekstowe
Forma zajęć - laboratoria	
	Treści programowe
L1	Analiza poprawności i złożoności obliczeniowej algorytmów
L2	Porównanie metod projektowania algorytmów
L3	Implementacja wybranych algorytmów sortujących i wyszukiwujących
L4	Implementacja algorytmów rekurencyjnych
L5	Implementacja wybranych struktur danych
L6	Implementacja kolejki priorytetowej
L7	Implementacja podstawowych algorytmów grafowych
L8	Implementacja wybranych algorytmów tekstowych

Metody dydaktyczne	
1	wykład informacyjny
2	praca wykonywana indywidualnie
3	ćwiczenia laboratoryjne

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena wykonanych ćwiczeń laboratoryjnych	51%
O3	ocena aktywności w trakcie zajęć	51%

Literatura podstawowa	
1	Banachowski, Lech, i in. Algorytmy i struktury danych. Wyd. Naukowe PWN, 2018.
2	Wirth, Niklaus, i in. Algorytmy + struktury danych = programy. Wydawnictwa Naukowo-Techniczne, 2002.
3	Dańko, Anna, i in. Algorytmy i struktury danych : zadania. Wyd. Polsko-Japońskiej Wyższej Szkoły Technik Komputerowych, 2006.

Literatura uzupełniająca

1	Debudaj-Grabysz, Agnieszka, i in. Algorytmy i struktury danych : wybór zaawansowanych metod. Wyd. Politechniki Śląskiej, 2011.
---	--

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	60
Udział w wykładach:	30
Udział w zajęciach laboratoryjnych:	30
Praca własna studenta, w tym:	40
Studiowanie tematyki wykładów, przygotowanie do egzaminu:	25
Przygotowanie do zajęć laboratoryjnych:	15
Łączny czas pracy studenta	100
Sumaryczna liczba punktów ECTS dla przedmiotu	4

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W06+++	C1	W3 - W6	1	O1
EK 2	CB1A_W06+++	C1	W1, W2	1	O1
EK 3	CB1A_U12++ CB1A_U24+++	C2	L1	2, 3	O2, O3
EK 4	CB1A_U24+++	C2	L2, L3	2, 3	O2, O3
EK 5	CB1A_U24+++	C2	L1 - L5	2, 3	O2, O3
EK 6	CB1A_K02+	C1, C2	L1-L5	2, 3	O2, O3

Autor programu:	dr Adam Kiersztyn; dr inż. Łukasz Gałka; mgr Krystyna Kiersztyn
Adres e-mail:	a.kiersztyn@pollub.pl; l.galka@pollub.pl; k.kiersztyn@pollub.pl
Jednostka organizacyjna:	Katedra Inteligencji Obliczeniowej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Podstawy kryptografii
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C204
Rok:	I
Semestr:	2
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	45
Wykład	15
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	3
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu

C1	Zrozumienie podstawowych pojęć kryptografii
C2	Nabycie umiejętności analizy algorytmów kryptograficznych
C3	Zrozumienie zastosowań kryptografii

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1	Znajomość matematyki z dotychczasowego toku studiów
2	Znajomość podstaw programowania obiektowego

Efekty uczenia się

	W zakresie wiedzy:
EK1	definiuje podstawowe pojęcia kryptografii oraz zna działanie podstawowych algorytmów kryptograficznych, oraz ich zastosowania w praktyce
	W zakresie umiejętności:
EK2	dobiera i implementuje podstawowe algorytmy kryptograficzne w wybranym języku programowania
EK3	potrafi ocenić bezpieczeństwo różnych metod kryptograficznych oraz zidentyfikować potencjalne zagrożenia i ataki
	W zakresie kompetencji społecznych:
EK4	jest gotów do zasięgnięcia opinii i wsparcia ekspertów w celu znalezienia optymalnych rozwiązań

Treści programowe przedmiotu

Forma zajęć - wykłady

	Treści programowe
W1	Wprowadzenie do kryptografii
W2	Szyfrowanie symetryczne
W3	Szyfrowanie asymetryczne
W4	Podpisy cyfrowe
W5	Steganografia
W6	Analiza bezpieczeństwa algorytmów
W7	Praktyczne zastosowania kryptografii. Przyszłość kryptografii
Forma zajęć - laboratoria	
	Treści programowe
L1	Wprowadzenie do narzędzi kryptograficznych. Praktyczne zastosowanie algorytmów szyfrowania
L2	Tworzenie i weryfikacja podpisów cyfrowych
L3	Szyfrowanie Cezara: Implementacja prostego algorytmu szyfrowania Cezara, stworzenie programu, który przesuwa litery w alfabecie o określoną liczbę miejsc
L4	Zarządzanie kluczami w praktyce
L5	Analiza ataków na systemy kryptograficzne
L6	Kryptografia w sieciach
L7	Szyfrowanie plików za pomocą narzędzi online
L8	Szyfrowanie i deszyfrowanie wiadomości: stworzenie programu, który szyfruje i deszyfruje krótkie wiadomości tekstowe przy użyciu algorytmu ROT13
L9	Szyfrowanie wiadomości przy użyciu alfabetu Morse'a: stworzenie programu, który konwertuje tekst na kod Morse'a i odwrotnie
L10	Szyfrowanie wiadomości przy użyciu szyfru Polibiusza
L11	Szyfrowanie wiadomości przy użyciu szyfru Atbash
L12	Kryptografia w chmurze. Analiza metod zabezpieczania danych w chmurze z wykorzystaniem szyfrowania
L13	Kryptografia w mediach społecznościowych. Zastosowania kryptografii w zabezpieczaniu danych użytkowników w aplikacjach społecznościowych

Metody dydaktyczne	
1	wykład informacyjny
2	metoda programowania z użyciem komputera
3	przygotowanie sprawozdania

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena wykonanych ćwiczeń laboratoryjnych	51%
O3	obserwacja pracy studenta	51%
O4	ocena wykonanych sprawozdań laboratoryjnych	51%

Literatura podstawowa	
1	Karbowski, Marcin. "Podstawy kryptografii." Helion, 2023.
2	Aumasson, Jean-Philippe, Dąbkowska Kowalik, Małgorzata (tłumacz), Sikorski, Witold (tłumacz), „Nowoczesna kryptografia : praktyczne wprowadzenie do szyfrowania.” Warszawa: PWN, 2018.
3	Biernat, Janusz, „Kodowanie i szyfrowanie.” Akademicka Oficyna Wydawnicza EXIT, Warszawa, 2017.

Literatura uzupełniająca	
1	Mosorov, Volodymyr, „Steganografia cyfrowa : sztuka ukrywania informacji”, Wyd. Uniwersytetu Łódzkiego, 2013.
2	Levy, Steven, Szporko, Jacek. (tłumacz), „Rewolucja w kryptografii.” Wydawnictwa Naukowo-Techniczne, Warszawa, 2002.
3	Ogiela, Marek R., „Podstawy kryptografii.” Akademia Górniczo-Hutnicza im. Stanisława Staszica (Kraków). AGH Uczelniane Wydawnictwa Naukowo-Dydaktyczne, 2000.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	45
Udział w wykładach:	15
Udział w zajęciach laboratoryjnych:	30
Praca własna studenta, w tym:	30
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	10
Przygotowanie do zajęć laboratoryjnych:	20
Łączny czas pracy studenta	75
Sumaryczna liczba punktów ECTS dla przedmiotu	3

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W07+++	C1, C2, C3	W1 - W7	1	O1
EK 2	CB1A_U19+++	C1, C2, C3	L1-L13	2, 3	O2, O3, O4

EK 3	CB1A_U15++	C2, C3	L1-L13	2, 3	O2, O3, O4
EK 4	CB1A_K02+	C2, C3	W4, L1-L13	1, 2, 3	O1, O2, O3, O4

Autor programu:	dr inż. Marek B. Horyński
Adres e-mail:	m.horynski@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Stosowanej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Administracja systemami operacyjnymi
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C205
Rok:	I
Semestr:	2
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	45
Wykład	15
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	3
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu

C1	Zapoznanie z praktycznymi umiejętnościami w zakresie konfiguracji i zarządzania systemami operacyjnymi
C2	Zapoznanie z umiejętnościami rozwiązywania problemów i reagowania na incydenty

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1	Wiedza z zakresu podstaw programowania
2	Wiedza z zakresu podstaw systemów operacyjnych
3	Wiedza z zakresu sieci komputerowych

Efekty uczenia się

	W zakresie wiedzy:
EK1	zna i rozumie koncepcje architektury systemów operacyjnych, w tym mechanizmy zarządzania procesami, pamięcią, urządzeniami wejścia_Wyjścia oraz systemami plików, i ich wpływ na efektywność oraz niezawodność systemów komputerowych
EK2	zna i rozumie mechanizmy ochrony i kontroli dostępu implementowane w systemach operacyjnych, a także ich znaczenie dla zapewnienia bezpieczeństwa informatycznego
	W zakresie umiejętności:
EK3	potrafi konfigurować oraz zarządzać systemami operacyjnymi, stosując odpowiednie mechanizmy zapewniające ich bezpieczeństwo
EK4	potrafi wdrażać i optymalizować działanie systemów operacyjnych, uwzględniając aspekty wydajnościowe i bezpieczeństwa

EK5	potrafi identyfikować i analizować wyzwania związane z bezpieczeństwem systemów operacyjnych, oraz na bieżąco doskonalić swoje umiejętności w zakresie ochrony systemów przed atakami
	W zakresie kompetencji społecznych:
EK6	jest gotów do odpowiedzialnego pełnienia roli specjalisty w dziedzinie bezpieczeństwa cyfrowego, angażując się w działania mające na celu ochronę danych oraz systemów operacyjnych

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Podstawowe funkcje i architektura systemów operacyjnych
W2	Zarządzanie procesami i wątkami
W3	Techniki zarządzania pamięcią i mechanizmy obrony
W4	Systemy plików i zarządzanie danymi
W5	Zarządzanie urządzeniami wejścia/wyjścia
W6	Bezpieczeństwo systemów operacyjnych
W7	Automatyzacja i skrypty w administracji systemami
Forma zajęć - laboratoria	
	Treści programowe
L1	Instalacja różnych systemów operacyjnych i konfiguracja podstawowych ustawień
L2	Tworzenie, modyfikacja i usuwanie kont użytkowników i grup. Zarządzanie uprawnieniami i politykami bezpieczeństwa
L3	Monitorowanie i kontrola procesów. Użycie narzędzi do zarządzania procesami
L4	Analiza wykorzystania pamięci. Konfiguracja pamięci wirtualnej i pamięci wymiany
L5	Tworzenie i zarządzanie systemami plików. Operacje na plikach i katalogach
L6	Instalacja, konfiguracja i zarządzanie urządzeniami peryferyjnymi
L7	Konfiguracja zapory sieciowej. Ustawienia zabezpieczeń systemowych
L8	Harmonogram zadań. Tworzenie skryptów automatyzujących
L9	Użycie narzędzi do monitorowania wydajności systemu. Analiza logów systemowych
L10	Konfiguracja ustawień sieciowych. Diagnostyka sieci
L11	Tworzenie i zarządzanie kopiami zapasowymi. Procedury odzyskiwania danych
L12	Instalacja i konfiguracja maszyn wirtualnych. Zarządzanie zasobami w środowisku wirtualnym
L13	Konfiguracja automatycznych aktualizacji. Ręczne instalowanie aktualizacji i poprawek
L14	Instalacja i konfiguracja wybranych usług sieciowych. Zarządzanie usługami systemowymi
L15	Diagnostyka i naprawa typowych problemów systemowych za pomocą odpowiednich narzędzi

Metody dydaktyczne	
1	wykład informacyjny
2	dyskusja dydaktyczna
3	ćwiczenia laboratoryjne

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena wykonanych ćwiczeń laboratoryjnych	51%

Literatura podstawowa	
1	Tanenbaum Andrew S. Systemy operacyjne. Helion, 2010.
2	Silberschatz Abraham, Galvin Peter B., Gagne Greg. Podstawy systemów operacyjnych T1. Wyd. naukowe PWN, 2021.
3	Silberschatz Abraham, Galvin Peter B., Gagne Greg. Podstawy systemów operacyjnych T2. Wyd. naukowe PWN, 2021.

Literatura uzupełniająca	
1	Remzi H Arpaci-Dusseau, Andrea C Arpaci-Dusseau. Operating Systems: Three Easy Pieces. CreateSpace Independent Publishing Platform, 2018.
2	Love Robert. Linux: Programowania systemowe. Helion, 2014.
3	Bott Ed, Siecher Carl, Stinson Craig. Windows 10 PL od środka. Helion, 2016.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	45
Udział w wykładach:	15
Udział w zajęciach laboratoryjnych:	30
Praca własna studenta, w tym:	30
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	10
Przygotowanie do zajęć laboratoryjnych:	20
Łączny czas pracy studenta	75
Sumaryczna liczba punktów ECTS dla przedmiotu	3

Macierz efektów uczenia się					
Symbol przedmiotowe	Odniesienie przedmiotowego efektu uczenia się	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny

go efektu uczenia się	do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania				
EK 1	CB1A_W05+++	C1	W1 - W7	1,2	O1
EK 2	CB1A_W05+++	C1	W6	1, 2	O1
EK 3	CB1A_U10+++	C1, C2	L1 - L15	2, 3	O2
EK 4	CB1A_U10+++	C1, C2	L1 - L15	2, 3	O2
EK 5	CB1A_U08++	C3	L1 - L15	2, 3	O2
EK 6	CB1A_K05+	C1 - C3	W1 - W7, L1 - L15	1 - 3	O1, O2

Autor programu:	dr hab. Arkadiusz Syta, profesor uczelni
Adres e-mail:	a.syta@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Technicznej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Programowanie skryptowe
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C206
Rok:	I
Semestr:	2
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	45
Wykład	15
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	3
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu

C1	Przekazanie podstawowej wiedzy na temat języków programowania skryptów powłoki
C2	Zapoznanie z zastosowaniami języków programowania skryptów powłoki
C3	Nabywanie umiejętności automatyzacji zadań

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1	Podstawowa wiedza z zakresu programowania
2	Podstawowa wiedza z zakresu systemów operacyjnych

Efekty uczenia się

	W zakresie wiedzy:
EK 1	posiada wiedzę na temat podstawowych konstrukcji języków skryptów powłoki oraz struktur danych
EK 2	posiada wiedzę na temat zastosowania języków skryptowych do automatyzacji
	W zakresie umiejętności:
EK3	potrafi tworzyć, testować oraz analizować skrypty dla najpopularniejszych powłok różnych systemów operacyjnych
EK4	rozwiązuje wybrane problemy programistyczne
	W zakresie kompetencji społecznych:
EK5	jest gotów do odpowiedzialnego wykorzystania umiejętności programowania skryptowego w celu automatyzacji zadań związanych z bezpieczeństwem systemów informatycznych, dbając o przestrzeganie zasad etyki zawodowej oraz norm prawnych

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Wprowadzenie do języków skryptów powłoki, narzędzia i środowisko tworzenia skryptów i ich uruchamiania, przegląd języków skryptowych w kontekście powłok różnych systemów operacyjnych
W2	Podstawy składni i konstrukcji wybranego języka skryptowego powłoki systemowej
W3	Tworzenie podstawowych programów oraz implementacje wybranych algorytmów
W4	Tworzenie funkcji wykorzystujących dostępne polecenia systemowe, instrukcje sterujące, warunkowe oraz pętle w językach skryptu powłoki
W5	Sposoby uruchamiania skryptów dla powłoki systemu
W6	Obsługa plików oraz strumieni wejściowych i wyjściowych, dopasowanie do szablonów i wyrażenia regularne
W7	Zastosowanie wybranego języka skryptowego do automatyzacji zadań systemowych, obsługa usług systemu
Forma zajęć - laboratoria	
	Treści programowe
L1	Wprowadzenie do środowiska tworzenia programów w języku skryptów powłoki systemowej dla różnych systemów operacyjnych
L2	Podstawowe konstrukcje języka skryptowego
L3	Tworzenie funkcji i wielokrotne wykorzystywanie kodu w ramach skryptów powłoki
L4	Obsługa plików i strumieni wejściowych/wyjściowych
L5	Praca z kolekcjami danych
L6	Stosowanie szablonów i wyrażeń regularnych
L7	Stosowanie bibliotek w programowaniu, ich instalacja i konfiguracja
L8	Debugowanie programu skryptu powłoki
L9	Obsługa błędów i raportowanie problemów

Metody dydaktyczne	
1	wykład informacyjny
2	ćwiczenia laboratoryjne

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena wykonanych programów komputerowych	51%

Literatura podstawowa	
1	Lakshman, S., Skrypty powłoki systemu Linux : receptury, najlepsze przepisy na smakowite skrypty!, Helion, 2012.

2	Lach M., Bash Praktyczne skrypty, Helion, 2015.
3	Foster-Johnson, E., Skrypty powłoki : od podstaw, Helion, 2006.
4	Newham, C., Bash : wprowadzenie, Helion, 2006.
5	Dawson, M., Python dla każdego : podstawy programowania, Helion, 2014.

Literatura uzupełniająca	
1	Jaworski, M., Profesjonalne programowanie w Pythonie : poziom ekspert, Helion, 2017.
2	Flanagan D., JavaScript. Przewodnik. Poznaj język mistrzów programowania, Wydanie VII, Helion, 2021.
3	Brash, R., Naik, G., Bash Cookbook: Leverage Bash Scripting to Automate Daily Tasks and Improve Productivity. 1st ed., Packt Publishing, 2018.
4	Taylor, D., Genialne skrypty powłoki : ponad 100 rozwiązań dla systemów Linux, macOS i Unix, Helion, 2017.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	45
Udział w wykładach:	15
Udział w zajęciach laboratoryjnych:	30
Praca własna studenta, w tym:	30
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	10
Przygotowanie do zajęć laboratoryjnych:	20
Łączny czas pracy studenta	75
Sumaryczna liczba punktów ECTS dla przedmiotu	3

Macierz efektów uczenia się					
Symbol przedmiotowe go efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W06++	C1,C2	W1-W7	1	O1
EK 2	CB1A_W06++	C1,C3	W1-W7	1	O1
EK 3	CB1A_U12++ CB1A_U24+++	C2,C3	L1-L9	2	O2
EK 4	CB1A_U12++ CB1A_U24+++	C2,C3	L1-L9	1	O2

EK 5	CB1A_K05+	C2,C3	W1-W7 L1-L9	1,2	O1,O2
------	-----------	-------	----------------	-----	-------

Autor programu:	dr Rafał Stęgiński
Adres e-mail:	r.stegierski@pollub.pl
Jednostka organizacyjna:	Katedra Inteligencji Obliczeniowej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Programowanie aplikacji internetowych
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C207
Rok:	I
Semestr:	2
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	75
Wykład	30
Ćwiczenia	
Laboratorium	45
Projekt	
Liczba punktów ECTS:	5
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zapoznanie z podstawowymi oraz zaawansowanymi zasadami projektowania, tworzenia i wdrażania aplikacji internetowych
C2	Rozwój umiejętności analizy wymagań użytkowników, projektowania interfejsów oraz implementacji aplikacji zgodnych z nowoczesnymi standardami
C3	Nabycie świadomości zagrożeń związanych z projektowaniem i użytkowaniem aplikacji internetowych oraz stosowanie dobrych praktyk zapewniających bezpieczeństwo

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Podstawy programowania obiektowego
2	Podstawowa wiedza z zakresu baz danych

Efekty uczenia się	
	W zakresie wiedzy:
EK1	rozpoznaje podstawowe pojęcia związane z architekturą aplikacji internetowych, w tym zasady działania modelu klient-serwer i protokołu HTTP
EK2	opisuje proces projektowania i implementacji aplikacji internetowych, w tym tworzenie interfejsu użytkownika, warstwy serwerowej i obsługi baz danych
EK3	rozdziela podstawowe techniki uwierzytelniania, autoryzacji oraz zabezpieczania aplikacji internetowych
	W zakresie umiejętności:
EK4	wykorzystuje technologie programowania po stronie klienta i serwera do tworzenia dynamicznych i interaktywnych aplikacji

EK5	stosuje mechanizmy bezpieczeństwa, a także metody uwierzytelniania i autoryzacji użytkowników do tworzenia bezpiecznych aplikacji internetowych
EK6	weryfikuje opracowane rozwiązania poprzez testowanie i wdraża odpowiednie strategie naprawcze w zakresie prawidłowego funkcjonowania i bezpieczeństwa aplikacji internetowych
	W zakresie kompetencji społecznych:
EK7	wykazuje postawę odpowiedzialności za jakość swojej pracy, szczególnie w kontekście bezpieczeństwa danych użytkowników i niezawodności aplikacji

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Wprowadzenie do programowania aplikacji internetowych - historia i rozwój technologii webowych
W2	Struktura aplikacji internetowej. Podział aplikacji na backend i frontend
W3	Struktura dokumentów i podstawy tworzenia stron internetowych. Protokół HTTP. Obiektowy model dokumentów
W4	Formatowanie i stylizacja dokumentów - kaskadowe arkusze stylów
W5	Podstawy programowania po stronie klienta. Wprowadzenie do języków skryptowych. Manipulacja strukturą dokumentu. Obsługa zdarzeń w aplikacjach internetowych
W6	Tworzenie komponentów interfejsu użytkownika. Dynamiczne ładowanie treści. Asynchroniczna wymiana danych pomiędzy klientem a serwerem. Animacje
W7	Projektowanie interfejsów użytkownika. Dostosowanie stron do różnych urządzeń (RWD), ich elastyczność i dostępność. Udoskonalanie witryn pod kątem wyszukiwarek oraz zasady SEO. Wykorzystanie narzędzi programistycznych dostępnych w przeglądarkach
W8	Podstawy programowania po stronie serwera. Przetwarzanie żądań HTTP. Obsługa formularzy i walidacja danych
W9	Tworzenie API dla aplikacji internetowych
W10	Integracja z bazami danych i zarządzanie danymi. Bazy danych relacyjne i nierelacyjne. Tworzenie i optymalizacja zapytań. Tworzenie aplikacji typu CRUD
W11	Zarządzanie sesją i uwierzytelnianie
W12	Wdrażanie i optymalizacja aplikacji internetowych
W13	Wprowadzenie do bezpieczeństwa aplikacji internetowych
Forma zajęć - laboratoria	
	Treści programowe
L1	Projektowanie i budowa szkieletu aplikacji internetowej. Tworzenie struktury projektu. Przygotowanie podstawowych konfiguracji środowiska pracy
L2	Struktura i tworzenie podstawowego dokumentu HTML. Wprowadzenie do protokołu HTTP. Przechwytywanie i analiza żądań
L3	Tworzenie interfejsu użytkownika aplikacji. Projektowanie struktury aplikacji. Implementacja podstawowych elementów interfejsu użytkownika

L4	Dodawania stylów do interfejsu użytkownika. Wykorzystanie CSS w projektowaniu wizualnym. Dostosowanie aplikacji do różnych urządzeń
L5	Implementacja podstawowych funkcjonalności po stronie klienta. Dodawanie dynamicznych elementów interfejsu. Obsługa zdarzeń użytkownika
L6	Tworzenie podstawowego API po stronie serwera. Przygotowanie serwera aplikacji. Definiowanie punktów końcowych do obsługi podstawowych operacji
L7	Obsługa formularzy i przysyłanie danych na serwer. Walidacja danych po stronie klienta. Przesyłanie danych formularzy do serwera i ich przetwarzanie
L8	Operacje na bazach danych. Połączenie aplikacji z bazą danych. Implementacja operacji dodawania, odczytu, edycji i usuwania danych (CRUD)
L9	Tworzenie systemu uwierzytelniania użytkowników. Rejestracja użytkowników. Logowanie i zarządzanie sesjami
L10	Dodawanie autoryzacji w aplikacji. Ograniczanie dostępu do wybranych zasobów. Weryfikacja uprawnień użytkowników
L11	Realizacja komunikacji pomiędzy klientem a serwerem. Wykorzystanie asynchronicznych żądań do wymiany danych. Obsługa odpowiedzi serwera i aktualizacja interfejsu
L12	Praca nad wydajnością aplikacji internetowej. Optymalizacja zapytań do bazy danych
L13	Dodawanie testów do aplikacji. Implementacja testów jednostkowych dla warstwy serwerowej. Testowanie interfejsu użytkownika
L14	Integracja aplikacji z zewnętrznymi usługami. Korzystanie z API zewnętrznych aplikacji. Pobieranie i przetwarzanie danych z innych systemów
L15	Przygotowanie aplikacji do wdrożenia. Konfiguracja środowiska produkcyjnego

Metody dydaktyczne	
1	wykład informacyjny
2	ćwiczenia laboratoryjne
3	metoda programowania z użyciem komputera

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena wykonanych programów komputerowych	51%
O2	ocena aktywności w trakcie zajęć	51%
O3	ocena pracy pisemnej	51%

Literatura podstawowa	
1	Duckett, Jon i in. HTML i CSS : zaprojektuj i zbuduj witrynę WWW. Gliwice: Helion, 2014.
2	Mikowski, Michael S i in. Single Page Web Applications : programowanie aplikacji internetowych z JavaScript. Gliwice: Wyd. Helion, 2015.
3	Kozieł, Grzegorz i in. Bezpieczne aplikacje internetowe w PHP. Lublin: Wyd. Politechniki Lubelskiej, 2022.

Literatura uzupełniająca	
1	Dickey, Jeff i in. Nowoczesne aplikacje internetowe : MongoDB, Express, AngularJS, Node.js. Gliwice: Helion, 2016.
2	Ater, Tal i in. Progresywne aplikacje webowe : potęga aplikacji natywnych w przeglądarce. Warszawa: APN Promise, 2018.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	75
Udział w wykładach:	30
Udział w zajęciach laboratoryjnych:	45
Praca własna studenta, w tym:	50
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	20
Przygotowanie do zajęć laboratoryjnych:	30
Łączny czas pracy studenta	125
Sumaryczna liczba punktów ECTS dla przedmiotu	5

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W17+++	C1	W1-W11	1	O3
EK 2	CB1A_W06++	C1	W1-W13	1	O3
EK 3	CB1A_W17+++, CB1A_W06++	C3	W11-W13	1	O3
EK 4	CB1A_U17+++, CB1A_U24+++	C1, C2	L1-L15	2,3	O1, O2, O3
EK 5	CB1A_U16+++, CB1A_U17+++, CB1A_U24+++	C3	L9-L15	2,3	O1, O2, O3
EK 6	CB1A_U24+++	C1, C2, C3	L12-L15	2,3	O1, O2, O3
EK 7	CB1A_K05+	C2, C3	W1-W13, L1-L15	1,2,3	O1, O2, O3

Autor programu:	dr inż. Jakub Gęca
Adres e-mail:	j.geca@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Stosowanej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	E-przedsiębiorczość
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C208
Rok:	I
Semestr:	2
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	30
Wykład	30
Ćwiczenia	
Laboratorium	
Projekt	
Liczba punktów ECTS:	2
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zapoznanie z procesem podejmowania własnej działalności gospodarczej oraz podstawowymi zasadami jej organizowania
C2	Pozyskanie wiedzy łączącej e-biznes z tradycyjnymi modelami biznesu
C3	Zrozumienie doboru form prawnych rozwiązań przy prowadzeniu działalności gospodarczej

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Umiejętność korzystania z wyszukiwarek internetowych, literatury oraz innych źródeł informacji
2	Umiejętność logicznego i kreatywnego myślenia

Efekty uczenia się	
	W zakresie wiedzy:
EK1	zna i rozumie przepisy prawne, normy oraz standardy dotyczące działalności przedsiębiorstw w środowisku cyfrowym, w tym dotyczące bezpieczeństwa w działalności e-biznesowej
EK2	zna i rozumie podstawowe zasady tworzenia i rozwoju przedsiębiorczości indywidualnej, jak i organizacyjnej
EK3	posiada wiedzę na temat e-przedsiębiorczości w praktyce działań biznesowych i społecznych oraz rozumie mechanizmy funkcjonowania rynku tradycyjnego i cyfrowego
	W zakresie kompetencji społecznych:
EK4	jest gotów do myślenia i działania w sposób przedsiębiorczy, zarówno samodzielnie, jak i w ramach grupy

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Pojęcie przedsiębiorczości; typy przedsiębiorczości i organizacji przedsiębiorczych, cechy osoby przedsiębiorczej oraz przedsiębiorcza orientacja. Specyfika przedsiębiorczego zarządzania w przestrzeni cyfrowej.
W2	Przedsiębiorczość tradycyjna a e-przedsiębiorczość. Istota e-przedsiębiorczości w praktyce działań biznesowych i społecznych - E-przedsiębiorczość indywidualna, korporacyjna i społeczna
W3	Rynek tradycyjny a rynek przestrzeni cyfrowej - Podejście platformowe jako model organizacji rynku
W4	Modele e-biznesu – definiowanie, główne składowe, kreowanie modeli biznesowych
W5	Nowe kierunki rozwoju modeli e-biznesu
W6	Działalność marketingowa w przestrzeni cyfrowej. Content marketing
W7	Planowanie finansowe w e-przedsiębiorstwie
W8	Od pomysłu do sukcesu finansowego przedsiębiorstwa
W9	Podatki w e-działalności gospodarczej. Stosunek pracy w e-przedsiębiorstwie
W10	Innowacje w e-przedsiębiorczości. Parki technologiczne i inne centra innowacji
W11	Crowdsourcing jako narzędzie wsparcia e-przedsiębiorczości
W12	Bezpieczeństwo przedsiębiorstw w przestrzeni cyfrowej - Charakterystyka wybranych zagrożeń – Phishing – Złośliwe oprogramowanie
W13	Cyberzagrożenia w kontekście wybranych nowych technologii

Metody dydaktyczne	
1	Wykład konwersatoryjny
2	Wykład problemowy
3	Wykład informacyjny

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	Ocena pracy pisemnej	51%

Literatura podstawowa	
1	Bednarczyk, Małgorzata, i in. E-przedsiębiorczość : zasady i praktyka. Wyd. Uniwersytetu Jagiellońskiego, 2019.
2	Tracy, Brian, i in. Przedsiębiorczość : jak założyć i rozwijać własną firmę. Helion, 2021.
3	Majkut, Robert, i CeDeWu. Wydawca. Przedsiębiorca wobec współczesnych uwarunkowań i czynników przedsiębiorczości. Wydanie I., CeDeWu, 2021.
4	Kaczorowska-Spychalska, Dominika, i Gregor, Bogdan . Technologie cyfrowe w biznesie: Przedsiębiorstwa 4.0 a sztuczna inteligencja. Wyd. Naukowe PWN, 2020.

Literatura uzupełniająca	
1	Hoffmann, Tomasz, i in. Wybrane aspekty cyberbezpieczeństwa w Polsce. FNCE, 2018.
2	Gwoździwicz, Sylwia, et al. Legal and Social Aspects of Cybersecurity. Difin, 2020.
3	ŚledziwskA_Kołodziejska, Katarzyna, i in. Gospodarka cyfrowa : jak nowe technologie zmieniają świat. Wydanie 1., Wyd. Uniwersytetu Warszawskiego, 2020.
4	Zieliński, Kazimierz, i Difin. Wydawca. Przedsiębiorczość a nowe technologie. Wydanie pierwsze., Difin, 2019.
5	Małecka-Ziemińska, Edyta. Podatki w ujęciu retrospektywnym i perspektywicznym. Poznań University of Economics and Business Press, 2022.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	30
Udział w wykładach:	30
Praca własna studenta, w tym:	20
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	20
Łączny czas pracy studenta	50
Sumaryczna liczba punktów ECTS dla przedmiotu	2

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W08+++ CB1A_W13+	C1, C3	W1-W13	1, 2, 3	O1
EK 2	CB1A_W08+++	C1, C2, C3	W1, W4, W6-W11	1, 2, 3	O1
EK 3	CB1A_W08+++	C1, C2	W2 - W5, W8 - W11	1, 2, 3	O1
EK 4	CB1A_K04+++	C1, C3	W8, W11	1, 2, 3	O1

Autor programu:	dr hab. Agnieszka Rzepka, profesor uczelni; dr Magdalena Czerwińska
Adres e-mail:	a.rzepka@pollub.pl; m.czerwinska@pollub.pl
Jednostka organizacyjna:	Katedra Ekonomii, Innowacji i Kapitału Społecznego

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Wprowadzenie do statystyki
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C301
Rok:	II
Semestr:	3
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	45
Wykład	15
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	3
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zdobycie wiedzy z zakresu podstaw statystyki matematycznej oraz wskazanie kontekstu zastosowań w naukach technicznych
C2	Wykształcenie umiejętności matematycznego opisu zmienności losowej procesów, w tym opracowania i prezentacji wyników obserwacji

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Wiadomości z zakresu kursu analizy matematycznej i algebry

Efekty uczenia się	
	W zakresie wiedzy:
EK 1	zna podstawowe pojęcia statystyki matematycznej
EK 2	zna kontekst zastosowań metod statystyki matematycznej
	W zakresie umiejętności:
EK3	stosuje metody statystyczne do opisu zmienności losowej procesów
EK4	opracowuje i interpretuje wyniki pomiarów obserwowanej wielkości
EK5	opracowuje wyniki doświadczenia porównawczego z zastosowaniem metod statystycznych
	W zakresie kompetencji społecznych:
EK6	jest gotów do krytycznej oceny posiadanej wiedzy oraz odbieranych treści związanych z bezpieczeństwem cyfrowym

Treści programowe przedmiotu
Forma zajęć - wykłady

Treści programowe	
W1	Podstawowe pojęcia statystyki matematycznej. Elementy statystyki opisowej. Rozkład empiryczny obserwacji i jego charakterystyka (szereg rozdzielczy)
W2	Podstawowe rozkłady prawdopodobieństwa i ich zastosowania
W3	Estymacja punktowa i przedziałowa. Zagadnienie opisu błędu pomiaru
W4	Procedura weryfikacji hipotez statystycznych. Testy parametryczne
W5	Testy nieparametryczne. Test zgodności dopasowania rozkładów
W6	Model regresji prostej i jego opracowanie
W7	Planowanie, realizacja i opracowanie doświadczeń wieloczynnikowych prowadzących do modeli regresji wielorakiej
Forma zajęć - laboratoria	
Treści programowe	
L1	Wprowadzenie do środowiska obliczeniowego/numerycznego
L2	Podstawowe metody prezentacji wyników obserwacji
L3	Statystyki opisowe i ich zastosowania
L4	Charakterystyka zbioru obserwacji z wykorzystaniem szeregu rozdzielczego
L5	Metody oceny zgodności dopasowania obserwacji do postulowanego rozkładu prawdopodobieństwa
L6	Właściwości i zastosowania rozkładu normalnego. Błąd pomiaru
L7	Doświadczenia porównawcze dla prób zależnych i niezależnych
L8	Zastosowania testów statystycznych w procedurze statystycznego sterowania procesem: etapy konstrukcji, wdrożenia i interpretacji kart kontrolnych
L9	Model regresji prostej. Doświadczenie jednoczynnikowe
L10	Model regresji wielorakiej. Planowanie i analiza wyników doświadczeń wieloczynnikowych

Metody dydaktyczne	
1	wykład problemowy
2	ćwiczenia laboratoryjne

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena odpowiedzi ustnej	51%
O2	ocena wykonanych ćwiczeń laboratoryjnych	51%

Literatura podstawowa	
1	Wasilewska Ewa, Statystyka matematyczna w praktyce, Difin, 2015.
2	Taylor John, Wstęp do analizy błędu pomiarowego, Wyd. Naukowe PWN, 1999.
3	Box George, Stuart Hunter, William Hunter, Statistics for experimenters : design, innovation, and discovery, Wiley & Sons, 2005.

Literatura uzupełniająca	
1	Montgomery Douglas, Modern Introduction to Statistical Process Control, Wiley & Sons, 2009.
2	Montgomery Douglas, Design and Analysis of Experiments, Wiley & Sons, 2005.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	45
Udział w wykładach:	15
Udział w zajęciach laboratoryjnych:	30
Praca własna studenta, w tym:	30
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	10
Przygotowanie do zajęć laboratoryjnych:	20
Łączny czas pracy studenta	75
Sumaryczna liczba punktów ECTS dla przedmiotu	3

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W01+++	C1	W1-W7	1	O1,O2
EK 2	CB1A_W01+++	C1	W1-W7	1	O1,O2
EK 3	CB1A_U15++	C2	L1-L10	2	O3
EK 4	CB1A_U14+++	C2	L1-L10	2	O2,O3
EK 5	CB1A_U14+++ CB1A_U12++	C2	L1-L10	2	O2,O3
EK 6	CB1A_K01+	C1, C2	W1-W7, L1-L10	1, 2	O1-O3

Autor programu:	dr Marcin Bogucki; dr Maciej Czarnacki
Adres e-mail:	m.bogucki@pollub.pl; m.czarnacki@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Technicznej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Zaawansowane sieci komputerowe
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C302
Rok:	II
Semestr:	3
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	45
Wykład	15
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	3
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zrozumienie zasad przełączania i routingu w sieci komputerowej
C2	Rozwój umiejętności projektowania i konfiguracji sieci nadmiarowych oraz zapewnienia wysokiej dostępności
C3	Bezpieczne zarządzanie siecią lokalną i implementacja najlepszych praktyk ochrony

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Podstawowa znajomość sieci komputerowych

Efekty uczenia się	
	W zakresie wiedzy:
EK 1	zna podstawowe koncepcje przełączania w sieciach komputerowych, w tym różnice między przełączaniem warstwy 2 i 3 oraz zasadami działania mostów, przełączników i routerów
EK 2	potrafi wyjaśnić strukturę i zastosowanie sieci VLAN (Virtual Local Area Network) oraz zna zasady konfiguracji i routingu pomiędzy VLAN-ami
EK3	objaśnia sieci nadmiarowe, technologie zapewniające wysoką dostępność i niezawodność
	W zakresie umiejętności:
EK4	potrafi zaprojektować i skonfigurować przełączanie warstwy 2 i 3 w sieci, w tym tworzenie VLAN-ów, przypisywanie portów i konfigurację trunków
EK5	potrafi skonfigurować i zarządzać routingiem pomiędzy VLAN-ami, implementując protokoły routingu statycznego i dynamicznego

EK6	potrafi zaplanować i wdrożyć sieć nadmiarową, zapewniając wysoką dostępność usług oraz konfigurację przełączników w celu uniknięcia pętli w sieci
	W zakresie kompetencji społecznych:
EK7	jest gotów uwzględniać znaczenie wysokiej dostępności i niezawodności sieci w organizacjach oraz podejmować decyzje projektowe z uwzględnieniem zarówno potrzeb biznesowych, jak i technologicznych, dążąc do zapewnienia ciągłości działania i efektywności systemów sieciowych

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Klasyfikacja routingu dynamicznego. Routing wektora odległości, wektora ścieżki i stanu łącza. Protokoły BGP i OSPF.
W2	Zagadnienia zaawansowanych technik ochrony sieci na poziomie dostępu, dystrybucji i rdzenia sieci.
W3	Koncepcje sieci rozległej. Technologia i protokoły wykorzystywane w realizacji komunikacji rozległej. Sieci SD-WAN.
W4	Zaawansowane techniki monitorowania sieci. Wykrywanie i usuwanie błędów w projektach i konfiguracjach sieci.
W5	Rozwiązania wysokiej dostępności. Nadmiarowość infrastruktury. Technologie wysokodostępnej sieci lokalnej. Protokoły FHRP.
Forma zajęć - laboratoria	
	Treści programowe
L1	Planowanie zaawansowanego routingu dynamicznego. Implementacja w sieci routingu OSPF.
L2	Projektowanie i wdrażanie zabezpieczenia sieci na poziomie warstw 1-4. Testowanie pod kątem wykrywania podatności rozwiązań sieciowych.
L3	Konfiguracja rozwiązań sieci rozległych. Testowanie i monitorowanie komunikacji rozległej. Zaawansowane rozwiązania VPN i IPSec.
L4	Wdrażanie mechanizmów QoS. Monitorowanie Network Transmission Quality.
L5	Rozwiązania SDN i wirtualizacja sieci. Zaawansowane zagadnienia projektowania.
L6	Wdrażanie konfiguracji FHRP. Konfiguracja VRRP. Routingi z równoważeniem obciążenia równo- i różnokosztowym.

Metody dydaktyczne	
1	wykład informacyjny
2	ćwiczenia laboratoryjne

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena wykonanych ćwiczeń laboratoryjnych	51%

Literatura podstawowa	
1	Materiały na platformie Netacad: CCNAv7: Switching, Routing, and Wireless Essentials.
2	Józefiok, Adam, i in. CCNA 200-125 : zostań administratorem sieci komputerowych Cisco. Helion, 2018.

Literatura uzupełniająca	
1	White, Russ, i in. Sieci komputerowe : najczęstsze problemy i ich rozwiązania : innowacyjne podejście do budowania odpornych, nowoczesnych sieci. Helion, 2019.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	45
Udział w wykładach:	15
Udział w zajęciach laboratoryjnych:	30
Praca własna studenta, w tym:	30
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	10
Przygotowanie do zajęć laboratoryjnych:	20
Łączny czas pracy studenta	75
Sumaryczna liczba punktów ECTS dla przedmiotu	3

Macierz efektów uczenia się					
Symbol przedmiotowe go efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W03++ CB1A_W09+++	C1	W1, W2	1	O1
EK 2	CB1A_W03++ CB1A_W09+++	C1, C3	W3	1	O1
EK 3	CB1A_W09++	C2, C3	W4, W5	1	O1
EK 4	CB1A_U16+++ CB1A_U21++	C1, C3	L1, L2, L4	2	O2
EK 5	CB1A_U16+++ CB1A_U21++ CB1A_U10+++	C1, C3	L6	2	O2

EK 6	CB1A_U16+++ CB1A_U21++	C1, C2	L5, L6	2	O2
EK 7	CB1A_K04+	C1	L1-L76	2	O1, O2

Autor programu:	dr Rafał Stęgiński
Adres e-mail:	r.stegierski@pollub.pl
Jednostka organizacyjna:	Katedra Inteligencji Obliczeniowej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Podstawy kryptografii kwantowej
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C303
Rok:	II
Semestr:	3
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	30
Wykład	15
Ćwiczenia	
Laboratorium	15
Projekt	
Liczba punktów ECTS:	2
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu

C1	Zapoznanie z podstawowymi koncepcjami kryptografii kwantowej
C2	Zdobycie praktycznych umiejętności dotyczących wykonywania operacji na kubitach i ich użycie w kryptografii

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1	Podstawowe zagadnienia z obszaru algebry
2	Podstawowe zagadnienia z kryptografii
3	Ogólne umiejętności programistyczne

Efekty uczenia się

	W zakresie wiedzy:
EK 1	definiuje podstawowe pojęcia kryptografii kwantowej i stojące za nimi zagadnienia fizyki kwantowej
EK 2	zna podstawowe algorytmy stosowane w kryptografii kwantowej
	W zakresie umiejętności:
EK3	potrafi zaimplementować podstawowe operacje wykonywane na bramkach bitowych
EK4	korzysta z dostępnych bibliotek do symulowania działania algorytmów kryptografii kwantowej
	W zakresie kompetencji społecznych:
EK5	jest gotów do uznawania znaczenia wiedzy z zakresu kryptografii w rozwiązywaniu problemów związanych z ochroną danych

Treści programowe przedmiotu

Forma zajęć - wykłady	
	Treści programowe
W1	Wprowadzenie do kryptografii kwantowej
W2	Kubity i wykonywanie na nich operacje
W3	Kwantowa dystrybucja klucza
W4	Kryptografia oparta na splątaniu kwantowym i protokół E91
W5	Algorytm faktoryzacji Shora
W6	Algorytm Grovera i przeszukiwanie kwantowe
W7	Kryptografia postkwantowa
Forma zajęć - laboratoria	
	Treści programowe
L1	Wprowadzenie do programowania kwantowego: implementacja prostych bramek kwantowych
L2	Symulacja protokołu BB84 do dystrybucji klucza kwantowego
L3	Symulacja splątania kwantowego i protokołu E91
L4	Implementacja algorytmu Shora do faktoryzacji liczby
L5	Przeszukiwanie za pomocą algorytmu Grovera
L6	Symulacja korekcji błędów kwantowych
L7	Kryptografia postkwantowa: symulacja ataku kwantowego na szyfr RSA

Metody dydaktyczne	
1	wykład informacyjny
2	ćwiczenia laboratoryjne

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena wykonanych ćwiczeń laboratoryjnych	51%

Literatura podstawowa	
1	Jacak, Monika, i in. Wprowadzenie do kryptografii kwantowej : implementacja protokołów kryptografii kwantowej na systemach niesplątanych fotonów (system Clavis II) i splątanych fotonów (system EPR S405 Quelle). Oficyna Wydawnicza Politechniki Wrocławskiej, 2013.
2	Białas, Andrzej. Klasyczne i kwantowe metody podniesienia bezpieczeństwa informacji w systemach komputerowych. Dąbrowa Górnicza: Wyższa Szkoła Biznesu, 2010.

Literatura uzupełniająca	
1	Grzywak, Andrzej i in. Współczesne problemy bezpieczeństwa informacji. Dąbrowa Górnicza: Wyższa Szkoła Biznesu, 2008.

Obciążenie pracą studenta

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	30
Udział w wykładach:	15
Udział w zajęciach laboratoryjnych:	15
Praca własna studenta, w tym:	20
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	10
Przygotowanie do zajęć laboratoryjnych:	10
Łączny czas pracy studenta	50
Sumaryczna liczba punktów ECTS dla przedmiotu	2

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W01++ CB1A_W07++	C1	W1 - W7	1	O1
EK 2	CB1A_W07++	C1	W1 - W7	1	O1
EK 3	CB1A_U19++ CB1A_U15+++	C2	L1 - L7	2	O2
EK 4	CB1A_U19++ CB1A_U15+++	C2	L1 - L7	2	O2
EK 5	CB1A_K02+	C1, C2	W1 - W7 L1 - L7	1, 2	O1, O2

Autor programu:	dr Michał Dolecki
Adres e-mail:	m.dolecki@pollub.pl
Jednostka organizacyjna:	Katedra Inteligencji Obliczeniowej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Bezpieczeństwo systemów operacyjnych
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C304
Rok:	II
Semestr:	3
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	60
Wykład	30
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	4
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zapoznanie z wektorami ataku w systemach operacyjnych oraz metodami ich minimalizowania
C2	Nabywanie umiejętności hartowania systemu i zarządzania usługami
C3	Przedstawienie technik monitorowania systemu operacyjnego, wykrywania i reagowania na zagrożenia, jak również przywracania systemu i danych po incydentach

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Podstawy znajomości systemów operacyjnych
2	Podstawowa wiedza z zakresu sieci komputerowych
3	Umiejętność programowania

Efekty uczenia się	
	W zakresie wiedzy:
EK 1	rozpoznaje zagrożenia, na które mogą być podatne systemy operacyjne
EK 2	objaśnia zasady i działania związane z zabezpieczeniem systemu operacyjnego, mające na celu minimalizację liczby wektorów ataku, a także przeprowadzanie audytów bezpieczeństwa oraz monitorowanie stanu systemu w celu ochrony przed potencjalnymi zagrożeniami
	W zakresie umiejętności:
EK3	stosuje praktyki i zasady minimalizujące obszar potencjalnych ataków

EK4	dobiera narzędzia w celach monitorowania systemu operacyjnego związane z analizą logów, konfiguracją zapór sieciowych i przywraca jego funkcjonalność po incydentach
	W zakresie kompetencji społecznych:
EK5	jest gotów do przestrzegania zasad etyki zawodowej oraz wykorzystania swojej wiedzy do poprawy bezpieczeństwa systemów informatycznych w swoim otoczeniu i rozumie konsekwencje prawne wynikające z nieuprawnionego naruszania cudzych danych i infrastruktury

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Wprowadzenie do bezpieczeństwa systemów operacyjnych, podstawowe pojęcia i zasady bezpieczeństwa systemów operacyjnych
W2	Ustawienia uprawnień plików i użytkowników, zasady zarządzania użytkownikami i grupami, konfiguracja ról i uprawnień
W3	Zabezpieczenie usług systemowych, konfiguracja uprawnień i zabezpieczenia rejestru, zarządzanie aktualizacjami
W4	Utwardzanie jądra i systemu operacyjnego. Ochrona przed nieautoryzowanym dostępem do jądra systemu. Wyłączenie niepotrzebnych modułów i funkcji systemowych. Wdrożenie polityk ograniczających dostęp do przestrzeni systemowej i interfejsów debugowania
W5	Zaawansowane modele kontroli dostępu w systemach operacyjnych. Implementacja polityk bezpieczeństwa opartych na różnych modelach kontroli dostępu, kontrola interakcji między procesami i zasobami systemowymi
W6	Wykrywanie i reakcja na incydenty bezpieczeństwa, analiza logów systemowych i detekcja naruszeń bezpieczeństwa, narzędzia do monitorowania systemów operacyjnych
W7	Bezpieczeństwo aplikacji w systemach operacyjnych, monitorowanie procesów i ich zachowania
W8	Audyt i testy penetracyjne systemów operacyjnych
W9	Bezpieczeństwo sieci w systemach operacyjnych, ochrona przed atakami sieciowymi, konfiguracja zapór sieciowych, konfiguracja protokołów bezpiecznego przesyłania danych
W10	Przywracanie systemu po ataku, rodzaje kopii zapasowych, tworzenie i przywracanie kopii zapasowych, reakcja na ransomware i inne poważne zagrożenia
Forma zajęć - laboratoria	
	Treści programowe
L1	Podstawowa konfiguracja bezpieczeństwa w systemach, zarządzanie użytkownikami, ustawienia uprawnień plików
L2	Zabezpieczenie usług systemowych, blokowanie nieużywanych usług i portów
L3	Ochrona przed złośliwym oprogramowaniem, wykorzystanie oprogramowania antywirusowego i antimalware

L4	Utwardzanie systemu operacyjnego: wyłączenie niepotrzebnych modułów i funkcji, implementacja polityk ograniczających dostęp
L5	Bezpieczeństwo aplikacji: monitorowanie procesów, wykrywanie nieautoryzowanych operacji, narzędzia do analizy aplikacji
L6	Monitorowanie i analiza logów systemowych: narzędzia i techniki, analiza incydentów
L7	Audyt bezpieczeństwa w systemach operacyjnych
L8	Testy penetracyjne, symulacja ataków na system, scenariusze ochrony przed różnego typu atakami, wdrażanie mechanizmów obronnych
L9	Zaawansowana konfiguracja zapór sieciowych: tworzenie reguł, filtrowanie ruchu, ochrona przed atakami sieciowymi
L10	Tworzenie kopii zapasowych i przywracanie systemu, strategie backupu, testowanie przywracania po incydentach

Metody dydaktyczne	
1	wykład informacyjny
2	ćwiczenia laboratoryjne

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena wykonanych ćwiczeń laboratoryjnych	51%

Literatura podstawowa	
1	Bravo C., i in.: Cyberbezpieczeństwo dla zaawansowanych : skuteczne zabezpieczenia systemu Windows, Linux, IoT i infrastruktury w chmurze. Gliwice: Helion, 2023. Print.
2	Binnie Ch., i in.: Linux Server : bezpieczeństwo i ochrona sieci. Gliwice: Wyd. Helion, 2017. Print.
3	Kalsi T., i in.: Bezpieczeństwo systemu Linux w praktyce : receptury. Gliwice: Helion, 2019. Print.

Literatura uzupełniająca	
1	Andress J.: The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. 2nd ed. Chantilly: Elsevier Science & Technology Books, 2014. Print.
2	Barrett D. J., i in.: Linux : bezpieczeństwo, receptury. Gliwice: Helion, 2003. Print.
3	Kovachich G. L.: The Information Systems Security Officer's Guide : Establishing and Managing an Information Protection Program. 2nd ed. Amsterdam ; Butterworth-Heinemann, 2003. Print.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności

Godziny kontaktowe z wykładowcą, w tym:	60
Udział w wykładach:	30
Udział w zajęciach laboratoryjnych:	30
Praca własna studenta, w tym:	40
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	20
Przygotowanie do zajęć laboratoryjnych:	20
Łączny czas pracy studenta	100
Sumaryczna liczba punktów ECTS dla przedmiotu	4

Macierz efektów uczenia się					
Symbol przedmiotowe go efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W12+++ CB1A_W15++	C1	W1 - W10	1	O1
EK 2	CB1A_W12+++ CB1A_W14+ CB1A_W15++	C1, C2, C3	W1 - W10	1	O1
EK 3	CB1A_U10+++ CB1A_U18+++	C1, C2	L1 - L10	2	O2
EK 4	CB1A_U10+++ CB1A_U18+++ CB1A_U21++	C1, C3	L1 - L10	2	O2
Ek 5	CB1A_K05+	C1, C2, C3	W1 - W10 L1 - L10	1, 2	O1, O2

Autor programu:	dr hab. Paweł Karczmarek, profesor uczelni; dr Rafał Stęgiński; mgr inż. Albert Rachwał; dr inż. Łukasz Gałka
Adres e-mail:	p.karczmarek@pollub.pl; r.stegierski@pollub.pl; a.rachwal@pollub.pl; l.galka@pollub.pl
Jednostka organizacyjna:	Katedra Inteligencji Obliczeniowej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Teoria informacji i kodowania
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C305
Rok:	II
Semestr:	3
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	60
Wykład	30
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	4
Sposób zaliczenia:	egzamin
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zapoznanie z podstawowymi pojęciami teorii informacji oraz różnymi metodami kodowania i algorytmami kompresji danych
C2	Opanowanie umiejętności zastosowania technik kodowania i kompresji danych w praktycznych zastosowaniach

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Znajomość podstaw programowania
2	Umiejętność pracy z dokumentacją techniczną
3	Podstawy matematyki dyskretniej

Efekty uczenia się	
	W zakresie wiedzy:
EK 1	rozróżnia podstawowe pojęcia teorii informacji i kodowania
EK 2	wskazuje różnice między kodowaniem bezstratnym i stratnym oraz ich zastosowaniem
	W zakresie umiejętności:
EK3	stosuje algorytmy kodowania i kompresji danych w praktycznych zastosowaniach, również z wykorzystaniem metod sztucznej inteligencji
EK4	analizuje skuteczność różnych algorytmów kodowania i korekcji błędów
	W zakresie kompetencji społecznych:
EK5	jest gotów do ciągłego doskonalenia wiedzy w związku z rozwojem technologii informacyjnych

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Podstawowe pojęcia teorii informacji i kodowania
W2	Zapis cyfrowy informacji
W3	Klasyfikacja kodów
W4	Przegląd algorytmów kompresji danych
W5	Opis kodów liniowych oraz kodów cyklicznych
W6	Wprowadzenie do kodów splotowych
W7	Metody korekcji błędów
W8	Techniki kodowania i kompresji tekstu
W9	Kompresja obrazów i dźwięku
W10	Zastosowanie sztucznej inteligencji do kompresji danych
Forma zajęć - laboratoria	
	Treści programowe
L1	Obliczanie entropii i pojemności kanału
L2	Digitalizacja sygnałów analogowych
L3	Implementacja bezstratnych metod kodowania
L4	Analiza stratnych metod kodowania
L5	Algorytmy kompresji danych
L6	Kody liniowe i cykliczne
L7	Kodowanie i dekodowanie splotowe
L8	Kody korekcyjne
L9	Kodowanie i kompresja tekstu, obrazu, dźwięku oraz wideo
L10	Wykorzystanie sztucznej inteligencji do kompresji danych

Metody dydaktyczne	
1	wykład informacyjny
2	dyskusja dydaktyczna
3	praca wykonywana indywidualnie
4	ćwiczenia laboratoryjne

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena wykonanych ćwiczeń laboratoryjnych	51%
O3	ocena aktywności w trakcie zajęć	51%

Literatura podstawowa

1	Kuriata, Eugeniusz. Teoria informacji i kodowania. Oficyna Wydawnicza Politechniki Zielonogórskiej, 2001.
2	Drozdek, Adam. Wprowadzenie do kompresji danych. Wydanie II., Wydawnictwa Naukowo-Techniczne, 2007.
3	Przelaskowski, Artur. Kompresja danych : podstawy, metody bezstratne, kodery obrazów. Wyd. BTC, 2005.

Literatura uzupełniająca	
1	Mazur, Marian. Jakościowa teoria informacji. Wydawnictwa Naukowo-Techniczne, 1970.
2	Abramson, Norman, i in. Teoria informacji i kodowania. Państwowe Wyd. Naukowe, 1969.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	60
Udział w wykładach:	30
Udział w zajęciach laboratoryjnych:	30
Praca własna studenta, w tym:	40
Studiowanie tematyki wykładów, przygotowanie do egzaminu:	25
Przygotowanie do zajęć laboratoryjnych:	15
Łączny czas pracy studenta	100
Sumaryczna liczba punktów ECTS dla przedmiotu	4

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W01++	C1	W1-W10	1, 2	O1
EK 2	CB1A_W07+++	C1	W1-W10	1, 2	O1
EK 3	CB1A_U19++ CB1A_U15+++ CB1A_U22++	C2	L1-L10	3, 4	O2, O3
EK 4	CB1A_U13++	C2	L1-L10	3, 4	O2, O3
EK 5	CB1A_K01+	C1	W1-W10	1, 2	O1

Autor programu:	dr hab. Paweł Karczmarek, profesor uczelni; dr inż. Łukasz Gałka
------------------------	--

Adres e-mail:	p.karczmarek@pollub.pl; l.galka@pollub.pl
Jednostka organizacyjna:	Katedra Inteligencji Obliczeniowej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Tworzenie aplikacji mobilnych
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C306.1
Rok:	II
Semestr:	3
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	60
Wykład	30
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	4
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zapoznanie z podstawowymi zasadami tworzenia aplikacji mobilnych, w tym projektowania interfejsów użytkownika i zarządzania cyklem życia aplikacji
C2	Zaznajomienie z technologiami i standardami wykorzystywanymi w aplikacjach mobilnych
C3	Zaznajomienie z technologiami i standardami wykorzystywanymi w aplikacjach mobilnych

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Znajomość programowanie obiektowego
2	Znajomość algorytmów i struktur danych
3	Podstawowa znajomość baz danych oraz sieci komputerowych

Efekty uczenia się	
	W zakresie wiedzy:
EK 1	wyjaśnia cykl życia aplikacji mobilnej oraz opisuje architekturę aplikacji mobilnych
EK 2	charakteryzuje metody integracji aplikacji z zewnętrznymi usługami oraz sposoby zarządzania danymi w aplikacjach mobilnych
	W zakresie umiejętności:
EK3	projektuje i implementuje interfejs użytkownika zgodny z wytycznymi dla platform mobilnych
EK4	optymalizuje wydajność aplikacji mobilnych, w tym zarządza zasobami i implementuje przetwarzanie wielowątkowe
	W zakresie kompetencji społecznych:

EK5	jest gotów do odpowiedzialnej realizacji zadań związanych z projektowaniem i wdrażaniem aplikacji mobilnych
------------	---

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Historia i rozwój platform mobilnych
W2	Rodzaje aplikacji mobilnych: natywne, hybrydowe, webowe, progresywne (PWA)
W3	Podstawy projektowania aplikacji mobilnych
W4	Projektowanie zorientowane na użytkownika (UI/UX)
W5	Wzorce projektowe w aplikacjach mobilnych (np. Model-View-Controller, MVVM)
W6	Bazy danych i przechowywanie danych w aplikacjach mobilnych
W7	Przechowywanie lokalne, SQLite, Room Database
W8	Integracja z zewnętrznymi bazami danych: Firebase, Supabase, MongoDB
W9	Komunikacja sieciowa w aplikacjach mobilnych i synchronizacja danych i obsługa trybu offline
W10	Zarządzanie stanem aplikacji
W11	Multimedia i funkcje urządzeń mobilnych
W12	Testowanie aplikacji mobilnych i publikowanie aplikacji mobilnych
W13	Trendy i przyszłość aplikacji mobilnych
Forma zajęć - laboratoria	
	Treści programowe
L1	Wprowadzenie do platform mobilnych i środowisk programistycznych
L2	Projektowanie interfejsów użytkownika (UI) dla urządzeń mobilnych
L3	Cykl życia aplikacji mobilnej
L4	Architektura aplikacji mobilnych
L5	Integracja z API i zewnętrznymi usługami
L6	Zarządzanie danymi w aplikacjach mobilnych
L7	Obsługa powiadomień push – integracja powiadomień, zarządzanie uprawnieniami użytkownika
L8	Optymalizacja wydajności – zarządzanie zasobami, przetwarzanie wielowątkowe, minimalizowanie zużycia pamięci
L9	Testowanie aplikacji mobilnych
L10	Wprowadzenie do zdalnej komunikacji

Metody dydaktyczne	
1	wykład informacyjny
2	ćwiczenia laboratoryjne

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy

O1	ocena pracy pisemnej	51%
O2	ocena wykonanych programów komputerowych	51%

Literatura podstawowa		
1	Płonkowski M.: Android Studio : tworzenie aplikacji mobilnych. Gliwice: Helion, 2018. Print.	
2	Eisenman B., i in.: React Native : tworzenie aplikacji mobilnych w języku JavaScript. Gliwice: Helion, 2018. Print.	
3	Lacey M., i i.n.: Postaw na użyteczność : UX dla programistów i projektantów na przykładzie aplikacji mobilnych. Wydanie I. Warszawa: PWN, 2019. Print.	

Literatura uzupełniająca		
1	Rzecki K.: Zagadnienia programowania aplikacji mobilnych i systemów wbudowanych : praca zbiorowa. Kraków: Wyd. PK, 2016. Print.	
2	Verma P. K., i in.: Bezpieczeństwo urządzeń mobilnych : receptury. Gliwice: Wyd. Helion, 2017. Print.	
3	Żółkiewska S., i in.: Biznes w świecie mobile : jak zaprojektować, wykonać i wypromować aplikację mobilną. Warszawa: Poltext, 2018. Print.	

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	60
Udział w wykładach:	30
Udział w zajęciach laboratoryjnych:	30
Praca własna studenta, w tym:	40
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	20
Przygotowanie do zajęć laboratoryjnych:	20
Łączny czas pracy studenta	100
Sumaryczna liczba punktów ECTS dla przedmiotu	4

Macierz efektów uczenia się					
Symbol przedmiotowe go efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W17+++	C1, C2, C3	W1 - W15	1	O1

	CB1A_W06++ CB1A_W10++				
EK 2	CB1A_W17+++ CB1A_W06++	C1, C2, C3	W1 - W15	1	O1
EK 3	CB1A_U17+++ CB1A_U24++	C1, C2, C3	L1 - L10	2	O2
EK 4	CB1A_U17+++ CB1A_U24++	C1, C2, C3	L1 - L10	2	O2
EK 5	CB1A_K05+	C1, C2, C3	W1 - W15 L1 - L10	1, 2	O1, O2

Autor programu:	dr Rafał Stęgiński; mgr inż. Albert Rachwał
Adres e-mail:	r.stegierski@pollub.pl; a.rachwal@pollub.pl
Jednostka organizacyjna:	Katedra Inteligencji Obliczeniowej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Programowanie przemysłowych urządzeń HMI
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C306.2
Rok:	II
Semestr:	3
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	60
Wykład	30
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	4
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Przekazanie wiedzy na temat konstrukcji i sposobu działania przemysłowych urządzeń operatorskich i serwisowych typu HMI (Human-Machine Interface) oraz rozwiązań wykorzystujących uniwersalne urządzenia do prezentacji danych (komputery, tablety)
C2	Nabywanie umiejętności konfigurowania i programowania urządzeń HMI do pracy w sieciach przemysłowych z uwzględnieniem zagadnień bezpieczeństwa procesu technologicznego i przesyłu danych
C3	Nabywanie umiejętności projektowania struktury praw dostępu oraz procedur awaryjnych

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Podstawowa wiedza z zakresu sieci komputerowych i programowania aplikacji internetowych

Efekty uczenia się	
	W zakresie wiedzy:
EK 1	zna zasady tworzenia interfejsów użytkownika przeznaczonych do pracy w systemach przemysłowych, w tym zasady bezpieczeństwa pracy urządzeń operatorskich włączonych do sieci przemysłowych i korzystających z rozproszonych baz danych
EK 2	opisuje wymagania stawiane rozproszonym systemom sterowania pracującym w sieciach przemysłowych oraz mechanizmy przetwarzania i przesyłu informacji w urządzeniach sieciowych
	W zakresie umiejętności:

EK3	projektuje i wykonuje oprogramowanie na urządzenia interfejsu użytkownika typowe dla środowiska przemysłowego, uwzględniając podstawowe zasady bezpieczeństwa oraz ochrony danych
EK4	opracowuje zasady dostępu do danych oraz procedury sterujące dla przemysłowych systemów interfejsu operatora (HMI) uwzględniając problemy związane z dostępem równoległym z kilku urządzeń, utratą urządzenia, zerwaniem połączenia sieciowego i innymi sytuacjami awaryjnymi
	W zakresie kompetencji społecznych:
EK5	jest gotów do krytycznej oceny i dbałości o jakość proponowanych rozwiązań przyczyniając się do utrwalenia dobrego wizerunku inżyniera

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Interfejsy użytkownika - klasyfikacja, zastosowania, przykładowe rozwiązania, historia rozwoju interfejsów przemysłowych
W2	Interfejs człowiek-maszyna (HMI) - podstawowe funkcje, urządzenia przemysłowe, współczesne rozwiązania systemów HMI, narzędzia do projektowania
W3	Zasady tworzenia oprogramowania na przemysłowe systemy HMI - funkcjonalność, struktura aplikacji, ergonomia interfejsu i aplikacji
W4	Podstawy bezpieczeństwa procesów przemysłowych - zasada fail-safe, priorytety, przesył i prezentacja danych, opóźnienie czasowe, stany awaryjne
W5	Podział kompetencji i wielodostęp w przemysłowych systemach sterowania
W6	Ochrona tajemnicy firmy i danych technologicznych
W7	Problem dostępu zdalnego do procesu technologicznego, systemy HMI na urządzenia mobilne
Forma zajęć - laboratoria	
	Treści programowe
L1	Konfigurowanie urządzenia HMI z bezpośrednim i wyłącznym dostępem do procesu, tworzenie prostej aplikacji, badanie czasu reakcji, zasada fail-safe
L2	Konfiguracja urządzenia HMI z dostępem poprzez sieć przemysłową
L3	Programowanie i testowanie aplikacji do sterowania procesem o zdarzeniach dyskretnych z możliwością wyboru wariantów
L4	Projektowanie aplikacji HMI do pracy w sieci z równoległym dostępem do procesu z wielu urządzeń, testowanie procedur bezpieczeństwa
L5	Programowanie aplikacji HMI na urządzenia przenośne z dostępem zdalnym poprzez sieć Internet, testowanie scenariuszy awaryjnych i serwisowych

Metody dydaktyczne	
1	wykład informacyjny
2	ćwiczenia laboratoryjne
3	gry symulacyjne

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena wykonanych ćwiczeń laboratoryjnych	51%
O3	ocena wykonanych symulacji	51%

Literatura podstawowa	
1	Solnik, Włodzimierz, i in. Sieci przemysłowe Profibus DP, ProfiNet, AS-i i EGD : przykłady zastosowań. Wydanie I., Wyd. BTC, 2018.
2	Gilewski, Tomasz. Tworzenie wizualizacji na panele HMI firmy Siemens. Helion, 2019.
3	Majewski, Maciej. Podstawy budowy inteligentnych systemów interakcji urządzeń technologicznych i ich operatorów. Wyd. Uczelniane Politechniki Koszalińskiej, 2010.

Literatura uzupełniająca	
1	Rao, P. V. S., and Sunil Kumar Kopparapu. Friendly Interfaces Between Humans and Machines. Springer Singapore, 2018, https://doi.org/10.1007/978-981-13-1750-7 .
2	Boy, Guy A. The Handbook of Human-Machine Interaction a Human-Centered Design Approach. Ashgate, 2011.
3	Świszcz, Piotr, i in. Laboratorium przemysłowych sieci komunikacyjnych. Wyd. Politechniki Śląskiej, 2011.
4	Szajnar, Stanisław Wojciech. Czynniki ludzkie w obsłudze urządzeń technicznych. Wojskowa Akademia Techniczna, 2010.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	60
Udział w wykładach:	30
Udział w zajęciach laboratoryjnych:	30
Praca własna studenta, w tym:	40
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	20
Przygotowanie do zajęć laboratoryjnych:	20
Łączny czas pracy studenta	100
Sumaryczna liczba punktów ECTS dla przedmiotu	4

Macierz efektów uczenia się					
Symbol przedmiotowe	Odniesienie przedmiotowego efektu uczenia się	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny

go efektu uczenia się	do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania				
EK 1	CB1A_W17+++	C1	W1-W7	1	O1
EK 2	CB1A_W06++ CB1A_W10++	C2,C3	L1-L5	2,3	O2,O3
EK 3	CB1A_U17+++	C2,C3	L1-L5	2,3	O2,O3
EK 4	CB1A_U24++	C2,C3	L1-L5	2,3	O2,O3
EK 5	CB1A_K05+	C1,C2,C3	L1-L5	1,2,3	O2,O3

Autor programu:	dr inż. Radosław Cechowicz
Adres e-mail:	r.cechowicz@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Technicznej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Analiza i zarządzanie ryzykiem w cyberbezpieczeństwie
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C307
Rok:	II
Semestr:	3
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	60
Wykład	30
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	5
Sposób zaliczenia:	egzamin
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zapoznanie z analizą ryzyka w kontekście cyberbezpieczeństwa
C2	Przekazanie wiedzy na temat metod identyfikacji, oceny i zarządzania ryzykiem w systemach informatycznych
C3	Wykształcenie umiejętności identyfikacji zagrożeń i podatności w systemach informatycznych oraz oceny ich wpływu na organizację
C4	Rozwinięcie kompetencji w zakresie ekonomicznej oceny rozwiązań bezpieczeństwa

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Znajomość podstawowych zagadnień z obszaru systemów informatycznych i cyberbezpieczeństwa
2	Umiejętność analitycznego myślenia i pracy z dokumentami
3	Znajomość kluczowych koncepcji zarządzania bezpieczeństwem informacji

Efekty uczenia się	
	W zakresie wiedzy:
EK1	zna i rozumie metody diagnozowania, analizy i oceny ryzyka występowania sytuacji stanowiących zagrożenie w cyberprzestrzeni
EK2	zna metody analizy ryzyka oraz podstawowe zasady szacowania kosztów i oceny efektywności ekonomicznej rozwiązań stosowanych w obszarze cyberbezpieczeństw w przedsiębiorstwach i instytucjach
EK3	zna etapy zarządzania ryzykiem w organizacjach
	W zakresie umiejętności:

EK4	identyfikuje i klasyfikuje ryzyka związane z bezpieczeństwem IT w organizacji
EK5	potrafi przeprowadzić ocenę ryzyka i opracować plan zarządzania ryzykiem
EK6	potrafi zastosować odpowiednie narzędzia i techniki wspomagające proces analizy ryzyka
EK7	potrafi oszacować koszty wdrożenia i utrzymania rozwiązań z zakresu cyberbezpieczeństwa oraz dokonać ich wstępnej oceny ekonomicznej, uwzględniając skuteczność, ryzyko i realne potrzeby organizacji
	W zakresie kompetencji społecznych:
EK8	jest gotów do myślenia i działania w sposób przedsiębiorczy, podejmując inicjatywy w upowszechnianiu dobrych praktyk zarządzania ryzykiem cybernetycznym oraz promując kulturę bezpieczeństwa informacji w środowiskach zawodowych i społecznych

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Wprowadzenie do analizy ryzyka w cyberbezpieczeństwie. Definicje ryzyka, zagrożeń i podatności. Przegląd podstawowych pojęć i ram zarządzania ryzykiem
W2	Metody analizy ryzyka. Podejścia jakościowe, półilościowe i ilościowe
W3	Modele i standardy zarządzania ryzykiem
W4	Identyfikacja zagrożeń i podatności. Klasyfikacja zagrożeń cybernetycznych. Narzędzia do identyfikacji podatności
W5	Ocena ryzyka i matryce ryzyka
W6	Strategie zarządzania ryzykiem. Unikanie, redukcja, akceptacja i transfer ryzyka. Dobór środków bezpieczeństwa do ograniczania ryzyka
W7	Monitorowanie i przegląd ryzyka. Cykl zarządzania ryzykiem
W8	Ekonomiczne aspekty zarządzania ryzykiem. TCO (Total Cost of Ownership) dla systemów zabezpieczeń. ROI/ROSI (Return on Security Investment) – metodyka i zastosowanie w analizie ryzyka
Forma zajęć - laboratoria	
	Treści programowe
L1	Identyfikacja kluczowych procesów oraz zasobów informatycznych w organizacji. Analiza wpływu biznesowego (BIA)
L2	Identyfikacja zagrożeń i podatności
L3	Ocena ryzyka. Tworzenie matrycy ryzyka dla organizacji. Ocena ryzyka z wykorzystaniem specjalistycznego oprogramowania
L4	Strategie minimalizacji ryzyka. Opracowanie planów minimalizacji ryzyka dla wybranych scenariuszy. Tworzenie procedur reagowania na incydenty
L5	Raportowanie i przedstawienie wyników. Opracowanie raportu z oceny ryzyka
L6	Oszacowanie kosztów wdrożenia i utrzymania środków bezpieczeństwa dla różnych scenariuszy. Praktyczne zastosowanie modelu ROSI. Ujęcie ekonomiczne w dokumentacji ryzyka – jak raportować koszty i efektywność

L 7	Symulacja decyzyjna: analiza wariantów zabezpieczeń. Porównanie dwóch rozwiązań pod kątem ryzyka, kosztów, zasobów. Tworzenie tabel kosztów, korzyści i ryzyk związanych z wdrożeniem
-----	---

Metody dydaktyczne	
1	wykład informacyjny
2	analiza przypadków
3	ćwiczenia laboratoryjne
4	przygotowanie sprawozdania

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena wykonanych ćwiczeń laboratoryjnych	51%
O3	ocena wykonanych sprawozdań laboratoryjnych	51%

Literatura podstawowa	
1	Hubbard, Douglas i in., Ryzyko w cyberbezpieczeństwie : metody modelowania, pomiaru i szacowania ryzyka. Wyd. Helion, 2024.
2	Liderman, Krzysztof, Analiza ryzyka i ochrona informacji w systemach komputerowych. Wyd. PWN, 2009.
3	Norma ISO/IEC 27005:2022 „Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji”.

Literatura uzupełniająca	
1	Dela, Piotr, Założenia działań w cyberprzestrzeni. Wyd. PWN, 2022.
2	Brotherston, Lee, i in., Bezpieczeństwo defensywne : podstawy i najlepsze praktyki. Wyd. Helion, 2019.
3	Krasuski, Andrzej, i in., Analiza ryzyka w ochronie danych osobowych. Wolters Kluwer Polska SA, 2022.
4	Zmitrowicz, Karolina, Analiza biznesowa w IT. Lessons learned. Wyd. Helion, 2024.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	60
Udział w wykładach:	30
Udział w zajęciach laboratoryjnych:	30
Praca własna studenta, w tym:	65
Studiowanie tematyki wykładów, przygotowanie do egzaminu:	38

Przygotowanie do zajęć laboratoryjnych:	27
Łączny czas pracy studenta	125
Sumaryczna liczba punktów ECTS dla przedmiotu	5

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W04++	C1, C2, C4	W1, W2, W4, W5	1, 2	O1
EK 2	CB1A_W13+++ CB1A_W14+++ CB1A_W08+	C1, C2	W1, W3, W6 - W8	1	O1
EK 3	CB1A_W13+++	C1, C2	W1 - W7	1, 2	O1
EK 4	CB1A_U13+++ CB1A_U01+	C2, C3	L1 - L3, L5	2 - 4	O2, O3
EK 5	CB1A_U11+++	C1 - C3	L1 - L5	2 - 4	O2, O3
EK 6	CB1A_U11+++	C1 - C3	L1 - L3	3, 4	O2, O3
EK 7	CB1A_U09+++	C4	L6, L7	2 - 4	O2, O3
EK 8	CB1A_K02+	C1 - C4	W1 - W7, L1 - L5	1 - 4	O1, O2, O3

Autor programu:	dr inż. Joanna Szulzyk-Cieplak
Adres e-mail:	j.szulzyk-cieplak@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Technicznej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Aspekty prawne cyberbezpieczeństwa
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C308
Rok:	II
Semestr:	3
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	45
Wykład	30
Ćwiczenia	
Laboratorium	
Projekt	15
Liczba punktów ECTS:	3
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu

C1	Zapoznanie z krajowymi i międzynarodowymi regulacjami prawnymi dotyczącymi cyberbezpieczeństwa
C2	Nabycie umiejętności sprawnego posługiwania się przepisami prawa w obszarze cyberprzestrzeni
C3	Rozwinięcie kompetencji w zakresie tworzenia dokumentacji zgodnej z wymaganiami prawnymi i standardami w środowisku cyfrowym

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1	Podstawowa wiedza na temat systemów informatycznych
2	Podstawowa wiedza na temat zagrożeń w cyberprzestrzeni
3	Umiejętność analizy tekstów oraz krytycznego myślenia

Efekty uczenia się

	W zakresie wiedzy:
EK 1	zna najważniejsze regulacje prawne związane z obszarem cyberbezpieczeństwa
EK 2	rozumie mechanizmy współpracy podmiotów zaangażowanych w system cyberbezpieczeństwa, zna ich kompetencje, role oraz zakres odpowiedzialności w kontekście reagowania na incydenty i zapewniania bezpieczeństwa cyfrowego
EK 3	identyfikuje podstawowe zasady ochrony własności intelektualnej w kontekście tworzenia, udostępniania i ochrony technologii informacyjnych i danych cyfrowych
	W zakresie umiejętności:
EK 4	potrafi korzystać z aktów prawnych oraz norm kluczowych z punktu widzenia cyberbezpieczeństwa oraz implementować wynikające z nich obowiązki

EK 5	rozwiązuje problemy z obszaru cyberbezpieczeństwa wymagające zastosowania wiedzy specjalistycznej oraz interdyscyplinarnej
	W zakresie kompetencji społecznych:
EK 6	jest gotów do podejmowania odpowiednich decyzji dotyczących bezpieczeństwa przy posługiwaniu się technologiami IT w przedsiębiorstwach oraz instytucjach

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Podstawy teorii prawa: struktura systemu prawnego, rodzaje źródeł prawa, zasady techniki prawodawczej
W2	Tło i uwarunkowania tworzenia najważniejszych regulacji prawnych dotyczących systemu cyberbezpieczeństwa w Polsce, ze szczególnym uwzględnieniem Dyrektywy NIS2 oraz ustawy o krajowym systemie cyberbezpieczeństwa (KSC)
W3	Charakterystyka podmiotów objętych regulacjami (operatorów usług kluczowych, dostawców usług cyfrowych i wybranych podmiotów publicznych) w świetle Dyrektywy NIS2 i ustawy o KSC, z uwzględnieniem ich roli w strukturze państwa i znaczenia dla bezpieczeństwa krytycznego
W4	Zadania oraz obowiązki związane z zapewnieniem cyberbezpieczeństwa przez podmioty kluczowe oraz podmioty ważne w oparciu o wymogi z dyrektywy NIS 2 oraz ustawy o KSC
W5	Definicja incydentu cyberbezpieczeństwa, cyklu życia incydentu oraz procedury reagowania. Przegląd zadań kluczowych podmiotów publicznych zaangażowanych w obsługę takich zdarzeń
W6	Znaczenie zespołów CERT w strukturze reagowania na incydenty i utrzymania bezpieczeństwa sieci oraz systemów informacyjnych
W7	Omówienie pozostałych istotnych aktów prawnych, m.in. DORA, CER, AI Act
W8	Prawo dotyczące cyberprzestępczości. Konwencja Budapesztańska. Przestępstwa komputerowe w polskim kodeksie karnym. Odpowiedzialność za naruszenie cyberbezpieczeństwa (prawna, administracyjna, cywilna, pracownicza)
W9	Zagadnienia prawa międzynarodowego odnoszące się do funkcjonowania państw w cyberprzestrzeni, ze wskazaniem ich roli, podstaw normatywnych oraz odmienności między przepisami krajowymi a regulacjami międzynarodowymi. Normy cyberbezpieczeństwa - nowe formy regulacji zachowań państw w cyberprzestrzeni
W10	Ocena incydentów naruszających bezpieczeństwo systemów informatycznych w kontekście obowiązujących norm prawa międzynarodowego, kwestie przypisywania cyberoperacji państwom oraz prawne uwarunkowania działań odwetowych w cyberprzestrzeni
W11	Ochrona własności intelektualnej w cyberprzestrzeni
Forma zajęć - projekt	
	Treści programowe
P1	Analiza i porównanie obowiązków podmiotów kluczowych i ważnych. Opracowanie tabeli obowiązków wynikających z Dyrektywy NIS2 i ustawy o KSC. Identyfikacja

	różnic w wymaganiach wobec operatorów usług kluczowych, dostawców usług cyfrowych i innych podmiotów publicznych
P2	Symulacja obsługi incydentu cyberbezpieczeństwa. Opracowanie schematu postępowania w przypadku incydentu. Podział ról (CERT, IOD, zarząd, podmiot objęty regulacją). Przygotowanie wzoru zgłoszenia incydentu do CSIRT
P3	Studium przypadku: odpowiedzialność prawna za naruszenie cyberbezpieczeństwa. Analiza wybranych przypadków z Polski lub UE (np. wycieki danych, ataki ransomware). Identyfikacja odpowiedzialności karnej, administracyjnej, cywilnej. Opracowanie notatki służbowej w reakcji na zdarzenie
P4	Stworzenie mapy regulacji (RODO, KSC, NIS2, DORA, CER, AI Act) i ich zastosowania w różnych obszarach działalności. Wskazanie konfliktów lub luk między przepisami
P5	Przestępstwa komputerowe – rozpoznawanie i kwalifikacja prawna. Analiza przypadków przestępstw z art. 267–269b Kodeksu karnego. Kwalifikacja czynów, propozycja działań prawnych i wewnętrznych procedur
P6	Dyskusja nad wyzwaniem związanym z regulacjami prawnymi w cyberprzestrzeni

Metody dydaktyczne	
1	wykład informacyjny
2	analiza przypadków
3	metoda projektu
4	praca wykonywana w grupach

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena przygotowanego projektu	51%

Literatura podstawowa	
1	Worona-Vlugt, Joanna, Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy. Wolters Kluwer Polska SA, 2020.
2	Białas, Adam, Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, Wyd. II. Wyd. PWN, 2021.
3	Szpor, Grażyna, i in., Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz. Wolters Kluwer Polska SA, 2019.
4	Gomularz, Mirosław, Świadczenie usług drogą elektroniczną. Komentarz. Wolters Kluwer Polska SA, 2019.

Literatura uzupełniająca	
1	Bułat, Adam, i in., Prawne aspekty cyberprzestrzeni. Wyd. Uniwersytetu Kazimierza Wielkiego w Bydgoszczy, 2020.

2	Kępa, Leszek, : Bezpieczeństwo danych osobowych. Podejście oparte na ryzyku. Wyd. C.H.Beck Sp. z o.o., 2019.
3	Sieńczyło-Chlabicz, Joanna, Własność intelektualna i nowe technologie w Internecie w dobie społeczeństwa cyfrowego. Wyd. Uniwersytetu w Białymstoku, 2022.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	45
Udział w wykładach:	30
Udział w zajęciach projektowych:	15
Praca własna studenta, w tym:	30
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	20
Przygotowanie projektu:	10
Łączny czas pracy studenta	75
Sumaryczna liczba punktów ECTS dla przedmiotu	3

Macierz efektów uczenia się					
Symbol przedmiotowe go efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W13+++ CB1A_W20+++	C1	W1 - W2, W7 - W11	1, 2	O1
EK 2	CB1A_W13+++ CB1A_W20+++	C1	W2 - W6	1, 2	O1
EK 3	CB1A_W16++	C1	W2, W7	1	O1
EK 4	CB1A_U20+++	C2, C3	P1 - P6	2 - 4	O2
EK 5	CB1A_U07++ CB1A_U09++	C2, C3	P1 - P6	2 - 4	O2
EK 6	CB1A_K04++	C1 - C3	W1 - W11, P1 - P6	1 - 4	O1, O2

Autor programu:	dr inż. Joanna Szulżyk-Cieplak
Adres e-mail:	j.szulzyk-cieplak@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Technicznej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Ochrona danych osobowych i informacji niejawnych
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C401
Rok:	II
Semestr:	4
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	45
Wykład	30
Ćwiczenia	
Laboratorium	
Projekt	15
Liczba punktów ECTS:	4
Sposób zaliczenia:	egzamin
Język wykładowy:	język polski

Cele przedmiotu	
C1	Przekazanie wiedzy na temat przepisów prawa dotyczących ochrony danych osobowych i informacji niejawnych
C2	Zapoznanie z zasadami klasyfikacji, przetwarzania i ochrony danych wrażliwych i informacji chronionych
C3	Kształtowanie umiejętności rozpoznawania ryzyk i reagowania na naruszenia ochrony danych i informacji
C4	Rozwijanie praktycznych kompetencji w zakresie projektowania bezpiecznych komponentów systemów informatycznych zgodnych z wymaganiami ochrony danych

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Znajomość kluczowych zagadnień z obszaru cyberbezpieczeństwa
2	Umiejętność analizy treści normatywnych i technicznych
3	Gotowość do pracy zespołowej i udziału w dyskusji problemowej

Efekty uczenia się	
	W zakresie wiedzy:
EK1	zna podstawowe przepisy prawne dotyczące ochrony danych osobowych (RODO) i informacji niejawnych

EK2	zna klasyfikację danych i informacji chronionych, role i obowiązki administratora danych, IOD oraz pełnomocnika ds. informacji niejawnych, a także zasady legalnego i bezpiecznego przetwarzania danych
EK3	rozumie wymagania techniczne i organizacyjne dotyczące bezpieczeństwa informacji
	W zakresie umiejętności:
EK4	potrafi analizować procesy przetwarzania danych i wskazać możliwe zagrożenia dla ich bezpieczeństwa
EK5	umie dobrać odpowiednie środki techniczne i organizacyjne zabezpieczające dane zgodnie z obowiązującym prawem
EK6	potrafi zaplanować i zaimplementować elementy systemu informatycznego z uwzględnieniem odpowiednich zabezpieczeń danych osobowych i informacji niejawnych
	W zakresie kompetencji społecznych:
EK7	jest gotów do odpowiedzialnego pełnienia ról zawodowych wykazując świadomość odpowiedzialności za naruszenia ochrony danych i informacji oraz przestrzegając zasad etyki i przepisów prawa w zakresie ochrony informacji

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Wprowadzenie do zagadnień ochrony danych osobowych i informacji niejawnych
W2	Przegląd regulacji: RODO, ustawa o ochronie danych osobowych, ustawa o ochronie informacji niejawnych
W3	Klasyfikacja informacji: dane osobowe, dane wrażliwe, informacje niejawne (ściśle tajne, tajne, poufne, zastrzeżone)
W4	Rola administratora danych, IOD i pełnomocnika ds. ochrony informacji niejawnych
W5	Zasady przetwarzania danych i informacji: legalność, celowość, minimalizacja, kontrola dostępu
W6	Wymagania techniczne i organizacyjne – szyfrowanie, pseudonimizacja, strefy bezpieczeństwa
W7	Systemy informatyczne przetwarzające dane osobowe i informacje niejawne – obowiązki, ograniczenia
W8	Zasady bezpieczeństwa informacji – poufność, integralność, dostępność (CIA)
W9	Reagowanie na incydenty i naruszenia – obowiązki, zgłaszanie, sankcje
W10	Wymagania dla systemów IT przetwarzających dane chronione – zgodność z prawem i normami (RODO, UOIN, ISO 27001)
W11	Privacy by design & security by design w projektowaniu systemów IT
W12	Problem prywatności. Prywatna komunikacja i śledzenie użytkowników
W13	Ochrona danych w spoczynku i ruchu. Scenariusze wycieków danych
W14	Technologiczne spojrzenie na RODO i zabezpieczenia w systemach informatycznych
W15	Współczesne zagrożenia dla danych – przypadki wycieków, cyberataki, odpowiedzialność prawna
Forma zajęć - projekt	

	Treści programowe
P1	Analiza przypadków naruszenia ochrony danych osobowych i informacji niejawnych
P2	Przygotowanie uproszczonej klasyfikacji informacji w przykładowej instytucji
P3	Symulacja procedury zgłoszenia naruszenia do PUODO lub pełnomocnika ds. OIN
P4	Projekt komponentu systemu IT (np. formularz, baza danych) z zastosowaniem środków ochrony danych zgodnych z wymaganiami prawnymi
P5	Ocena zgodności proponowanych zabezpieczeń z wybranymi regulacjami (RODO, ustawa o OIN, ISO/IEC 27001)

	Metody dydaktyczne
1	wykład informacyjny
2	analiza przypadków
3	metoda projektu
4	praca wykonywana w grupach

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena przygotowanego projektu	51%

	Literatura podstawowa
1	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE
2	Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych. Dz.U. 2018 poz. 1000
3	Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Dz.U. 2010 nr 182 poz. 1228
4	Norma ISO/IEC 27001 – Systemy zarządzania bezpieczeństwem informacji
5	Śmiałek, Katarzyna, Aleksandra Kominek, Technologiczny wymiar ochrony danych osobowych. Wydawnictwo Naukowe FNCE, 2021.
6	Dominik, Lubasz, i in., Ochrona danych osobowych. Poradnik praktyczny. Wydawnictwo: Wolters Kluwer Polska, 2023.

	Literatura uzupełniająca
1	Prasal, Artur i in. Procedury elektronicznego zarządzania dokumentacją w administracji. Wydanie 2. Stan prawny: styczeń 2023. Warszawa: C. H. Beck, 2023.
2	Klaudia Gaczoł, i Maciej Pichlak. Refleksyjna regulacja ryzyka w ochronie danych osobowych. Podstawy teoretyczne i praktyka działalności Prezesa UODO. Wydanie 1. Wydawnictwo Uniwersytetu Łódzkiego, 2022.

Obciążenie pracą studenta

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	45
Udział w wykładach:	30
Udział w zajęciach projektowych:	15
Praca własna studenta, w tym:	55
Studiowanie tematyki wykładów, przygotowanie do egzaminu:	35
Przygotowanie projektu:	20
Łączny czas pracy studenta	100
Sumaryczna liczba punktów ECTS dla przedmiotu	4

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W13+++	C1, C2	W1 - W15	1	O1
EK 2	CB1A_W13+++ CB1A_W14+	C1, C2	W1 - W15	1	O1
EK 3	CB1A_W15++	C2	W6 - W12	1	O1
EK 4	CB1A_U01+++ CB1A_U13+++ CB1A_U09++	C3	P1 - P5	2 - 4	O2
EK 5	CB1A_U20++ CB1A_U23+++	C3, C4	P1 - P5	2 - 4	O2
EK 6	CB1A_U23+++ CB1A_U07++ CB1A_U03++	C4	P5	2 - 4	O2
EK 7	CB1A_K05++	C1 - C4	W1 - W6, L1 - L4, P1 - P6	1 - 6	O1 - O4

Autor programu:	dr inż. Joanna Szulżyk-Cieplak, dr inż. Stanisław Sulenta
Adres e-mail:	j.szulzyk-cieplak@pollub.pl, s.sulenta@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Technicznej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Bezpieczeństwo chmury obliczeniowej
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C402
Rok:	II
Semestr:	4
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	45
Wykład	15
Ćwiczenia	
Laboratorium	
Projekt	30
Liczba punktów ECTS:	3
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Przedstawienie podstawowych koncepcji i architektur chmury obliczeniowej oraz ich roli w nowoczesnych systemach informatycznych
C2	Zrozumienie zagrożeń i mechanizmów ochrony w środowisku chmury obliczeniowej
C3	Rozwijanie umiejętności projektowania i wdrażania systemów zabezpieczających w chmurze obliczeniowej

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Znajomość podstaw technologii informatycznych oraz systemów operacyjnych
2	Umiejętność obsługi narzędzi sieciowych
3	Podstawowa wiedza z zakresu cyberbezpieczeństwa

Efekty uczenia się	
	W zakresie wiedzy:
EK 1	zna podstawowe pojęcia, modele i architektury chmury obliczeniowej
EK 2	rozumie zagrożenia wynikające z używania technologii chmurowych i mechanizmy ich minimalizacji
	W zakresie umiejętności:
EK3	potrafi zaprojektować i wdrożyć bezpieczne środowisko w chmurze obliczeniowej
EK4	umie zastosować odpowiednie narzędzia do monitorowania i reagowania na incydenty w chmurze
	W zakresie kompetencji społecznych:
EK5	jest gotów do odpowiedzialnego wykonywania zadań związanych z zarządzaniem bezpieczeństwem systemów w chmurze, przestrzegając zasad etyki zawodowej

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Wprowadzenie do chmury obliczeniowej (modele IaaS, PaaS, SaaS)
W2	Podstawy architektury chmury obliczeniowej i jej zastosowań
W3	Typowe zagrożenia w środowisku chmurowym (np. ataki DDoS, utrata danych)
W4	Mechanizmy zabezpieczeń w chmurze obliczeniowej (szyfrowanie, kontrola dostępu, firewall)
W5	Wprowadzenie do zarządzania incydentami w chmurze
W6	Polityki bezpieczeństwa i zgodność z regulacjami prawnymi w kontekście chmury
W7	Zabezpieczenia danych w chmurze (backup, ochrona przed nieautoryzowanym dostępem)
W8	Przyszłość technologii chmurowych i rozwijające się wyzwania bezpieczeństwa
Forma zajęć - projekt	
	Treści programowe
P1	Projektowanie architektury bezpiecznej chmury obliczeniowej
P2	Implementacja mechanizmów zabezpieczeń (np. konfiguracja kontroli dostępu, szyfrowania danych)
P3	Symulacja i analiza incydentów bezpieczeństwa w chmurze
P4	Monitorowanie środowiska chmurowego pod kątem bezpieczeństwa
P5	Opracowanie polityki bezpieczeństwa dla usług chmurowych
P6	Testowanie i ocena skuteczności zaimplementowanych rozwiązań

Metody dydaktyczne	
1	wykład problemowy
2	analiza przypadków
3	metoda projektu

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena przygotowanego projektu	51%
O3	ocena obrony projektu	51%

Literatura podstawowa	
1	Bravo, Cesar, i in. Cyberbezpieczeństwo dla zaawansowanych : skuteczne zabezpieczenia systemu Windows, Linux, IoT i infrastruktury w chmurze. Helion, 2023.
2	Jatkiewicz, Przemysław, i in. Bezpieczeństwo systemów informatycznych firm i instytucji. Wyd. Uniwersytetu Gdańskiego, 2020.

Literatura uzupełniająca	
1	T. Erl, Cloud Computing Design Patterns, Prentice Hall, 2015.
2	K. Krutz, R. Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Wiley, 2010.
3	C. Dotson, Bezpieczeństwo w chmurze, Wyd. Naukowe PWN, 2020.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	45
Udział w wykładach:	15
Udział w zajęciach projektowych:	30
Praca własna studenta, w tym:	30
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	10
Przygotowanie projektu:	20
Łączny czas pracy studenta	75
Sumaryczna liczba punktów ECTS dla przedmiotu	3

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W02++, CB1A_W12++	C1	W1-W4	1, 2	O1
EK 2	CB1A_W12++	C1, C2	W5-W8	1, 2	O1
EK 3	CB1A_U16+++	C3	P1-P3	3	O2, O3
EK 4	CB1A_U16++ CB1A_U18++	C3	P4-P6	3	O2, O3
EK 5	CB1A_K05+	C3	P5, P6	3	O2, O3

Autor programu:	dr hab. inż. Dariusz Czerwiński, profesor uczelni; mgr Dariusz Głuchowski
Adres e-mail:	d.czerwinski@pollub.pl; d.gluchowski@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Stosowanej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Bezpieczeństwo oprogramowania i aplikacji mobilnych
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C403
Rok:	II
Semestr:	4
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	60
Wykład	30
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	4
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zapoznanie z zasadami bezpiecznego programowania, zarządzania uprawnieniami oraz ochrony danych w aplikacjach mobilnych
C2	Zdobycie umiejętności implementacji mechanizmów uwierzytelniania, autoryzacji, szyfrowania danych oraz ochrony aplikacji przed atakami
C3	Rozwijanie kompetencji w zakresie analizy zagrożeń oraz monitorowania aplikacji mobilnych pod kątem bezpieczeństwa

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Znajomość programowanie obiektowego
2	Znajomość algorytmów i struktur danych

Efekty uczenia się	
	W zakresie wiedzy:
EK 1	wyjaśnia praktyki bezpiecznego programowania i opisuje zagrożenia oraz podatności
EK 2	opisuje zasady bezpiecznego programowania i zarządzania uprawnieniami w aplikacjach mobilnych
EK 3	wyjaśnia techniki ochrony danych użytkownika oraz zabezpieczania komunikacji między aplikacją a serwerem
	W zakresie umiejętności:
EK 4	tworzy aplikacje pozbawione podatności na poziomie kodu i zarządzania pamięcią
EK 5	projektuje i implementuje mechanizmy uwierzytelniania i autoryzacji, w tym bezpieczne metody logowania i zarządzania sesjami użytkowników

EK 6	implementuje mechanizmy szyfrowania danych, techniki ochrony aplikacji przed odtwarzaniem kodu oraz zabezpieczenia danych przechowywanych lokalnie i przesyłanych
	W zakresie kompetencji społecznych:
EK 7	jest gotów do odpowiedzialnego projektowania aplikacji mobilnych z uwzględnieniem aspektów bezpieczeństwa oraz współpracy w zespołach realizujących zadania związane z analizą i ochroną aplikacji

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Modele bezpieczeństwa oprogramowania
W2	Zasady Security by Design
W3	Zarządzanie pamięcią (unikanie buffer overflow, use-after-free)
W4	DevSecOps – automatyzacja testów bezpieczeństwa
W5	Wprowadzenie do bezpieczeństwa systemów i aplikacji mobilnych
W6	Zarządzanie uprawnieniami i dostępem w systemach mobilnych
W7	Bezpieczeństwo danych użytkownika i biblioteki realizujące techniki szyfrowania
W8	Mechanizmy uwierzytelniania i autoryzacji użytkowników
W9	Bezpieczeństwo przechowywanych danych w systemach mobilnych
W10	Ochrona aplikacji przed reverse engineering
W11	Testowanie bezpieczeństwa aplikacji mobilnych
W12	Monitoring i analiza zagrożeń w aplikacjach mobilnych
W13	Najlepsze praktyki w bezpieczeństwie aplikacji mobilnych
Forma zajęć - laboratoria	
	Treści programowe
L1	Wprowadzenie do metody STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege)
L2	Koncepcja zarządzania pamięcią i jej ochrony
L3	Omówienie i implementacja koncepcji Least Privilege, Fail-Safe Defaults, Defense in Depth
L4	Zasady bezpiecznego programowania, dobre praktyki w tworzeniu bezpiecznego kodu dla aplikacji mobilnych
L5	Zarządzanie uprawnieniami i dostępem w aplikacjach mobilnych, kontrola dostępu do zasobów urządzenia
L6	Ochrona danych użytkownika, techniki szyfrowania danych lokalnych i przesyłanych
L7	Implementacja technik uwierzytelniania i autoryzacji oraz bezpiecznych mechanizmów logowania i sesji użytkownika
L8	Bezpieczeństwo danych przechowywanych w urządzeniach mobilnych
L9	Zapobieganie atakom typu reverse engineering, techniki ochrony kodu aplikacji przed odtwarzaniem

L10	Testy penetracyjne aplikacji mobilnych, analiza aplikacji pod kątem luk i podatności na ataki
L11	Monitoring i analiza zagrożeń w aplikacjach mobilnych – narzędzia i techniki monitorowania aplikacji pod kątem bezpieczeństwa

Metody dydaktyczne	
1	wykład informacyjny
2	ćwiczenia laboratoryjne

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51 %
O2	ocena wykonanych programów komputerowych	51 %

Literatura podstawowa	
1	Verma P. K., i in.: Bezpieczeństwo urządzeń mobilnych : receptury. Gliwice: Wyd. Helion, 2017. Print.
2	Boniewicz A.: Wydawca. Analiza śledcza urządzeń mobilnych : teoria i praktyka. Gliwice: Helion, 2023. Print.
3	Laskowski M.: Techniki ochrony informacji. Lublin: Politechnika Lubelska, 2013. Print.

Literatura uzupełniająca	
1	Ściborek P.: Uwierzytelnianie i Autoryzacja Zasobów w Sieciach Definiowanych Programowo. Elektronika 1.10 (2017): 58–62. Web.
2	Rzecki K.: Zagadnienia programowania aplikacji mobilnych i systemów wbudowanych : praca zbiorowa. Kraków: Wyd. PK, 2016. Print.
3	Poniszewska-Marańda A.: Modele bezpieczeństwa logicznego i ich implementacje w systemach informatycznych. Warszawa: Akademicka Oficyna Wydawnicza EXIT, 2013. Print.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	60
Udział w wykładach:	30
Udział w zajęciach laboratoryjnych:	30
Praca własna studenta, w tym:	40
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	20
Przygotowanie do zajęć laboratoryjnych:	20
Łączny czas pracy studenta	100

Sumaryczna liczba punktów ECTS dla przedmiotu	4
---	---

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W17+++ CB1A_W12++	C1, C2, C3	W1 - W5	1	O1
EK 2	CB1A_W17+++ CB1A_W12++	C1, C2, C3	W5 - W13	1	O1
EK 3	CB1A_W17+++ CB1A_W12++	C1, C2, C3	W5 - W13	1	O1
EK 4	CB1A_U24+++ CB1A_U15++ CB1A_U17++	C1, C2	L1 - L4	2	O2
EK 5	CB1A_U24+++ CB1A_U15++ CB1A_U17++	C1, C2	L3 - L11	2	O2
EK 6	CB1A_U24+++ CB1A_U15++ CB1A_U17++	C1, C3	L3 - L11	2	O2
EK 7	CB1A_K05+	C1, C2, C3	W1 - W13, L1 - L11	1, 2	O1, O2

Autor programu:	dr Rafał Stęgiński; mgr inż. Albert Rachwał
Adres e-mail:	r.stegierski@pollub.pl; a.rachwal@pollub.pl
Jednostka organizacyjna:	Katedra Inteligencji Obliczeniowej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Bezpieczeństwo danych
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C404
Rok:	II
Semestr:	4
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	60
Wykład	30
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	4
Sposób zaliczenia:	egzamin
Język wykładowy:	język polski

Cele przedmiotu

C1	Zapoznanie z kluczowymi pojęciami ochrony danych, zasadami jej stosowania i standardami bezpieczeństwa
C2	Wykształcenie zdolności wdrażania środków ochrony danych takich jak zapewnienie integralności danych, szyfrowanie i autoryzacja

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1	Znajomość podstaw arytmetyki modularnej
2	Podstawowa wiedza z zakresu baz danych
3	Podstawowe umiejętności programistyczne

Efekty uczenia się

	W zakresie wiedzy:
EK 1	rozróżnia podstawowe zagadnienia dotyczące zagrożeń w cyberprzestrzeni i sposobów ochrony przed nimi
EK 2	opisuje wybrane aspekty cyklu życia zasobów informatycznych w obszarach integralności, poufności i niezaprzeczalności
	W zakresie umiejętności:
EK3	potrafi praktycznie analizować, oceniać i stosować metody ochrony danych przed zagrożeniami w tworzonych aplikacjach
EK4	korzysta z dostępnych narzędzi do zaprezentowania działania algorytmów zabezpieczania danych
	W zakresie kompetencji społecznych:

EK5	jest gotów do sumiennego wykonywania zadań zawodowych związanych z zabezpieczaniem danych wypełniając zobowiązania społeczne dotyczące promocji bezpiecznych praktyk cyfrowych
------------	--

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Wprowadzenie do bezpieczeństwa danych
W2	Entropia i mierzenie ilości informacji w danych
W3	Integralność danych i sumy kontrolne
W4	Poufność danych, klucz kryptograficzny i typy kryptografii
W5	Algorytm szyfrowania AES
W6	Algorytm szyfrowania RSA
W7	Podpis cyfrowy i niezaprzeczalność
W8	Krzywe eliptyczne
W9	Mechanizmy uwierzytelniania i autoryzacji
W10	Zapewnienie dostępności i ochrona przed atakami DDoS
W11	Bezpieczeństwo danych w chmurze i wirtualizacji
Forma zajęć - laboratoria	
	Treści programowe
L1	Kopie zapasowe i odzyskiwanie usuniętych plików
L2	Ilość informacji w danych - obliczanie entropii
L3	Implementacja prostych algorytmów szyfrowania
L4	Integralność danych - wybrane kody EDC i ECC
L5	Sumy kontrolne - obliczanie i kolizje
L6	Protokół uzgadniania kluczy Diffiego-Hellmana
L7	Praktyczne użycie algorytmów AES i RSA
L8	Podpisy cyfrowe
L9	Kryptosystemy oparte na krzywych eliptycznych
L10	Implementacja mechanizmów rejestracji i uwierzytelniania użytkownika
L11	SQL injection i zabezpieczenia przed tą formą ataku

Metody dydaktyczne	
1	wykład informacyjny
2	ćwiczenia laboratoryjne

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena wykonanych ćwiczeń laboratoryjnych	51%

Literatura podstawowa	
1	Stinson, Douglas R., Paterson Maura B. Kryptografia. W Teorii i Praktyce. Wyd. Naukowe PWN, 2021.
2	Aumasson, Jean-Philippe i in. Nowoczesna kryptografia : praktyczne wprowadzenie do szyfrowania. Wydanie I. Warszawa: PWN, 2018. Print.

Literatura uzupełniająca	
1	Laskowski, Maciej, Bezpieczeństwo systemów informatycznych. Politechnika Lubelska, 2013.
2	Laskowski, Maciej, Techniki Ochrony Informacji. Politechnika Lubelska, 2013.
3	Menezes, Alfred J i in. Kryptografia stosowana. Warszawa: Wydawnictwa Naukowo-Techniczne, 2005.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	60
Udział w wykładach:	30
Udział w zajęciach laboratoryjnych:	30
Praca własna studenta, w tym:	40
Studiowanie tematyki wykładów, przygotowanie do egzaminu:	25
Przygotowanie do zajęć laboratoryjnych:	15
Łączny czas pracy studenta	100
Sumaryczna liczba punktów ECTS dla przedmiotu	4

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W02+++ CB1A_W10+ CB1A_W15++	C1	W1 - W11	1	O1
EK 2	CB1A_W21+++	C1	W1 - W11	1	O1
EK 3	CB1A_U13++ CB1A_U24+++	C2	L1 - L11	2	O2

	CB1A_U12++				
EK 4	CB1A_U13++ CB1A_U24+++ CB1A_U12++	C2	L1 - L11	2	O2
EK 5	CB1A_K02++	C1, C2	W1 - W11 L1 - L11	1 - 2	O1, O2

Autor programu:	dr Michał Dolecki
Adres e-mail:	m.dolecki@pollub.pl
Jednostka organizacyjna:	Katedra Inteligencji Obliczeniowej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Podstawy uczenia maszynowego
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C405
Rok:	II
Semestr:	4
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	60
Wykład	30
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	5
Sposób zaliczenia:	egzamin
Język wykładowy:	język polski

Cele przedmiotu

C1	Zapoznanie z podstawowymi metodami uczenia maszynowego
C2	Nabycie praktycznej wiedzy z zakresu uczenia maszynowego i sztucznej inteligencji

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1	Znajomość podstaw algorytmiki i struktur danych
2	Podstawowe umiejętności programowania w językach algorytmicznych
3	Podstawowa znajomość algebry liniowej, analizy matematycznej, matematyki dyskretnej oraz statystyki

Efekty uczenia się

	W zakresie wiedzy:
EK 1	identyfikuje podstawowe modele uczenia maszynowego
EK 2	charakteryzuje własności i zastosowania wybranych modeli i pojęć z zakresu uczenia maszynowego i sztucznej inteligencji
	W zakresie umiejętności:
EK3	potrafi programować aplikacje w zakresie podstaw uczenia maszynowego
EK4	stosuje wybrane biblioteki w celu efektywnego tworzenia aplikacji w zależności od problemu
	W zakresie kompetencji społecznych:
EK5	jest gotów do podejmowania wyzwań związanych z wykorzystaniem narzędzi programistycznych i ich krytycznej oceny

Treści programowe przedmiotu

Forma zajęć - wykłady	
	Treści programowe
W1	Wprowadzenie do uczenia maszynowego. Definicja uczenia maszynowego. Typy uczenia maszynowego: nadzorowane, nienadzorowane, ze wzmocnieniem. Przegląd narzędzi i środowisk
W2	Przygotowanie danych. Zrozumienie danych: cechy, etykiety, brakujące wartości, wyciszanie szumu. Podział danych: zbiór treningowy, walidacyjny, testowy. Normalizacja, standaryzacja i inżynieria cech
W3	Uczenie nadzorowane. Regresja liniowa i logistyczna. Drzewa decyzyjne i las losowy. Algorytm k najbliższych sąsiadów. Maszyny wektorów nośnych
W4	Uczenie nienadzorowane. Klasteryzacja (K-means, hierarchiczna klasteryzacja). Redukcja wymiaru (PCA, LDA)
W5	Wprowadzenie do sieci neuronowych i uczenia głębokiego. Podstawy sieci neuronowych: perceptron, wielowarstwowy perceptron (MLP). Funkcje aktywacji. Trenowanie sieci neuronowych
W6	Ocena i optymalizacja modeli. Metryki jakości. Walidacja krzyżowa. Przeuczenie i regularyzacja. Dobór hiperparametrów
W7	Sieci konwolucyjne. Autoenkodery. Sieci typu GAN
W8	Zbiory rozmyte i ich zastosowania
W9	Optymalizacja. Algorytmy genetyczne. Optymalizacja rojem cząstek
W10	Etyka i odpowiedzialność w uczeniu maszynowym
Forma zajęć - laboratoria	
	Treści programowe
L1	Wstępne przetwarzanie danych
L2	Implementacja modeli uczenia nadzorowanego
L3	Implementacja modeli uczenia nienadzorowanego
L4	Implementacja sieci neuronowych. Uczenie głębokie
L5	Ocena i optymalizacja modeli
L6	Implementacja zaawansowanych architektur sieci neuronowych
L7	Zbiory rozmyte
L8	Optymalizacja modeli za pomocą algorytmów genetycznych i optymalizacji rojem cząstek (PSO)

Metody dydaktyczne	
1	wykład informacyjny
2	ćwiczenia laboratoryjne
3	metoda programowania z użyciem komputera

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%

O2	ocena wykonanych ćwiczeń laboratoryjnych	51%
----	--	-----

Literatura podstawowa	
1	Géron, Aurélien, Uczenie maszynowe z użyciem Scikit-Learn i TensorFlow, Helion, Gliwice 2020.

Literatura uzupełniająca	
1	Chollet F., Deep Learning. Praca z językiem Python i biblioteką Keras, Helion, Gliwice 2019.
2	Esposito, Dino, Esposito, Francesco, Wprowadzenie do uczenia maszynowego, APN Promise, Warszawa 2020.
3	Ponteves, Hadelin de, Sztuczna inteligencja : błyskawiczne wprowadzenie do uczenia maszynowego, uczenia ze wzmocnieniem i uczenia głębokiego, Helion 2021.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	60
Udział w wykładach:	30
Udział w zajęciach laboratoryjnych:	30
Praca własna studenta, w tym:	65
Studiowanie tematyki wykładów, przygotowanie do egzaminu:	38
Przygotowanie do zajęć laboratoryjnych:	27
Łączny czas pracy studenta	125
Sumaryczna liczba punktów ECTS dla przedmiotu	5

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W06++, CB1A_W19+++	C1, C2	W1-W10	1	O1
EK 2	CB1A_W06++, CB1A_W19+++	C1, C2	W1-W10	1	O1
EK 3	CB1A_U12++ CB1A_U22+++	C1, C2	L1-L8	2, 3	O2
EK 4	CB1A_U12++	C1, C2	L1-L8	2, 3	O2

	CB1A_U22+++				
EK 5	CB1A_K01+	C1, C2	W1-W10	1	O1

Autor programu:	dr hab. Paweł Karczmarek, profesor uczelni; mgr Alicja Żmudzińska; mgr Krystyna Kiersztyn; dr Konrad Smoliński; dr inż. Łukasz Gałka
Adres e-mail:	p.karczmarek@pollub.pl; a.zmudzinska@pollub.pl; k.kiersztyn@pollub.pl; k.smolinski@pollub.pl; l.galka@pollub.pl
Jednostka organizacyjna:	Katedra Inteligencji Obliczeniowej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
 Studia pierwszego stopnia

Przedmiot:	Bezpieczeństwo aplikacji webowych
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C406
Rok:	II
Semestr:	4
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	45
Wykład	15
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	3
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu

C1	Zrozumienie zagrożeń i podatności aplikacji internetowych
C2	Poznanie zasad projektowania bezpiecznych aplikacji
C3	Praktyczne wykorzystanie narzędzi do testowania bezpieczeństwa

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1	Znajomość fundamentalnych zagadnień związanych z bezpieczeństwem informacji
2	Umiejętność programowania aplikacji internetowych
3	Podstawowa wiedza z zakresu baz danych

Efekty uczenia się

	W zakresie wiedzy:
EK 1	identyfikuje najczęstsze zagrożenia bezpieczeństwa w aplikacjach internetowych
EK 2	wskazuje mechanizmy podnoszące poziom bezpieczeństwa aplikacji internetowych
	W zakresie umiejętności:
EK3	analizuje podatność aplikacji internetowych na wybrane zagrożenia
EK4	dobiera, projektuje i implementuje odpowiednie techniki ochrony aplikacji internetowych
	W zakresie kompetencji społecznych:
EK5	jest gotów postępować etycznie w obszarze bezpieczeństwa, promując odpowiedzialne i bezpieczne korzystanie z aplikacji internetowych oraz propagując dobre praktyki ochrony danych

Treści programowe przedmiotu

Forma zajęć - wykłady	
	Treści programowe
W1	Wprowadzenie do bezpieczeństwa aplikacji internetowych
W2	Przegląd OWASP Top 10. Omówienie najczęstszych zagrożeń. Przykłady rzeczywistych incydentów
W3	Ataki na warstwę serwerową i bazodanową
W4	Ataki na pliki i przesyłanie danych
W5	Zabezpieczenia na poziomie aplikacji i serwera
W6	Autoryzacja i uwierzytelnianie
W7	Bezpieczeństwo komunikacji w aplikacjach internetowych
Forma zajęć - laboratoria	
	Treści programowe
L1	Wprowadzenie do środowiska testowego. Konfiguracja stanowiska i omówienie zasad pracy
L2	Testowanie podatności XSS i sposoby zabezpieczania
L3	SQL Injection i ochrona przed atakami
L4	Ataki CSRF i implementacja zabezpieczeń
L5	Bezpieczeństwo plików i przesyłanych danych
L6	Zabezpieczenie uwierzytelniania i autoryzacji
L7	Ataki Man In The Middle i TLS Stripping
L8	Bezpieczna konfiguracja serwera i nagłówków HTTP
L9	Wykrywanie i analiza błędów aplikacji
L10	Wykorzystanie poznanych technik do przeprowadzenia audytu bezpieczeństwa aplikacji internetowej

Metody dydaktyczne	
1	wykład konwersatoryjny
2	ćwiczenia laboratoryjne
3	metoda programowania z użyciem komputera

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena aktywności w trakcie zajęć	51%
O3	ocena wykonanych ćwiczeń laboratoryjnych	51%

Literatura podstawowa	
1	Hoffman, Andrew i in. Bezpieczeństwo nowoczesnych aplikacji internetowych : przewodnik po zabezpieczeniach. Gliwice: Helion, 2021.
2	Miłosz, Marek, i Maciej Bąbol. Zagrożenia i ochrona aplikacji internetowych. Politechnika Lubelska, 2014.

3	Kozieł, Grzegorz i in. Bezpieczne aplikacje internetowe w PHP. Lublin: Wyd. Politechniki Lubelskiej, 2022.
---	--

Literatura uzupełniająca	
1	OWASP Top 10 – 2024, https://owasp.org/www-project-top-ten/ .
2	„Bezpieczeństwo aplikacji webowych”. Bezpieczeństwo aplikacji webowych - Securitum, r 2019, https://ksiazka.sekurak.pl/ .

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	45
Udział w wykładach:	15
Udział w zajęciach laboratoryjnych:	30
Praca własna studenta, w tym:	30
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	10
Przygotowanie do zajęć laboratoryjnych:	20
Łączny czas pracy studenta	75
Sumaryczna liczba punktów ECTS dla przedmiotu	3

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W17+++, CB1A_W10++ CB1A_W15++	C1	W1-W7	1	O1,O2
EK 2	CB1A_W10++, CB1A_W15++	C2	W3-W7	1	O1,O2
EK 3	CB1A_U11+++, CB1A_U13++	C1 ,C2	L8-L10	2	O2,O3
EK 4	CB1A_U24++	C1, C2, C3	L1-L10	2,3	O2,O3
EK 5	CB1A_K03+ CB1A_K05+	C1	W1-W7, L1-L10	1,2,3	O1,O2

Autor programu:	dr inż. Jakub Gęca
------------------------	--------------------

Adres e-mail:	j.geca@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Stosowanej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Socjotechniki i psychologia cyberprzestrzeni
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C407
Rok:	II
Semestr:	4
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	45
Wykład	30
Ćwiczenia	
Laboratorium	15
Projekt	
Liczba punktów ECTS:	3
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zrozumienie psychologicznych i socjologicznych mechanizmów wykorzystywanych w atakach socjotechnicznych
C2	Poznanie metod obrony przed manipulacją w cyberprzestrzeni
C3	Rozwinięcie umiejętności analizy zachowań użytkowników i ich podatności na zagrożenia cybernetyczne

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Znajomość podstawowych zagadnień z obszaru cyberbezpieczeństwa
2	Umiejętność krytycznego myślenia i analizy treści

Efekty uczenia się	
	W zakresie wiedzy:
EK1	zna i rozumie podstawowe mechanizmy psychologiczne i socjologiczne wpływające na zachowania użytkowników w cyberprzestrzeni
EK2	rozumie rolę socjotechnik w realizacji cyberataków oraz ich wpływ na bezpieczeństwo systemów informatycznych
	W zakresie umiejętności:
EK3	potrafi zidentyfikować techniki socjotechniczne stosowane w atakach
EK4	potrafi analizować przypadki incydentów związanych z manipulacją użytkowników w cyberprzestrzeni
EK5	potrafi zaprojektować kampanię edukacyjną mającą na celu zwiększenie świadomości użytkowników
	W zakresie kompetencji społecznych:

EK6	jest gotów do krytycznego oceniania treści i komunikatów otrzymywanych w środowisku cyfrowym
EK7	jest gotów do wypełniania zobowiązań społecznych w aspekcie podnoszenia świadomości społeczeństwa na temat zagrożeń socjotechnicznych

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Wprowadzenie do psychologii w kontekście jej historii, specjalizacji psychologicznych
W2	Psychologia rozwoju człowieka: zmiany w okresach dzieciństwa, adolescencji, dorosłości i starości
W3	Psychologia procesów poznawczych, relacje między afektem a poznaniem, poznanie społeczne. Dysonans poznawczy, samoocena i mechanizmy psychologiczne podtrzymujący pozytywny wizerunek własny
W4	Psychologia społeczna - główne zagadnienia, badane procesy. Psychologia wpływu społecznego: mechanizmy konformizmu, autorytaryzmu, nastroj a wpływ społeczny. Psychologia reklamy jako formy wpływu społecznego
W5	Wybrane neurofizjologiczne mechanizmy regulujące relacje grupowe, wpływ społeczny i schematy relacji interpersonalnych, wpływ podprogowy
W6	Człowiek w cyberprzestrzeni - główne zjawiska psychologiczne. Psychologia człowieka w środowisku cyfrowym - podstawowe mechanizmy
W7	Mechanizmy psychologiczne w cyberprzestrzeni. Psychologiczne aspekty podatności na manipulację
W8	Definicja socjotechnik i ich rola w cyberbezpieczeństwie. Główne techniki socjotechniczne stosowane w cyberatakach: phishing, vishing, smishing, spear phishing, fake news i dezinformacja
W9	Obrona przed socjotechnikami. Rozpoznawanie ataków socjotechnicznych. Budowanie świadomości użytkowników w zakresie zagrożeń
Forma zajęć - laboratoria	
	Treści programowe
L1	Sieć internetowa i media społecznościowe jako przestrzeń psychologiczna
L2	Sekwencyjne techniki wpływu społecznego
L3	Reklama polityczna i kreowanie wizerunku - metody, uwarunkowania skuteczności
L4	Kulturowe różnice w poziomie indywidualizmu i kolektywizmu a metody wpływu społecznego w Internecie
L5	Fake newsy i tzw. "fermy trolli" - zasady działania i główne cele
L6	Anonimowość w cyberprzestrzeni - mechanizmy i konsekwencje
L7	Phishing, Whaling & Whaling Phising
L8	Co wzmacnia "klikalność" i przyciąga uwagę użytkowników cyberprzestrzeni
L9	Specyfika wpływu społecznego i manipulacji cyberprzestrzeni państw autorytarnych - wpływ wewnętrzny i zewnętrzny
L10	Profil psychologiczny osoby podatnej na socjotechniki w cyberprzestrzeni

L11	Opracowanie prezentacji multimedialnej wspierającej kampanię zwiększającą świadomość użytkowników w aspekcie psychologii cyberprzestrzeni i ataków socjotechnicznych
------------	--

Metody dydaktyczne	
1	wykład informacyjny
2	analiza przypadków
3	ćwiczenia laboratoryjne
4	przygotowanie prezentacji

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena wykonanych ćwiczeń laboratoryjnych	51%
O3	ocena przygotowanej prezentacji	51%

Literatura podstawowa	
1	Doliński, Dariusz, Psychologia wpływu społecznego. Ossolineum, 2000.
2	Elliot, Aronson, i in., Psychologia społeczna. Zysk i Ska, 2006.
3	Wojciech, i in., Marketing polityczny. Perspektywa psychologiczna. GWP, 2006.
4	Jabłońska, Marta, Człowiek w cyberprzestrzeni Wprowadzenie do psychologii Internetu. Wyd. Uniwersytetu Łódzkiego, 2018.

Literatura uzupełniająca	
1	Suler, John, The psychology of cyberspace. The classic text. (online) https://www.johnsuler.com/pdfs/psycyber.pdf .
2	Suworow, Wiktor, Akwarium. Rebis, 2022.
3	Mohiuddin A. i in., Explainable Artificial Intelligence for Cyber Security: Next Generation Artificial Intelligence. Springer Nature, 2023.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	45
Udział w wykładach:	30
Udział w zajęciach laboratoryjnych:	15
Praca własna studenta, w tym:	30
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	20
Przygotowanie do zajęć laboratoryjnych:	10

Łączny czas pracy studenta	75
Sumaryczna liczba punktów ECTS dla przedmiotu	3

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W15+++	C1, C2	W1 - W7	1, 2	O1
EK 2	CB1A_W02++	C1, C2	W8 - W9	1, 2	O1
EK 3	CB1A_U01++ CB1A_U09++	C3	L5 - L11	3, 4	O2, O3
EK 4	CB1A_U01++ CB1A_U09++	C3	L1 - L11	3, 4	O2, O3
EK 5	CB1A_U05++	C3	L11	4	O3
EK 6	CB1A_K01++	C1 - C3	W1-W9, L1-L11	1 - 4	O1, O2, O3
EK 7	CB1A_K03+	C1 - C3	W1-W9, L1-L11	1 - 4	O1, O2, O3

Autor programu:	dr hab. inż. Kamil Jonak, profesor uczelni
Adres e-mail:	k.jonak@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Technicznej, Politechnika Lubelska

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Zarządzanie kryzysowe
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C408
Rok:	II
Semestr:	4
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	30
Wykład	15
Ćwiczenia	
Laboratorium	
Projekt	15
Liczba punktów ECTS:	2
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zapoznanie z podstawami systemu zarządzania kryzysowego w Polsce i jego znaczeniem w kontekście cyberzagrożeń
C2	Rozwijanie umiejętności przygotowania planów reagowania na incydenty i ciągłości działania w organizacjach.
C3	Kształtowanie kompetencji zespołowego podejmowania decyzji w warunkach kryzysowych

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Znajomość podstawowych zagadnień oraz regulacja prawnych z zakresu cyberbezpieczeństwa
2	Umiejętność analitycznego myślenia i pracy w grupie

Efekty uczenia się	
	W zakresie wiedzy:
EK1	zna i rozumie podstawy funkcjonowania systemu zarządzania kryzysowego w Polsce, w tym w aspekcie cyberzagrożeń
EK2	rozumie specyfikę sytuacji kryzysowych związanych z cyberatakami i incydentami w systemach informatycznych
	W zakresie umiejętności:
EK4	potrafi zidentyfikować zagrożenia oraz opracować prosty plan reagowania kryzysowego oraz uproszczony plan ciągłości działania
EK5	potrafi skutecznie komunikować się i współpracować z innymi uczestnikami działań w sytuacjach kryzysowych, uwzględniając znaczenie koordynacji i przepływu informacji

	W zakresie kompetencji społecznych:
EK8	jest gotów do odpowiedzialnego pełnienia ról zawodowych w sektorze bezpieczeństwa cyfrowego, podejmowania decyzji w sytuacjach kryzysowych oraz wspierania działań na rzecz ochrony infrastruktury krytycznej i zasobów cyfrowych organizacji

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Wprowadzenie do zarządzania kryzysowego. Rodzaje i etapy sytuacji kryzysowych
W2	System zarządzania kryzysowego w Polsce: struktura, kompetencje, akty prawne
W3	Planowanie kryzysowe: dokumenty, procedury, koordynacja międzyinstytucjonalna
W4	Zarządzanie kryzysem cyberbezpieczeństwa: typowe zagrożenia i scenariusze incydentów
W5	Podstawy planowania: plany reagowania na incydenty (IRP), plany ciągłości działania (BCP)
W6	Komunikacja kryzysowa: zarządzanie informacją, kontakty z mediami, reakcja organizacyjna
W7	Zarządzanie kryzysowe w instytucjach i firmach – podejście organizacyjne i praktyczne
Forma zajęć - projekt	
	Treści programowe
P1	Opracowanie scenariusza sytuacji kryzysowej i przygotowanie planu reagowania
P2	Identyfikacja zagrożeń, analiza wpływu i ocena ryzyka
P3	Opracowanie IRP – planu reagowania na incydent
P4	Przygotowanie uproszczonego planu ciągłości działania (BCP)
P5	Symulacja sytuacji kryzysowej i praca zespołowa – podejmowanie decyzji, rozdział ról

Metody dydaktyczne	
1	wykład informacyjny
2	analiza przypadków
3	metoda projektu
4	praca wykonywana w grupach

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena przygotowanego projektu	51%
O3	ocena aktywności w trakcie zajęć	51%

Literatura podstawowa	
1	Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym Dz.U. 2007 nr 89 poz. 590
2	Grocki, Romuald, Zarządzanie kryzysowe : dobre praktyki. Wydanie II. Wydawnictwo Difin, 2020.
3	Wiśniewski, Bernard i in. Podejmowanie decyzji w sytuacjach kryzysowych. Wydawnictwo Wyższej Szkoły Policji w Szczytnie. 2017.
4	Chalubinska-Jentkiewicz, Katarzyna, Modele rozwiązań prawnych w systemie cyberbezpieczeństwa. Wydawnictwo Towarzystwa Wiedzy Obronne. 2021.

Literatura uzupełniająca	
1	Tworzydło, Dariusz, Komunikowanie organizacji w kryzysie : modele i metody ograniczania ryzyka. Wydanie I. Wydawnictwo Naukowe PWN SA, 2022.
2	Skomra, Witold, Panowanie nad ryzykiem w ramach publicznego zarządzania kryzysowego. Wydanie I. BEL Studio, 2018.
3	Pietrek, Grzegorz, System zarządzania kryzysowego. Diagnoza i kierunki doskonalenia. Wydawnictwo Difin, 2018.
4	Lebiedź, Jacek, Krztoń, Waldemar, Stefaniuk, Barbara, Współczesne wyzwania bezpieczeństwa narodowego – Zarządzanie kryzysowe, wojna informacyjna w cyberprzestrzeni, rzeczywistość wirtualna. Wydawnictwo naukowe TEXTER, 2018.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	30
Udział w wykładach:	15
Udział w zajęciach projektowych:	15
Praca własna studenta, w tym:	20
Studiowanie tematyki wykładów, przygotowanie do zaliczenia:	10
Przygotowanie projektu:	10
Łączny czas pracy studenta	50
Sumaryczna liczba punktów ECTS dla przedmiotu	2

Macierz efektów uczenia się					
Symbol przedmiotowe go efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny

EK 1	CB1A_W13+++ CB1A_W14++	C1	W1 - W7	1	O1
EK 2	CB1A_W15++	C1	W1 - W7	1, 2	O1
EK 3	CB1A_U01++ CB1A_U20++ CB1A_U23+++	C2	P1 - P5	2 - 4	O2, O3
EK 4	CB1A_U03+++	C3	P1 - P5	2 - 4	O2, O3
EK 5	CB1A_K05+++	C1 - C3	W1 - W7, P1 - P5	1 - 4	O1 - O3

Autor programu:	dr inż. Stanisław Sulenta, mgr inż. Aleksandra Prus
Adres e-mail:	s.sulenta@pollub.pl, a.prus@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Technicznej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Analiza złośliwego oprogramowania
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C501
Rok:	III
Semestr:	5
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	45
Wykład	15
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	3
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu

C1	Poznanie metod analizy złośliwego oprogramowania
C2	Poznanie narzędzi i zasad analizy złośliwego oprogramowania
C3	Nabywanie umiejętności analizy złośliwego oprogramowania

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1	Wiedza i umiejętności z zakresu administrowania systemów operacyjnych
2	Umiejętności konfiguracji systemów operacyjnych lokalnych i w chmurze
3	Wiedza z zakresu kontroli procesów w systemie operacyjnym

Efekty uczenia się

	W zakresie wiedzy:
EK 1	zna i rozumie wybrane metody diagnozowania, analizy oraz oceny ryzyka związanego z występowaniem zagrożeń w cyberprzestrzeni, w tym także zasad monitorowania sieci teleinformatycznych i reagowania na incydenty bezpieczeństwa
EK 2	wskazuje metody i narzędzia służące do analizy złośliwego oprogramowania oraz techniki informatyki śledczej
	W zakresie umiejętności:
EK 3	szacuje analizę ryzyka w kontekście bezpieczeństwa systemu informatycznego
EK 4	wykorzystuje metody analityczne, symulacyjne oraz eksperymentalne do analizy złośliwego oprogramowania
	W zakresie kompetencji społecznych:
EK 5	jest gotów do odpowiedzialnego pełnienia ról zawodowych w sektorze cyberbezpieczeństwa, rozumiejąc znaczenie etycznych standardów specjalisty oraz

	dbając o stworzenie kultury odpowiedzialności w swoim otoczeniu zawodowym, angażuje się w działania promujące profesjonalizm i odpowiedzialność w obszarze cyberbezpieczeństwa
--	--

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Klasyfikacja złośliwego oprogramowania
W2	Funkcjonalność i cele złośliwego oprogramowania
W3	Systemy narażone na złośliwe oprogramowanie, furtki
W4	Statyczna analiza złośliwego oprogramowania
W5	Dynamiczna analiza złośliwego oprogramowania
W6	Hybrydowa analiza złośliwego oprogramowania
W7	Analiza właściwości statycznych
W8	Interaktywna analiza zachowania
W9	Analiza w pełni zautomatyzowana
W10	Inżynieria wsteczna kodu
Forma zajęć - laboratoria	
	Treści programowe
L1	Narzędzia do analizy złośliwego oprogramowania. Zasady bezpieczeństwa
L2	Analiza statyczna i dynamiczna
L3	Konfigurowanie piaskownicy lokalnej i w chmurze
L4	Pozyskiwanie złośliwego oprogramowania
L5	Sprawdzanie właściwości statycznych
L6	Monitorowanie zachowania złośliwego oprogramowania
L7	Analiza ruchu sieciowego
L8	Deasemblacja i dekompilacja
L9	Opracowanie raportu
L10	Analiza przypadków złośliwego oprogramowania

Metody dydaktyczne	
1	wykład informacyjny
2	ćwiczenia laboratoryjne
3	analiza przypadków

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena przygotowanej prezentacji	51%
O2	ocena wykonanych ćwiczeń laboratoryjnych	51%
O3	ocena wykonanych sprawozdań laboratoryjnych	51%

Literatura podstawowa	
1	Bravo, Cesar. Cyberbezpieczeństwo dla zaawansowanych: skuteczne zabezpieczenia systemu Windows, Linux, IoT i infrastruktury w chmurze. Helion, 2023.
2	DiMaggio, Jon. Sztuka wojny cyfrowej. Przewodnik dla śledczego po szpiegostwie, oprogramowaniu ransomware i cyberprzestępczości zorganizowanej. Helion, 2023.
3	Troia, Vinny. Upoluj cyberprzestępcę. Przewodnik dla hakerów prowadzących śledztwa online. Helion, 2022.

Literatura uzupełniająca	
1	Diogenes, Yuri, Ozkaya, Erdal. Cyberbezpieczeństwo - strategie ataku i obrony. Jak osiągnąć najwyższy możliwy stan zabezpieczeń systemu informatycznego. Helion, 2023.
2	Johansen, Gerard. Informatyka śledcza. Narzędzia i techniki skutecznego reagowania na incydenty bezpieczeństwa. Helion, 2024.
3	Parasram, Shiva V. N. Informatyka śledcza i Kali Linux. Przeprowadź analizy nośników pamięci, ruchu sieciowego i zawartości RAM-u za pomocą narzędzi systemu Kali Linux 2022.x. Helion, 2024.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	45
Udział w wykładach:	15
Udział w zajęciach laboratoryjnych:	30
Praca własna studenta, w tym:	30
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	10
Przygotowanie do zajęć laboratoryjnych:	20
Łączny czas pracy studenta	75
Sumaryczna liczba punktów ECTS dla przedmiotu	3

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W04+++	C1	W1-W10	1	O1
EK 2	CB1A_W18+++	C1	W1-W10	1	O1

EK 3	CB1A_U11++	C2, C3	L1-L4	2, 3	O2, O3
EK 4	CB1A_U12+++	C2, C3	L1-L4	2, 3	O2, O3
EK 5	CB1A_K05+	C1-C3	W1-W10, L1-L4	1, 2, 3	O1-O3

Autor programu:	dr inż. Michał Charlak
Adres e-mail:	m.charlak@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Stosowanej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Systemy IoT: infrastruktura, aplikacje i bezpieczeństwo
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C502
Rok:	III
Semestr:	5
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	60
Wykład	30
Ćwiczenia	
Laboratorium	
Projekt	30
Liczba punktów ECTS:	4
Sposób zaliczenia:	egzamin
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zapoznanie z infrastrukturą i zastosowaniami Internetu Rzeczy (IoT)
C2	Zapoznanie z zagrożeniami bezpieczeństwa w systemach IoT
C3	Rozwinięcie umiejętności projektowania i implementacji zabezpieczeń w urządzeniach i sieciach IoT

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Wiedza z zakresu sieci komputerowych
2	Umiejętność programowania w co najmniej jednym języku programowania
3	Podstawowa wiedza z zakresu kryptografii i bezpieczeństwa informatycznego

Efekty uczenia się	
	W zakresie wiedzy:
EK1	zna architekturę i technologie stosowane w IoT
EK2	rozumie zasady komunikacji i integracji urządzeń IoT
EK3	zna zagrożenia związane z bezpieczeństwem IoT i metody ich minimalizacji
	W zakresie umiejętności:
EK4	potrafi zaprojektować i wdrożyć system IoT, dobierając odpowiednie technologie komunikacyjne oraz komponenty sprzętowe
EK5	potrafi ocenić przydatność wykorzystania wybranych rozwiązań sprzętowych i programowych do rozwiązywania zadań inżynierskich, polegających na budowie wydajnych i bezpiecznych systemów IoT

EK6	potrafi pracować indywidualnie oraz w zespole, aktywnie uczestnicząc w realizacji zadań związanych z bezpieczeństwem systemów IoT
	W zakresie kompetencji społecznych:
EK8	jest gotów do myślenia i działania w sposób przedsiębiorczy, przewidując konsekwencje naruszeń bezpieczeństwa systemów IoT w organizacji

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Definicja i historia Internetu Rzeczy. Kluczowe technologie i komponenty IoT
W2	Modele architektoniczne IoT (warstwa sprzętowa, sieciowa i aplikacyjna)
W3	Standardy i protokoły IoT (MQTT, CoAP, HTTP, LoRaWAN, ZigBee, BLE)
W4	Platformy sprzętowe IoT (Arduino, Raspberry Pi, ESP32, STM32)
W5	Sieci IoT: komunikacja urządzeń i wymiana danych. Chmura obliczeniowa i przetwarzanie brzegowe w IoT
W6	Aplikacje i zastosowania IoT, m.in. IoT w przemyśle (Przemysł 4.0, SCADA, automatyka), inteligentne miasta i domy (Smart Home, Smart Grid), logistyka i transport z wykorzystaniem IoT
W7	Wyzwania związane z bezpieczeństwem systemów IoT. Przegląd zagrożeń i ataków na urządzenia IoT
W8	Zastosowania kryptografii w IoT. Metody szyfrowania i zabezpieczenia komunikacji w IoT
W9	Bezpieczne uwierzytelnianie i autoryzacja urządzeń IoT
W10	Strategie reagowania na incydenty w systemach IoT
W11	Przyszłość bezpieczeństwa IoT. Rozwój technologii. Integracja IoT z AI i jej konsekwencje dla bezpieczeństwa
Forma zajęć - projekt	
	Treści programowe
P1	Analiza możliwych tematów projektowych (np. inteligentne czujniki, monitorowanie środowiska, systemy automatyki domowej, IoT w przemyśle). Określenie celów systemu i kluczowych funkcji. Identyfikacja głównych wymagań sprzętowych, komunikacyjnych i bezpieczeństwa
P2	Analiza i wybór odpowiedniego sprzętu (np. ESP32, Raspberry Pi, STM32, Arduino). Wybór czujników i aktuatorów (np. temperatura, detekcja ruchu, NFC, itp.). Określenie technologii komunikacyjnej
P3	Implementacja warstwy sprzętowej: montaż urządzeń i czujników, konfiguracja mikrokontrolerów, programowanie podstawowej funkcjonalności urządzeń IoT, testowanie poprawności działania sprzętu i komunikacji
P4	Programowanie i konfiguracja transmisji danych: implementacja komunikacji między urządzeniami IoT a serwerem/chmurą, konfiguracja protokołów komunikacyjnych, zarządzanie danymi – zbieranie, filtrowanie, przesyłanie i przechowywanie, testowanie poprawności transmisji i analizy wydajności
P5	Przetwarzanie i analiza danych IoT w chmurze lub na urządzeniach brzegowych: integracja systemu IoT z bazą danych lub chmurą obliczeniową,

	wizualizacja danych w czasie rzeczywistym, tworzenie interfejsu użytkownika
P6	Zabezpieczenie systemu IoT: implementacja metod uwierzytelniania i kontroli dostępu do urządzeń, zabezpieczenie transmisji danych, wykrywanie i ochrona przed atakami na urządzenia IoT
P7	Testowanie działania systemu i ocena zgodności z założeniami

Metody dydaktyczne	
1	wykład informacyjny
2	analiza przypadków
3	metoda projektu
4	praca wykonywana w grupach

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena przygotowanego projektu	51%
O3	obserwacja pracy studenta	51%

Literatura podstawowa	
1	Sikorski, Marcin, Internet Rzeczy. Wyd. Naukowe PWN, 2020.
2	Bravo, Cesar, Cyberbezpieczeństwo dla zaawansowanych. Skuteczne zabezpieczenia systemu Windows, Linux, IoT i infrastruktury w chmurze. Wyd. Helion, 2023.
3	Stallings, William, i in., Bezpieczeństwo systemów informatycznych. Zasady i praktyka. Tom 1 i 2. Wyd. Helion, 2023.
4	Buchwald, Paweł, i in., Internet Rzeczy i jego przemysłowe zastosowania. Polskie Wyd. Ekonomiczne, 2022.

Literatura uzupełniająca	
1	Krawiec, Jerzy, Internet Rzeczy (IoT). / problemy cyberbezpieczeństwa. Wyd. Politechniki Warszawskiej, 2020.
2	Wytrębowski, Jacek, i in., Inżynieria systemów internetu rzeczy. Zagadnienia bezpieczeństwa i komunikacji. Oficyna wydawnicza Politechniki Warszawskiej, 2020.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	60
Udział w wykładach:	30
Udział w zajęciach projektowych:	30
Praca własna studenta, w tym:	40
Studiowanie tematyki wykładów, przygotowanie	25

do egzaminu:	
Przygotowanie projektu:	15
Łączny czas pracy studenta	100
Sumaryczna liczba punktów ECTS dla przedmiotu	4

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W03+++	C1	W1 - W6, W11	1	O1
EK 2	CB1A_W03+++ CB1A_W09++	C1	W1 - W6	1	O1
EK 3	CB1A_W15++	C2	W7 - W11	1	O1
EK 4	CB1A_U12+++	C3	P1 - P5, P7	2 - 4	O2, O3
EK 5	CB1A_U12+++ CB1A_U19++	C3	P6, P7	2 - 4	O2, O3
EK 6	CB1A_U03++	C3	P1 - P7	3 - 4	O2, O3
EK 7	CB1A_K04+	C1, C2, C3	W1-W7, P1-P7	1 - 4	O1, O2, O3

Autor programu:	mgr inż. Jacek Zaburko; dr inż. Piotr Krupski
Adres e-mail:	j.zaburko@pollub.pl; p.krupski@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Technicznej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Kryminalistyka komputerowa
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C503
Rok:	III
Semestr:	5
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	60
Wykład	30
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	4
Sposób zaliczenia:	egzamin
Język wykładowy:	język polski

Cele przedmiotu	
C1	Poznanie metod i narzędzi służących do analizy zagrożeń oraz technik wykorzystywanych w informatyce śledczej
C2	Uzyskanie umiejętności identyfikowania, analizowania i oceniania incydentów bezpieczeństwa informacyjnego, a także mechanizmów prowadzących do manipulacji użytkowników i naruszenia bezpieczeństwa
C3	Nabywanie kompetencji odpowiedzialnego pełnienia ról zawodowych w sektorze cyberbezpieczeństwa i przestrzegania zasad etyki zawodowej

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Umiejętność administrowania systemami operacyjnymi
2	Zaawansowane umiejętności administrowania sieciami komputerowymi
3	Wiedza i umiejętności zarządzania incydentami bezpieczeństwa

Efekty uczenia się	
	W zakresie wiedzy:
EK 1	charakteryzuje metody i narzędzia służące do analizy zagrożeń oraz techniki informatyki śledczej
EK 2	rozróżnia sposoby oraz metody przetwarzania obrazów cyfrowych, jak również strumieni audio i video, co stanowi podstawę do analizy, ochrony i zabezpieczania danych
	W zakresie umiejętności:
EK 3	identyfikuje, analizuje oraz ocenia incydenty bezpieczeństwa informacyjnego, a także mechanizmy prowadzące do manipulacji użytkowników i naruszenia bezpieczeństwa

EK 4	przedstawia otrzymane wyniki realizacji zadania inżynierskiego wykorzystując różnorodne narzędzia oraz potrafi dokonać oceny, poprawnej interpretacji oraz wyciągnąć wnioski
EK 5	potrafi przy identyfikowaniu problemów związanych z zapewnieniem cyberbezpieczeństwa oraz rozwiązywaniu tych zadań, dostrzec i uwzględnić ich aspekty systemowe i pozatechniczne, w tym aspekty etyczne
	W zakresie kompetencji społecznych:
EK 6	jest gotów do odpowiedzialnego pełnienia ról zawodowych w sektorze bezpieczeństwa cyfrowego, przestrzegania zasad etyki zawodowej, rozumiejąc znaczenie etycznych standardów specjalisty ds. cyberbezpieczeństwa

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Wprowadzenie do kryminalistyki cyfrowej
W2	Techniki śledcze w odzyskiwaniu usuniętych lub brakujących danych
W3	Metodologia i procedury w informatyce śledczej, regulacje prawne
W4	Metody i techniki kryminalistyki cyfrowej w zabezpieczaniu infrastruktury
W5	Platformy kryminalistyczne
W6	Źródła danych
W7	Kryminalistyka urządzeń mobilnych
W8	Zarządzanie materiałem dowodowym
Forma zajęć - laboratoria	
	Treści programowe
L1	Porównanie systemów operacyjnych dla informatyki śledczej
L2	Systemy plików i nośniki pamięci masowej
L3	Dane ulotne i nieulotne oraz kolejność gromadzenia dowodów cyfrowych
L4	Pamięć RAM oraz plik stronicowania i pamięć podręczna w dochodzeniach DFIR
L5	Funkcjonalna metoda dochodzenia cyfrowego
L6	Zbieranie dowodów sieciowych
L7	Pozyskiwanie dowodów opartych na hoście
L8	Zdalne gromadzenie dowodów
L9	Obrazowanie kryminalistyczne
L10	Tworzenie raportu o incydencie

Metody dydaktyczne	
1	wykład informacyjny
2	dyskusja dydaktyczna
3	ćwiczenia laboratoryjne
4	analiza przypadków

Metody i kryteria oceny

Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena wykonanych ćwiczeń laboratoryjnych	51%
O3	ocena wykonanych sprawozdań laboratoryjnych	51%

Literatura podstawowa	
1	Johansen, Gerard. Informatyka śledcza. Narzędzia i techniki skutecznego reagowania na incydenty bezpieczeństwa. Helion, 2024.
2	Hayes, Darren R. Informatyka w kryminalistyce. Praktyczny przewodnik. Helion 2021.
3	Parasram, Shiva V. N. Informatyka śledcza i Kali Linux. Przeprowadź analizy nośników pamięci, ruchu sieciowego i zawartości RAM-u za pomocą narzędzi systemu Kali Linux 2022.x. Helion, 2024.

Literatura uzupełniająca	
1	DiMaggio, Jon. Sztuka wojny cyfrowej. Przewodnik dla śledczego po szpiegostwie, oprogramowaniu ransomware i cyberprzestępczości zorganizowanej. Helion, 2023.
2	Bravo, Cesar. Cyberbezpieczeństwo dla zaawansowanych. Skuteczne zabezpieczenia systemu Windows, Linux, IoT i infrastruktury w chmurze. Helion, 2023.
3	Troia, Vinny. Upoluj cyberprzestępcę. Przewodnik dla hakerów prowadzących śledztwa online. Helion, 2022.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	60
Udział w wykładach:	30
Udział w zajęciach laboratoryjnych:	30
Praca własna studenta, w tym:	40
Studiowanie tematyki wykładów, przygotowanie do egzaminu:	25
Przygotowanie do zajęć laboratoryjnych:	15
Łączny czas pracy studenta	100
Sumaryczna liczba punktów ECTS dla przedmiotu	4

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny

	wraz z określeniem stopnia powiązania				
EK 1	CB1A_W18+++	C1, C3	W1-W8	1, 2	O1
EK 2	CB1A_W11+++	C1, C3	W1-W8	1, 2	O1
EK 3	CB1A_U23+++	C1-C3	L1-L10	3, 4	O2, O3
EK 4	CB1A_U04+++	C1-C3	L1-L10	3, 4	O2, O3
EK 5	CB1A_U09++	C1-C3	L1-L10	3, 4	O2, O3
EK 6	CB1A_K05+	C1-C3	W1-W8; L1-L10	1 - 4	O1-O3

Autor programu:	dr inż. Michał Charlak
Adres e-mail:	m.charlak@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Stosowanej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Wykrywanie incydentów bezpieczeństwa
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C504
Rok:	III
Semestr:	5
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	30
Wykład	15
Ćwiczenia	
Laboratorium	15
Projekt	
Liczba punktów ECTS:	2
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu

C1	Zapoznanie z definicjami, klasyfikacjami i cyklem życia incydentów bezpieczeństwa
C2	Poznanie technik rozpoznawania i analizy incydentów bezpieczeństwa
C3	Nabywanie umiejętności praktycznych w zakresie reagowania na incydenty oraz dokumentowania ich przebiegu

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1	Wiedza na temat architektury komputerów, systemów operacyjnych i sieci komputerowych
2	Znajomość podstawowych pojęć związanych z bezpieczeństwem informacji, takich jak poufność, integralność i dostępność
3	Wiedza na temat różnych typów zagrożeń (np. malware, phishing, DDoS) oraz metod ataków

Efekty uczenia się

	W zakresie wiedzy:
EK 1	definiuje i rozróżnia wybrane metody diagnozowania, analizy oraz oceny ryzyka związanego z występowaniem zagrożeń w cyberprzestrzeni
EK 2	zna zasady monitorowania sieci teleinformatycznych do identyfikacji anomalii i potencjalnych incydentów bezpieczeństwa
	W zakresie umiejętności:
EK3	posiada praktyczne umiejętności w zakresie reagowania na incydenty oraz dokumentowania ich przebiegu

EK4	dobiera odpowiednie narzędzia i techniki do identyfikacji potencjalnych incydentów bezpieczeństwa
	W zakresie kompetencji społecznych:
EK5	jest gotów do wypełniania zobowiązań społecznych, dzieląc się wiedzą na temat ochrony przed cyberzagrożeniami i promując kulturę bezpieczeństwa w środowisku cyfrowym, zarówno w organizacji, jak i w społeczności

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Wprowadzenie do incydentów bezpieczeństwa
W2	Metody wykrywania incydentów
W3	Analiza incydentów
W4	Reagowanie na incydenty
W5	Dokumentacja incydentów
W6	Przypadki incydentów w rzeczywistości
W7	Przyszłość wykrywania incydentów
Forma zajęć - laboratoria	
	Treści programowe
L1	Wprowadzenie do narzędzi wykrywania incydentów bezpieczeństwa
L2	Praktyczne ćwiczenia z analizy logów systemowych i aplikacyjnych
L3	Tworzenie i analiza symulowanych incydentów bezpieczeństwa
L4	Praktyczne ćwiczenia w zakresie reagowania na incydenty
L5	Tworzenie raportów z incydentów na podstawie przeprowadzonych ćwiczeń
L6	Praca nad rzeczywistymi przypadkami incydentów bezpieczeństwa
L7	Zaawansowane techniki analizy z użyciem narzędzi do wykrywania incydentów bezpieczeństwa

Metody dydaktyczne	
1	wykład informacyjny
2	analiza przypadków
3	ćwiczenia laboratoryjne
4	metoda programowania z użyciem komputera

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	obserwacja pracy studenta	51%
O3	ocena wykonanych sprawozdań laboratoryjnych	51%

Literatura podstawowa

1	Tanner, Nadean H., i in. Blue team i cyberbezpieczeństwo : zestaw narzędzi dla specjalistów od zabezpieczeń w sieci. Helion, 2021.
2	Troncone, Paul, i in. Cyberbezpieczeństwo w bashu : jak za pomocą wiersza poleceń prowadzić działania zaczepne i obronne. Helion SA, 2022.
3	Banasiński, Cezary, i in. Cyberbezpieczeństwo. Wolters Kluwer, 2020.

Literatura uzupełniająca	
1	Dela, Piotr, i in. Założenia działań w cyberprzestrzeni. PWN, 2022.
2	Bravo, Cesar, i in. Cyberbezpieczeństwo dla zaawansowanych : skuteczne zabezpieczenia systemu Windows, Linux, IoT i infrastruktury w chmurze. Helion, 2023.
3	El Ghamari, Magdalena, "Ochrona cyberprzestrzeni – wyzwanie naszych czasów?", Safety & fire technology, 2018 (49).

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	30
Udział w wykładach:	15
Udział w zajęciach laboratoryjnych:	15
Praca własna studenta, w tym:	20
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	10
Przygotowanie do zajęć laboratoryjnych:	10
Łączny czas pracy studenta	50
Sumaryczna liczba punktów ECTS dla przedmiotu	2

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W04++	C1, C2	W1-W7	1	O1
EK 2	CB1A_W11++ CB1A_W18++	C2, C3	W1-W7	1	O1
EK 3	CB1A_U12+++	C3	L1-L7	2 - 4	O2, O3
EK 4	CB1A_U21++	C2, C3	L1-L7	2 - 4	O2, O3
EK 5	CB1A_K03+	C3	W1, L4-L6	1 - 4	O1, O2, O3

Autor programu:	dr inż. Marek B. Horyński
Adres e-mail:	m.horynski@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Stosowanej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Testy penetracyjne
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C505
Rok:	III
Semestr:	5
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	60
Wykład	15
Ćwiczenia	
Laboratorium	30
Projekt	15
Liczba punktów ECTS:	4
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu

C1	Zapoznanie z podstawami testów penetracyjnych oraz ich rolą w procesie zarządzania bezpieczeństwem informatycznym
C2	Wykształcenie umiejętności przeprowadzania testów penetracyjnych z wykorzystaniem profesjonalnych narzędzi i technik
C3	Wykształcenie umiejętności identyfikacji i analizy podatności na ataki w systemach informatycznych
C4	Rozwinięcie umiejętności dokumentowania wyników testów i formułowania zaleceń naprawczych

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1	Wiedza z zakresu sieci komputerowych i systemów operacyjnych
2	Znajomość podstawowych narzędzi z zakresu bezpieczeństwa IT
3	Umiejętność pracy w trybie wiersza poleceń (Linux/Windows)

Efekty uczenia się

	W zakresie wiedzy:
EK1	zna wybrane techniki i potrzeby przeprowadzania testów penetracyjnych
EK2	rozumie zasady działania popularnych narzędzi do testowania bezpieczeństwa
EK3	zna przepisy prawne i etyczne dotyczące przeprowadzania testów penetracyjnych
	W zakresie umiejętności:
EK4	potrafi przeprowadzić analizę podatności i test penetracyjny wybranego systemu lub aplikacji
EK5	potrafi posługiwać się narzędziami do testów penetracyjnych

EK6	potrafi przygotować raport z testów penetracyjnych i przedstawić rekomendacje
	W zakresie kompetencji społecznych:
EK7	jest gotów do przeprowadzania testów penetracyjnych systemów informatycznych z poszanowaniem norm prawnych i etycznych

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Wprowadzenie do testów penetracyjnych. Definicja, cele, typy testów penetracyjnych. Proces pentestingu: planowanie, wykonanie, raportowanie
W2	Przepisy prawne i etyka testów penetracyjnych
W3	Metodologia testów penetracyjnych
W4	Ataki na środowiska aplikacyjne. Ataki na systemy sieci bezprzewodowych
W5	Przegląd technologii i narzędzi do testów penetracyjnych (zasada działania, struktura, wykorzystanie)
Forma zajęć - laboratoria	
	Treści programowe
L1	Podstawy korzystania z narzędzi do testów penetracyjnych
L2	Przeprowadzanie testów penetracyjnych w infrastrukturze IT
L3	Testy podatności aplikacji webowych
L4	Testy penetracyjne urządzeń i aplikacji mobilnych
L5	Ataki na infrastrukturę sieci bezprzewodowych
Forma zajęć - projekt	
	Treści programowe
P1	Wybór obszaru do testów penetracyjnych
P2	Przeprowadzenie testów wybranego systemu/aplikacji
P3	Przygotowanie raportu z testów i prezentacja wyników

Metody dydaktyczne	
1	wykład informacyjny
2	ćwiczenia laboratoryjne
3	metoda projektu
4	przygotowanie sprawozdania

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena wykonanych ćwiczeń laboratoryjnych	51%
O3	ocena przygotowanego projektu	51%

Literatura podstawowa

1	Hickey, Matthew, i in., Warsztat hakera. Testy penetracyjne i inne techniki wykrywania podatności. Wyd. Helion, 2022.
2	Forshaw, James, Atak na sieć okiem hakera. Wykrywanie i eksploatacja luk w zabezpieczeniach sieci. Wyd. Helion, 2019.
3	Messier, Rick, Kali Linux: testy bezpieczeństwa, testy penetracyjne i etyczne hakowanie. Wyd. Helion, 2019.
4	Weidman, Georgia, Bezpieczny system w praktyce. Wyższa szkoła hackingu i testy penetracyjne. Wyd. Helion, 2015.

Literatura uzupełniająca	
1	Khawaja, Gus, Kali Linux i testy penetracyjne. Wyd. Helion, 2022.
2	Bentkowski, Michał, i in., Bezpieczeństwo aplikacji webowych. Wyd. SECURITUM, 2019.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	60
Udział w wykładach:	15
Udział w zajęciach laboratoryjnych:	30
Udział w zajęciach projektowych:	15
Praca własna studenta, w tym:	40
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	10
Przygotowanie do zajęć laboratoryjnych:	20
Przygotowanie projektu:	10
Łączny czas pracy studenta	100
Sumaryczna liczba punktów ECTS dla przedmiotu	4

Macierz efektów uczenia się					
Symbol przedmiotowe go efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W04+++	C1	W1, W3, W4	1	O1
EK 2	CB1A_W12+++ CB1A_W04+++	C1	W1, W5	1	O1
EK 3	CB1A_W07++	C1	W2	1	O1
EK 4	CB1A_U21+++	C2, C3	L2 - L5, P1 - P2	2, 3	O2, O3

EK 5	CB1A_U06++	C2, C3	L1 - L5, P1 - P2	2, 3	O2, O3
EK 6	CB1A_U05++	C4	P3	3, 4	O3
EK 7	CB1A_K05++	C1 - C4	W1 - W5, L1 - L5, P1 - P3	1 - 4	O1, O2, O3

Autor programu:	mgr inż. Jacek Zaburko; dr inż. Joanna Szulzyk-Cieplak
Adres e-mail:	j.zaburko@pollub.pl; j.szulzyk-cieplak@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Technicznej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Najnowsze trendy w sztucznej inteligencji
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C506.1
Rok:	III
Semestr:	5
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	45
Wykład	45
Ćwiczenia	
Laboratorium	
Projekt	
Liczba punktów ECTS:	3
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu

C1	Zapoznanie z najnowszymi osiągnięciami w dziedzinie sztucznej inteligencji, w tym technologiami i algorytmami
C2	Zdobycie wiedzy teoretycznej związanych z aktualnymi trendami w sztucznej inteligencji

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1	Znajomość narzędzi programistycznych do tworzenia aplikacji związanych ze sztuczną inteligencją
2	Znajomość podstawowych algorytmów uczenia maszynowego
3	Znajomość podstawowych zagadnień ze sztucznej inteligencji

Efekty uczenia się

	W zakresie wiedzy:
EK 1	potrafi wymienić i szczegółowo opisać najnowsze osiągnięcia i trendy w sztucznej inteligencji, takie jak głębokie uczenie, przetwarzanie języka naturalnego (NLP), uczenie maszynowe, rozpoznawanie obrazów oraz uczenie ze wzmocnieniem
EK 2	ma wiedzę na temat klasycznych i nowoczesnych algorytmów stosowanych w SI, takich jak sieci neuronowe (CNN, RNN, GAN), transformery, i inne zaawansowane techniki
	W zakresie kompetencji społecznych:
EK3	jest gotów do odpowiedzialnego pełnienia ról zawodowych rozumiejąc znaczenie odpowiedzialnego wykorzystania sztucznej inteligencji w kontekście etycznym, społecznym i prawnym

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Wprowadzenie do współczesnej sztucznej inteligencji i krytyczna analiza metod
W2	Omówienie aktualnych trendów
W3	Wybrane zastosowania
W4	Etyka i odpowiedzialność w sztucznej inteligencji
W5	Perspektywy rozwoju i przyszłość sztucznej inteligencji

Metody dydaktyczne	
1	wykład informacyjny

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%

Literatura podstawowa	
1	Francois Chollet, Deep learning: praca z językiem Python i biblioteką Keras, Helion, 2019.

Literatura uzupełniająca	
1	Denis Rothman, Transformers for Natural Language Processing: Build innovative deep neural network architectures for NLP with Python, PyTorch, TensorFlow, BERT, RoBERTa, and more , Packt Publishing, 2021.
2	Ben Auffarth, Generatywna sztuczna inteligencja z LangChain. Budowanie aplikacji AI opartych na LLM z użyciem Pythona, ChatGPT i innych modeli językowych, Helion, 2024.
3	Aman Kedia, Mayank Rasu, Hands-On Python Natural Language Processing. Explore tools and techniques to analyze and process text with a view to building real-world NLP applications, Birmingham, England ; Mumbai : Packt, 2020.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	45
Udział w wykładach:	45
Praca własna studenta, w tym:	30
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	30
Łączny czas pracy studenta	75
Sumaryczna liczba punktów ECTS dla przedmiotu	3

Macierz efektów uczenia się

Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W02++ CB1A_W19++	C1, C2	W1 - W15	1	O1
EK 2	CB1A_W02++ CB1A_W19++	C1, C2	W1 - W15	1	O1
EK 3	CB1A_K05+	C1, C2	W1 - W15	1	O1

Autor programu:	dr Michał Dolecki; mgr Alicja Żmudzińska
Adres e-mail:	m.dolecki@pollub.pl; a.zmudzinska@pollub.pl
Jednostka organizacyjna:	Katedra Inteligencji Obliczeniowej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Spółeczne i technologiczne aspekty sztucznej inteligencji
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C506.2
Rok:	III
Semestr:	5
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	45
Wykład	45
Ćwiczenia	
Laboratorium	
Projekt	
Liczba punktów ECTS:	3
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język angielski /język niemiecki

Cele przedmiotu

C1	Zapoznanie z najnowszymi trendami w rozwoju sztucznej inteligencji oraz jej wpływem na różne obszary życia
C2	Zapoznanie z najnowszymi technologiami, prognozami rozwoju AI oraz jej potencjalnymi zastosowaniami

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1	Znajomość narzędzi programistycznych do tworzenia aplikacji związanych ze sztuczną inteligencją
2	Podstawowa wiedza z zakresu algorytmów i uczenia maszynowego

Efekty uczenia się

	W zakresie wiedzy:
EK1	zna i rozumie główne trendy rozwojowe w obszarze sztucznej inteligencji, w tym dotyczące uczenia maszynowego, głębokiego uczenia oraz generatywnej AI
EK2	rozumie wpływ sztucznej inteligencji na cyberbezpieczeństwo, w tym zarówno jej potencjalne zagrożenia, jak i korzyści
EK3	rozumie etyczne i społeczne wyzwania związane z wdrażaniem sztucznej inteligencji w różnych dziedzinach
	W zakresie kompetencji społecznych:
EK3	jest gotów do krytycznego podejścia do nowych technologii w obszarze sztucznej inteligencji, uwzględniając ich etyczne i społeczne konsekwencje

Treści programowe przedmiotu

Forma zajęć - wykłady	
	Treści programowe
W1	Wprowadzenie do współczesnej sztucznej inteligencji. Kluczowe technologie i pojęcia (uczenie maszynowe, głębokie uczenie, generatywna AI). Sztuczna inteligencja jako kluczowy element transformacji cyfrowej
W2	Sztuczna inteligencja, a cyberbezpieczeństwo
W3	Etyka i społeczne konsekwencje sztucznej inteligencji
W4	Prognozy i przyszłość sztucznej inteligencji
W5	Główne wyzwania stojące przed specjalistami ds. AI i cyberbezpieczeństwa

Metody dydaktyczne	
1	wykład informacyjny
2	dyskusja dydaktyczna

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena aktywności w trakcie zajęć	51%

Literatura podstawowa	
1	Kalyan, Suman and Alla, Sridhar, Beginning Anomaly Detection Using Python-Based Deep Learning: Implement Anomaly Detection Applications with Keras and Pytorch. Second edition. Berkeley, CA: Apress L. P, 2024.

Literatura uzupełniająca	
1	Denis Rothman, Transformers for Natural Language Processing: Build innovative deep neural network architectures for NLP with Python, PyTorch, TensorFlow, BERT, RoBERTa, and more , Packt Publishing, 2021.
2	Ben Auffarth, Generatywna sztuczna inteligencja z LangChain. Budowanie aplikacji AI opartych na LLM z użyciem Pythona, ChatGPT i innych modeli językowych, Helion, 2024.
3	Aman Kedia, Mayank Rasu, Hands-On Python Natural Language Processing. Explore tools and techniques to analyze and process text with a view to building real-world NLP applications, Birmingham, England ; Mumbai : Packt, 2020.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	45
Udział w wykładach:	45
Praca własna studenta, w tym:	30
Studiowanie tematyki wykładów, przygotowanie	30

do kolokwium:	
Łączny czas pracy studenta	75
Sumaryczna liczba punktów ECTS dla przedmiotu	3

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W02++ CB1A_W19++	C1, C2	W1 - W5	1, 2	O1, O2
EK 2	CB1A_W02++ CB1A_W19++	C1, C2	W1 - W5	1, 2	O1, O2
EK 3	CB1A_W02++ CB1A_W20+	C1, C2	W3, W5	1, 2	O1, O2
EK 4	CB1A_K01+	C1, C2	W1 - W5	1, 2	O1, O2

Autor programu:	dr Michał Dolecki; mgr Alicja Żmudzińska
Adres e-mail:	m.dolecki@pollub.pl; a.zmudzinska@pollub.pl
Jednostka organizacyjna:	Katedra Inteligencji Obliczeniowej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Big Data
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C507.1
Rok:	III
Semestr:	5
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	60
Wykład	30
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	4
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Przedstawienie podstawowych koncepcji i technologii przetwarzania danych na dużą skalę (Big Data)
C2	Zrozumienie roli analizy dużych zbiorów danych w cyberbezpieczeństwie
C3	Rozwijanie umiejętności implementacji narzędzi i metod analizy danych w celu identyfikacji zagrożeń i zapewnienia bezpieczeństwa

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Znajomość podstaw algorytmów i struktur danych
2	Umiejętność programowania i pracy z bazami danych
3	Podstawowa wiedza z zakresu cyberbezpieczeństwa

Efekty uczenia się	
	W zakresie wiedzy:
EK 1	zna podstawowe technologie i narzędzia stosowane w Big Data
EK 2	rozumie zastosowanie analizy dużych zbiorów danych w identyfikacji zagrożeń w cyberprzestrzeni
	W zakresie umiejętności:
EK3	potrafi zastosować metody analizy danych do wykrywania anomalii w systemach informatycznych
EK4	implementuje i optymalizuje procesy przetwarzania danych na dużą skalę
	W zakresie kompetencji społecznych:

EK5	jest gotów do odpowiedzialnego wypełniania, prawidłowego identyfikowania i rozstrzygania dylematów związanych z wykonywaniem zawodu specjalisty ds. cyberbezpieczeństwa z nastawieniem wykorzystania w swojej pracy Big Data
------------	--

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Wprowadzenie do Big Data (definicja, cechy, zastosowania)
W2	Architektury systemów przetwarzania dużych zbiorów danych
W3	Modele przetwarzania danych (batch processing, stream processing)
W4	Technologie składowania i przetwarzania danych (np. hurtownie danych, systemy rozproszone)
W5	Zastosowanie algorytmów uczenia maszynowego w Big Data
W6	Rola Big Data w wykrywaniu zagrożeń cyberbezpieczeństwa
W7	Analiza przypadków wykorzystania Big Data w cyberbezpieczeństwie
W8	Przyszłość Big Data i wyzwania związane z jego rozwojem
Forma zajęć - laboratoria	
	Treści programowe
L1	Instalacja i konfiguracja środowisk Big Data
L2	Wykorzystanie narzędzi do przetwarzania danych w trybie batch processing
L3	Implementacja analizy danych w czasie rzeczywistym (stream processing)
L4	Optymalizacja procesów przetwarzania danych
L5	Wykrywanie anomalii i zagrożeń w danych sieciowych
L6	Projekt - analiza danych pod kątem cyberzagrożeń

Metody dydaktyczne	
1	wykład problemowy
2	ćwiczenia laboratoryjne
3	metoda projektu

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51 %
O2	ocena wykonanych sprawozdań laboratoryjnych	51 %
O3	ocena przygotowanego projektu	51 %

Literatura podstawowa	
1	Holmes, Dawn E., i in. Big Data. Wydanie I., Wyd. Uniwersytetu Łódzkiego, 2021.
2	McKinney, Wes, i in. Python w analizie danych : przetwarzanie danych za pomocą pakietów Pandas i NumPy oraz środowiska IPython. Helion, 2018.

3	Lantz, Brett, i in. Uczenie maszynowe w języku R : tworzenie i doskonalenie model - od przygotowania danych po dostrajanie, ewaluację i pracę z big data. Helion, 2024.
---	---

Literatura uzupełniająca	
1	S. Onur, J. Deng, Big data analytics in cybersecurity. CRC Press, 2017.
2	Y. Maleh, M. Shojaifar, M. Alazab, Y. Baddi, Machine intelligence and big data analytics for cybersecurity applications. Cham, Switzerland: Springer, 2021.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	60
Udział w wykładach:	30
Udział w zajęciach laboratoryjnych:	30
Praca własna studenta, w tym:	40
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	20
Przygotowanie do zajęć laboratoryjnych:	20
Łączny czas pracy studenta	100
Sumaryczna liczba punktów ECTS dla przedmiotu	4

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W21++ CB1A_W06++	C1	W1-W4	1, 2	O1
EK 2	CB1A_W06++	C2, C3	W5-W8	1, 2	O1
EK 3	CB1A_U06++ CB1A_U17++	C3	L1-L3	2, 3	O2
EK 4	CB1A_U17+++	C3	L4-L6	2, 3	O2
EK 5	CB1A_K05+	C3	L6	2, 3	O2

Autor programu:	dr hab. inż. Dariusz Czerwiński, profesor uczelni; mgr Dariusz Głuchowski
Adres e-mail:	d.czerwinski@pollub.pl; d.głuchowski@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Stosowanej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Nowoczesne technologie w przestrzeni cyfrowej
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C507.2
Rok:	III
Semestr:	5
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	60
Wykład	30
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	4
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu

C1	Zapoznanie z technikami prezentacji danych wykorzystujących wirtualne modele cyfrowe
C2	Zdobycie umiejętności przygotowania prezentacji zbiorów danych badawczych lub technicznych z wykorzystaniem sieci komputerowych, modeli cyfrowych i wirtualnej rzeczywistości
C3	Nabycie umiejętności bezpiecznego organizowania wirtualnych spotkań, prezentacji i telekonferencji połączonych z prezentacją złożonych zbiorów danych

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1	Wiedza z zakresu bezpieczeństwa aplikacji i sieci komputerowych
2	Znajomość technik chmurowych, w tym tworzenia i współdzielenia dokumentów i obiektów w chmurze

Efekty uczenia się

	W zakresie wiedzy:
EK 1	posiada wiedzę w zakresie bezpiecznego wykorzystania komputerów i sieci komputerowych do organizowania prezentacji danych i projektów technicznych z wykorzystaniem współczesnych narzędzi, w tym w środowisku wirtualnej i rozszerzonej rzeczywistości
EK 2	zna zagrożenia związane ze stosowaniem współczesnych metod komunikacji i prezentacji danych w cyberprzestrzeni oraz funkcjonowania człowieka w środowisku wirtualnym
	W zakresie umiejętności:

EK3	potrafi zidentyfikować zagrożenia związane ze stosowaniem współczesnych technik obróbki i prezentacji danych, w szczególności związanych z organizacją konferencji i prezentacji w środowisku wirtualnym
EK4	posługuje się techniką wirtualnej i rozszerzonej rzeczywistości do realizacji zadań związanych z przygotowaniem bezpiecznej prezentacji danych naukowych i projektów technicznych
	W zakresie kompetencji społecznych:
EK5	jest gotów do krytycznej oceny przydatności technik wykorzystujących wirtualną rzeczywistość i cyberprzestrzeń do zastosowań naukowych, technicznych i rozrywkowych

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	współczesne metody prezentacji informacji: metody immersyjne (np. modelowanie 3D, animacja, dźwięk przestrzenny, techniki audio 3D), metody wizualizacji danych (np. wizualizacja interaktywna, wizualizacja w czasie rzeczywistym)
W2	wirtualna rzeczywistość (VR): sprzęt, oprogramowanie, przykłady zastosowań w rozrywce, edukacji, przemyśle; prezentacja obiektów 3D, interakcja z obiektami i aktorami w środowisku VR, zagrożenia związane z używaniem techniki VR
W3	rozszerzona rzeczywistość (AR): sprzęt, oprogramowanie, przykłady zastosowań
W4	przemysłowe zastosowania VR i AR: projektowanie i weryfikacja systemu przemysłowego (np. celi robota), zastosowania szkoleniowe, serwis i pomoc techniczna
W5	wymiana idei, prezentacje i konferencje w przestrzeni cyfrowej (teleprezencja, wirtualne sale konferencyjne)
W6	zastosowania medyczne i okołomedyczne technologii VR, AR; integracja danych z przestrzeni cyfrowej z systemem nerwowym organizmów żywych; perspektywy rozwojowe i zagrożenia
W7	nowości z obszaru obróbki i prezentacji danych - prezentacja wybranego systemu lub technologii
Forma zajęć - laboratoria	
	Treści programowe
L1	śledzenie położenia i orientacji w przestrzeni 3D
L2	przygotowanie danych do prezentacji w systemie VR lub AR w wybranym środowisku programowania
L3	prezentacja w środowisku wirtualnym (VR)
L4	konferencja w świecie wirtualnym
L5	interakcja z obiektami w świecie wirtualnym
L6	przygotowanie prezentacji w rozszerzonej rzeczywistości (AR)
L7	symulacja procedury z użyciem technik AR/VR (np. wsparcie pracownika w zadaniu serwisowym lub szkolenie operatora)

Metody dydaktyczne

1	wykład informacyjny
2	ćwiczenia laboratoryjne
3	metoda symulacji

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena wykonanych ćwiczeń laboratoryjnych	51%
O3	ocena wykonanych symulacji	51%

Literatura podstawowa	
1	Burdea, Grigore C., and Philippe Coiffet. Virtual Reality Technology. 2nd ed., John Wiley & Sons, Incorporated, 2003.
2	Olbrzych, Barbara, i in. Wirtualna rzeczywistość w perspektywie prawnej, bezpieczeństwa cyfrowego i technologii informacyjnych. T. 1 i 2. Akademia Handlowa Nauk Stosowanych w Radomiu, 2022.

Literatura uzupełniająca	
1	Peddie, Jon. The History of Visual Magic in Computers : How Beautiful Images Are Made in CAD, 3D, VR and AR. 1st ed. 2013., Springer, 2013, https://doi.org/10.1007/978-1-4471-4932-3 .
2	Peddie, Jon. Augmented Reality: Where We Will All Live. 1st ed. 2017., Springer International Publishing AG, 2023, https://doi.org/10.1007/978-3-319-54502-8 .
3	tom Dieck, M. Claudia, et al. Augmented Reality and Virtual Reality: The Power of AR and VR for Business. 1st ed. 2019., Springer International Publishing AG, 2019, https://doi.org/10.1007/978-3-030-06246-0 .
4	Glover, Jesse, and Jonathan Linowes. Complete Virtual Reality and Augmented Reality Development with Unity: Leverage the Power of Unity and Become a Pro at Creating Mixed Reality Applications. 1st ed., Packt Publishing, Limited, 2019.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	60
Udział w wykładach:	30
Udział w zajęciach laboratoryjnych:	30
Praca własna studenta, w tym:	40
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	20
Przygotowanie do zajęć laboratoryjnych:	20
Łączny czas pracy studenta	100

Sumaryczna liczba punktów ECTS dla przedmiotu	4
---	---

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W03++	C1	W1-W7	1	O1
EK 2	CB1A_W02++	C1	W1-W7	1	O1
EK 3	CB1A_U01++	C2, C3	L1-L7	2,3	O2,O3
EK 4	CB1A_U06++	C2, C3	L1-L7	2,3	O2,O3
EK 5	CB1A_K01+	C1, C3	W1-W7, L1-L7	1,2,3	O2,O3

Autor programu:	dr inż. Radosław Cechowicz
Adres e-mail:	r.cechowicz@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Technicznej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Zarządzanie tożsamością i dostępem
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C508.1
Rok:	III
Semestr:	5
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	60
Wykład	30
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	4
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zrozumienie podstawowych zasad i mechanizmów zarządzania tożsamością i dostępem
C2	Nabycie praktycznych umiejętności projektowania i implementacji systemów IAM
C3	Nabycie umiejętności przygotowania audytu i zapewnienia bezpieczeństwa systemów IAM

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Podstawowa wiedza z zakresu technologii informatycznych
2	Znajomość podstaw oraz zasad bezpieczeństwa informacji

Efekty uczenia się (zmniejszych ilość)	
	W zakresie wiedzy:
EK 1	definiuje kluczowe pojęcia dotyczące zarządzania tożsamością i dostępem
EK 2	charakteryzuje najważniejsze protokoły stosowane w zarządzaniu tożsamością i dostępem
EK 3	zna zasady i techniki zarządzania cyklem życia tożsamości, w tym procesy tworzenia, aktualizacji, dezaktywacji oraz usuwania tożsamości użytkowników w systemach informacyjnych
	W zakresie umiejętności:
EK 4	projektuje podstawowe elementy systemu IAM, takie jak magazyny tożsamości, procesy uwierzytelniania i autoryzacji
EK 5	wdraża procesy rejestracji, logowania, zmiany ról i usuwania kont w systemach IAM
	W zakresie kompetencji społecznych:

EK 6	jest gotów do odpowiedzialnego pełnienia roli zawodowej specjalisty ds. cyberbezpieczeństwa, mając świadomość konsekwencji wynikających z niewłaściwym zarządzaniem tożsamością i dostępem
-------------	--

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Wprowadzenie do zarządzania tożsamością i dostępem (IAM)
W2	Architektura systemów zarządzania tożsamością i dostępem
W3	Protokoły i standardy w zarządzaniu tożsamością
W4	Active Directory, usługi katalogowe
W5	Metody uwierzytelniania i autoryzacji
W6	Podstawy projektowanie modułów systemowych, magazynów tożsamości, mechanizmów uwierzytelniania i autoryzacji
W7	Zarządzanie cyklem życia tożsamości użytkowników w organizacjach
W8	Technika jednokrotnego logowania (SSO)
W9	Technika dostępu uprzywilejowanego (PAM) i zarządzanie ryzykiem
W10	Zarządzanie zgodne z przepisami, audyt tożsamości i dostępu
W11	Trendy rozwoju systemów zarządzania tożsamością i dostępem
Forma zajęć - laboratoria	
	Treści programowe
L1	Wprowadzenie do środowiska systemów zarządzania tożsamością i dostępem
L2	Przegląd wybranych standardów
L3	Zarządzanie tożsamością użytkowników, rolami, uprawnieniami i kontrola dostępu
L4	Projektowanie magazynów tożsamości
L5	Projektowanie mechanizmów uwierzytelniania i autoryzacji
L6	Implementacja kontroli dostępu opartej na rolach (RBAC)
L7	Implementacja techniki jednokrotnego logowania (SSO)
L8	Wdrażanie mechanizmów zarządzania dostępem uprzywilejowanym (PAM)

Metody dydaktyczne	
1	wykład informacyjny
2	ćwiczenia laboratoryjne

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena wykonanych programów komputerowych	51%
O3	ocena wykonanych sprawozdań laboratoryjnych	51%

Literatura podstawowa	
1	Plucińska, M., Analiza Technik Biometrycznych Do Uwierzytelniania Os b, Elektronika 1.4 (2014): 66–68.
2	Adamus-Kowalska, J., Techniki Elektronicznej Identyfikacji Użytkowników i Ich Rola We Współczesnej Komunikacji z Instytucjami Systemu Administracyjnego, Zagadnienia informacji naukowej 53.2 (106) (2015): 115–128.
3	Polaczek, T., Audyt bezpieczeństwa informacji w praktyce : praktyczny przewodnik po zagadnieniach ochrony informacji, Helion, 2006.
4	Poniszewska-Marańda, A., Modele bezpieczeństwa logicznego i ich implementacje w systemach informatycznych, Akademicka Oficyna Wydawnicza EXIT, 2013.

Literatura uzupełniająca	
1	Stallings, W., Brown L., Bezpieczeństwo systemów informatycznych. Zasady i praktyka, Wydanie IV, Tom 1, Helion, 2019.
2	Stallings, W., Brown L., Bezpieczeństwo systemów informatycznych. Zasady i praktyka, Wydanie IV, Tom 2, Helion, 2019.
3	Ściborek, P., Uwierzytelnianie i autoryzacja zasobów w sieciach definiowanych programowo, Elektronika 1.10, 2017.
4	Schwartz, M., Machulak M., LDAP Securing the Perimeter, Apress L. P, 2018. 17–57.
5	Krause, J., Mastering Windows Group Policy : Control and Secure Your Active Directory Environment with Group Policy. Birmingham ; Packt Publishing, 2018.
6	Hunter, Laura E. Active Directory Field Guide. 1st ed. 2005. Berkeley, CA: Apress, 2005.
7	Jochen N., Mastering Identity and Access Management with Microsoft Azure: Empower Users by Managing and Protecting Identities and Data, 2nd Edition, Packt Publishing, 2019.
8	Thorgersen S., Silva P.I., Keycloak - Identity and Access Management for Modern Applications: Harness the Power of Keycloak, OpenID Connect, and OAuth 2.0 Protocols to Secure Applications, Packt Publishing, 2021.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	60
Udział w wykładach:	30
Udział w zajęciach laboratoryjnych:	30
Praca własna studenta, w tym:	40
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	20
Przygotowanie do zajęć laboratoryjnych:	20
Łączny czas pracy studenta	100
Sumaryczna liczba punktów ECTS dla przedmiotu	4

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W14++ CB1A_W15++	C1,C3	W1-W11	1	O1
EK 2	CB1A_W14++ CB1A_W15++	C1,C3	W1-W11	1	O1
EK 3	CB1A_W21++	C1,C3	W1-W11	1	O1
EK 4	CB1A_U18++ CB1A_U10++	C1,C2	L1-L8	2	O2,O3
EK 5	CB1A_U18++ CB1A_U10++	C1,C2	L1-L8	2	O2,O3
EK 6	CB1A_K05++	C3	W1-W11	1	O1

Autor programu:	dr Rafał Stęgiński
Adres e-mail:	r.stegierski@pollub.pl
Jednostka organizacyjna:	Katedra Inteligencji Obliczeniowej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Techniki uwierzytelniania i autoryzacji w systemach informacyjnych
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C508.2
Rok:	III
Semestr:	5
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	60
Wykład	30
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	4
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Poznanie podstawowych koncepcji i protokołów uwierzytelniania oraz autoryzacji
C2	Nabycie praktycznych umiejętności projektowania i implementacji rozwiązań uwierzytelniania i autoryzacji
C3	Zapewnienia bezpieczeństwa w systemach uwierzytelniania i autoryzacji

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Podstawowa znajomość sieci komputerowych i systemów operacyjnych
2	Podstawowa znajomość programowania i technologii webowych lub mobilnych
3	Znajomość podstaw bezpieczeństwa informacji

Efekty uczenia się	
	W zakresie wiedzy:
EK 1	objaśnia podstawowe pojęcia związane z uwierzytelnianiem i autoryzacją w systemach informacyjnych
EK 2	posiada wiedzę na temat podstawowych oraz zaawansowanych protokołów uwierzytelniania i autoryzacji
	W zakresie umiejętności:
EK3	przygotowuje środowisko testowe do implementacji mechanizmów uwierzytelniania i autoryzacji
EK4	wdraża i konfiguruje protokoły uwierzytelniania i autoryzacji
	W zakresie kompetencji społecznych:

EK5	jest gotów do odpowiedzialnego pełnienia roli zawodowej specjalisty ds. cyberbezpieczeństwa mając świadomość odpowiedzialności za projektowanie i wdrażanie bezpiecznych systemów uwierzytelniania i autoryzacji
EK6	jest gotów do krytycznego myślenia i rozwiązywania problemów w obszarze uwierzytelniania i autoryzacji oraz w kontekście zagrożeń

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Podstawowe pojęcia związane z uwierzytelnianiem i autoryzacją w systemach informacyjnych
W2	Wprowadzenie do technik uwierzytelniania i autoryzacji
W3	Podstawowe protokoły uwierzytelniania i autoryzacji, przegląd
W4	Środowisko testowe implementacji protokołów uwierzytelniania i autoryzacji
W5	Uwierzytelnianie wieloskładnikowe (MFA)
W6	Uwierzytelnianie oparte o proxy i usługi katalogowe
W7	Biometryczne techniki uwierzytelniania
W8	Zaawansowane protokoły uwierzytelniania i autoryzacji
W9	Zagadnienia bezpieczeństwa oraz ataków w kontekście uwierzytelniania i autoryzacji
W10	Zagadnienia single-tenant i multi-tenant
W11	Trendy i kierunki rozwoju uwierzytelniania i autoryzacji
Forma zajęć - laboratoria	
	Treści programowe
L1	Przygotowanie środowiska testowego
L2	Implementacja podstawowego mechanizmu uwierzytelniania oraz autoryzacji użytkowników
L3	Analiza, konfiguracja i użycie rozwiązania opartych o podstawowe protokoły uwierzytelniania i autoryzacji (HTTP Basic Authentication, LDAP, Kerberos, RADIUS)
L4	Usługi katalogowe, Active Directory
L5	Analiza i konfiguracja rozwiązania opartego o zaawansowane protokoły uwierzytelniania i autoryzacji (Auth 2.0, OIDC, SAML, JWT)
L6	Zastosowanie biometrycznego uwierzytelniania w wybranej aplikacji
L7	Zarządzania tożsamością i dostępem w środowiskach chmurowych (IDaaS)
L8	Audyt uwierzytelniania i autoryzacji

Metody dydaktyczne	
1	wykład informacyjny
2	ćwiczenia laboratoryjne

Metody i kryteria oceny

Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena wykonanych programów komputerowych	51%
O3	ocena wykonanych sprawozdań laboratoryjnych	51%

Literatura podstawowa	
1	Andress, J., Podstawy bezpieczeństwa informacji : praktyczne wprowadzenie, Helion, 2022.
2	Catlow, J., Tworzenie bezpiecznych aplikacji Microsoft ASP.NET : uwierzytelnianie, autoryzacja i bezpieczna komunikacja : wzorce i przykłady, APN Promise, 2003.
3	Mikulski, M., Dwuczynnikowe Uwierzytelnianie Klienta Serwisu Webowego Poprzez Weryfikację Twarzy i Jej Mimiki z Wykorzystaniem Sztucznych Sieci Neuronowych, Elektronika 1.7, 2021.
4	Adamus-Kowalska, J., Techniki Elektronicznej Identyfikacji Użytkowników i Ich Rola We Współczesnej Komunikacji z Instytucjami Systemu Administracyjnego, Zagadnienia informacji naukowej 53.2 (106) (2015): 115-128.

Literatura uzupełniająca	
1	Plucińska, M., Potrzeba Silnego Uwierzytelniania Motorem Rozwoju Rynku Biometrycznego, Elektronika 1.8 (2015): 36-39.
2	Schwartz, M., and Machulak M., Securing the Perimeter: Deploying Identity and Access Management with Free Open Source Software. 1st ed., Apress L. P, 2018, https://doi.org/10.1007/978-1-4842-2601-8 .
3	Wilson, Y., Hingnikar, A., Solving Identity Management in Modern Applications: Demystifying OAuth 2.0, OpenID Connect, and SAML 2.0. 1st ed., Berkeley, Apress, 2019.
4	Nascimento, A. E., OAuth 2.0 Cookbook : Protect Your Web Applications Using Spring Security. 1st edition. Birmingham, Packt Publishing, 2017.
5	Narayanan, S., Securing Hadoop. 1st edition. Birmingham: Packt Publishing, 2013.
6	Siriwardena, P., HTTP Basic/Digest Authentication, Advanced API Security, Apress L. P, 2014. 33-46.
7	Jajodia, S., van Tilborg, H. C. A, HTTP Basic Authentication. Encyclopedia of Cryptography and Security, Springer US, 2011. 565-565.
8	Tomcy, J., Authentication Using SAML, LDAP, and OAuth/OIDC, Hands-On Spring Security 5 for Reactive Applications, Packt Publishing, Limited, 2018.
9	Freato, R., Microsoft Azure Security. 1st ed., Packt Publishing, 2015.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	60
Udział w wykładach:	30
Udział w zajęciach laboratoryjnych:	30

Praca własna studenta, w tym:	40
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	20
Przygotowanie do zajęć laboratoryjnych:	20
Łączny czas pracy studenta	100
Sumaryczna liczba punktów ECTS dla przedmiotu	4

Macierz efektów uczenia się					
Symbol przedmiotowe go efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W12++ CB1A_W15++	C1,C3	W1-W11	1	O1
EK 2	CB1A_W12++ CB1A_W15++	C1,C3	W1-W11	1	O1
EK 3	CB1A_U18++ CB1A_U10++	C2	L1-L8	2	O2,O3
EK 4	CB1A_U18++ CB1A_U10++	C2	L1-L8	2	O2,O3
EK 5	CB1A_K05+	C3	W1-W11	1	O1
EK 6	CB1A_K01+	C3	W1-W11	1	O1

Autor programu:	dr Rafał Stęgiński
Adres e-mail:	r.stegierski@pollub.pl
Jednostka organizacyjna:	Katedra Inteligencji Obliczeniowej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Bezpieczeństwo infrastruktury krytycznej w systemach przemysłowych
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C601
Rok:	III
Semestr:	6
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	60
Wykład	30
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	4
Sposób zaliczenia:	egzamin
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zapoznanie z pojęciami, standardami i regulacjami związanymi z cyberbezpieczeństwem infrastruktury krytycznej w systemach przemysłowych
C2	Nabycie praktycznej wiedzy z zakresu identyfikacji i analizy zagrożeń cybernetycznych, oceniania ryzyka i analizy podatności w systemach przemysłowych
C3	Nabycie wiedzy i umiejętności w zakresie projektowania, wdrażania rozwiązań bezpieczeństwa i testowania mechanizmów zabezpieczających systemy przemysłowe, z uwzględnieniem wymagań specyficznych dla infrastruktury krytycznej
C4	Przygotowanie do skutecznego reagowania na incydenty bezpieczeństwa w infrastrukturze krytycznej, w tym planowania procedur awaryjnych

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Znajomość algebry liniowej, analizy matematycznej oraz statystyki
2	Podstawowe umiejętności programowania w wybranym języku programowania wysokiego poziomu
3	Podstawowe umiejętności z elektrotechniki i elektroniki

Efekty uczenia się	
	W zakresie wiedzy:
EK1	rozpoznaje zróżnicowane zagrożenia cybernetyczne w systemach przemysłowych
EK2	identyfikuje metody zapobiegawcze przed incydentami bezpieczeństwa, formułuje i opisuje metody działania w trakcie i po zakończeniu incydentu lub awarii
	W zakresie umiejętności:

EK3	analizuje i ocenia podatność systemów przemysłowych na ataki cybernetyczne
EK4	projektuje bezpieczne systemy przemysłowe w kontekście zapewnienia cyberbezpieczeństwa infrastruktury krytycznej
EK5	interpretuje informacje i dane w kontekście cyberbezpieczeństwa na potrzeby rozwiązywania problemów związanych z cyberbezpieczeństwem w systemach przemysłowych
	W zakresie kompetencji społecznych:
EK6	jest gotów do krytycznej oceny posiadanej wiedzy oraz odbieranych treści dotyczących bezpieczeństwa cyfrowego, rozumiejąc potrzebę ciągłego doskonalenia oraz aktualizacji informacji dla skutecznej ochrony infrastruktury krytycznej

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Wprowadzenie do cyberbezpieczeństwa w systemach przemysłowych
W2	Zagrożenia cybernetyczne dla systemów przemysłowych
W3	Architektura bezpieczeństwa systemów przemysłowych
W4	Bezpieczeństwo systemów SCADA
W5	Zarządzanie ryzykiem cybernetycznym w systemach przemysłowych
W6	Monitorowanie i wykrywanie zagrożeń w systemach przemysłowych
W7	Reagowanie na incydenty cybernetyczne w systemach przemysłowych
W8	Bezpieczeństwo komunikacji w systemach przemysłowych
W9	Zarządzanie dostępem i tożsamością w systemach przemysłowych
W10	Bezpieczeństwo urządzeń IoT w systemach przemysłowych
W11	Testowanie penetracyjne systemów przemysłowych
W12	Normy i regulacje dotyczące cyberbezpieczeństwa w systemach przemysłowych
W13	Przyszłość cyberbezpieczeństwa w systemach przemysłowych
Forma zajęć - laboratoria	
	Treści programowe
L1	Wykrywanie i analiza malware w systemach przemysłowych
L2	Wykrywanie i analiza ransomware w systemach przemysłowych
L3	Wykrywanie i analiza DDoS w systemach przemysłowych
L4	Konfiguracja i zabezpieczenie systemów SCADA
L5	Bezpieczeństwa interfejsów komunikacyjnych cz. 1
L6	Bezpieczeństwo interfejsów komunikacyjnych cz. 2
L7	Konfiguracja i analiza ruchu w protokołach przemysłowych
L8	Bezpieczeństwo urządzeń IoT - implementacja szyfrowania i autoryzacji dla urządzeń IoT
L9	Wykrywanie i obrona przed atakami typu Man-in-the-Middle w sieciach przemysłowych i systemach SCADA
L10	Praktyczne wstrzykiwanie danych do interfejsu CAN

L11	Bezpieczeństwo chmur w systemach przemysłowych: Wdrożenie i konfiguracja systemów zarządzania w chmurze z zachowaniem wymogów bezpieczeństwa
L12	Ocena ryzyka w systemach przemysłowych: Analiza typowych zagrożeń i ryzyk w systemach przemysłowych oraz projektowanie systemu zarządzania ryzykiem
L13	Analiza podatności systemów przemysłowych: Skanowanie i ocena podatności przy użyciu typowych narzędzi
L14	Bezpieczna konfiguracja PLC: Zabezpieczanie ustawień, kontrola dostępu i monitorowanie logów PLC
L15	Kompleksowa analiza systemu – interfejsy, pamięci, szyfrowanie i zabezpieczenia, metody Return Oriented Programming i stack overflow, deasemblacja kodu z zastosowaniem

Metody dydaktyczne	
1	wykład informacyjny
2	ćwiczenia laboratoryjne

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena odpowiedzi ustnej	51%
O3	ocena wykonanych ćwiczeń laboratoryjnych	51%

Literatura podstawowa	
1	Banasiński, Cezary, i in. Cyberbezpieczeństwo. Wolters Kluwer, 2020.
2	Culic, Ioana. Komercyjne i przemysłowe aplikacje Internetu rzeczy na Raspberry Pi: prototypowanie rozwiązań IoT. APN Promise, 2020.
3	Bravo, Cesar. Cyberbezpieczeństwo dla zaawansowanych: skuteczne zabezpieczenia systemu Windows, Linux, IoT i infrastruktury w chmurze. Helion, 2023.
4	Piotr Arabas, i in. Bezprzewodowe sieci czujników w internecie rzeczy: Modele - Algorytmy - Protokoły. 1. wyd., Wyd. Naukowe PWN, 2023.
5	Systemy DCS i SCADA. Oficyna Wydawnicza Politechniki Warszawskiej, 2022.

Literatura uzupełniająca	
1	Internet rzeczy IoT i IoE w symulatorze Cisco Packet Tracer : praktyczne przykłady i ćwiczenia - Politechnika Lubelska.
2	Długosz, Tomasz. Protokoły komunikacyjne w pojazdach samochodowych. Oficyna Wydawnicza Politechniki Wrocławskiej, 2013.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności

Godziny kontaktowe z wykładowcą, w tym:	60
Udział w wykładach:	30
Udział w zajęciach laboratoryjnych:	30
Praca własna studenta, w tym:	40
Studiowanie tematyki wykładów, przygotowanie do egzaminu:	25
Przygotowanie do zajęć laboratoryjnych:	15
Łączny czas pracy studenta	100
Sumaryczna liczba punktów ECTS dla przedmiotu	4

Macierz efektów uczenia się					
Symbol przedmiotowe go efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W15+++ CB1A_W12+++	C1,C2	W1-W13	1	O1, O2
EK 2	CB1A_W15+++ CB1A_W12+++	C1,C2	W1-W13	1	O1, O2
EK 3	CB1A_U01++ CB1A_U09++	C2, C3, C4	L1-L15	2	O3
EK 4	CB1A_U09++ CB1A_U17++	C2, C3, C4	L1-L15	2	O3
EK 5	CB1A_K01+	C3, C4	W1-W13	1	O2

Autor programu:	dr hab. inż. Michał Wydra, profesor uczelni
Adres e-mail:	m.wydra@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Stosowanej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Zarządzanie bezpieczeństwem informacji i audyt IT
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C602
Rok:	III
Semestr:	6
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	60
Wykład	30
Ćwiczenia	
Laboratorium	
Projekt	30
Liczba punktów ECTS:	4
Sposób zaliczenia:	egzamin
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zapoznanie z podstawowymi pojęciami, normami i standardami dotyczącymi zarządzania bezpieczeństwem informacji i audytu systemów IT
C2	Przekazanie wiedzy na temat roli i struktury polityk bezpieczeństwa informacji oraz ich znaczenia dla ochrony zasobów cyfrowych i infrastruktury IT
C3	Rozwinięcie umiejętności planowania i przeprowadzania audytu systemów bezpieczeństwa informacji z wykorzystaniem odpowiednich narzędzi
C4	Kształtowanie kompetencji w zakresie oceny skuteczności polityk bezpieczeństwa oraz przygotowywania i realizacji szkoleń z zakresu cyberbezpieczeństwa

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Podstawowa wiedzę z zakresu cyberbezpieczeństwa, w tym znajomość zagrożeń, pojęcia bezpieczeństwa informacji oraz podstawowych zabezpieczeń technicznych
2	Znajomość struktury i działania systemów informatycznych, w szczególności systemów operacyjnych, sieci komputerowych oraz usług sieciowych
3	Umiejętność czytania i interpretacji dokumentów technicznych i prawnych
4	Zdolność logicznego myślenia oraz pracy zespołowej przy realizacji projektów i zadań praktycznych

Efekty uczenia się	
	W zakresie wiedzy:
EK1	zna normy i standardy dotyczące zarządzania bezpieczeństwem informacji oraz ich zastosowanie w audycie i kontroli wewnętrznej

EK2	rozumie rolę polityk bezpieczeństwa informacji w ochronie zasobów cyfrowych i IT oraz znaczenie edukacji i kultury bezpieczeństwa w organizacjach
EK3	zna metody planowania, przeprowadzania i dokumentowania audytu bezpieczeństwa informacji, uwzględniając zgodność z przepisami prawa i wymaganiami normatywnym
	W zakresie umiejętności:
EK4	potrafi opracować, wdrożyć i dostosować polityki bezpieczeństwa informacji do specyfiki organizacji, uwzględniając aktualne ryzyka i obowiązujące regulacje
EK5	potrafi zaplanować i przeprowadzić audyt systemu zarządzania bezpieczeństwem informacji, zebrać dane audytowe, ocenić poziom bezpieczeństwa i sformułować rekomendacje
EK6	potrafi przygotować i przeprowadzić szkolenie z zakresu bezpieczeństwa cyfrowego oraz brać aktywny udział w dyskusji nad doskonaleniem polityk i procedur bezpieczeństwa
	W zakresie kompetencji społecznych:
EK7	jest gotów do podejmowania działań na rzecz edukacji i promocji bezpiecznych praktyk cyfrowych oraz inicjowania inicjatyw wspierających interes publiczny i podnoszenie świadomości społecznej w zakresie cyberzagrożeń

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Normy i standardy w bezpieczeństwie informacji: ISO/IEC 27001, ISO/IEC 27002, ISO 19011 – wytyczne dot. Audytu.
W2	System Zarządzania Bezpieczeństwem Informacji według ISO/IEC 27001 – struktura, wdrażanie i znaczenie w organizacji. Zasady i struktura tworzenia polityk bezpieczeństwa
W3	Rola polityki bezpieczeństwa w ochronie informacji i zasobów cyfrowych. Rodzaje polityk bezpieczeństwa: bezpieczeństwa informacji, dostępu i zarządzania tożsamością, ochrony danych osobowych, zarządzania urządzeniami mobilnymi i dostępem zdalnym, ciągłości działania
W4	Pojęcia: audyt, kontrola, zgodność, efektywność, skuteczność. Typy audytu: wewnętrzny, zewnętrzny, zgodności, systemowy
W5	Proces audytu zgodnie z ISO 19011
W6	Ocena polityk bezpieczeństwa w organizacji
W7	Audyt zgodności z przepisami prawa i normami branżowymi
W8	Narzędzia w audycie i wykrywaniu nadużyć
W9	Audyt systemów IT: analiza infrastruktury i procesów. Zbieranie dowodów audytowych, śledzenie przepływu informacji
W10	Dokumentacja audytowa: lista kontrolna, raport, zalecenia. Skuteczna komunikacja wyników audytu
W11	Edukacja i kultura bezpieczeństwa w organizacjach: programy szkoleń, komunikacja wewnętrzna, podnoszenie świadomości
Forma zajęć - projekt	

	Treści programowe
P1	Stworzenie dokumentu polityki bezpieczeństwa dostosowanego do konkretnej firmy lub instytucji
P2	Analiza polityki bezpieczeństwa znanej firmy: przegląd publicznie dostępnych polityk, porównanie ich z dobrymi praktykami i normami bezpieczeństwa, ocena skuteczności i możliwych słabych punktów
P3	Audyt dokumentacji: analiza polityk bezpieczeństwa informacji, procedur i rejestrów, ocena zgodności dokumentacji z normami lub regulacjami prawnymi
P4	Audyt techniczny: praca z narzędziami do analizy bezpieczeństwa, wykrywanie niezgodności technicznych (brak szyfrowania, słabe hasła, nieaktualne systemy)
P6	Przygotowanie raportu audytowego i rekomendacji dla organizacji
P7	Opracowanie szkolenia z cyberbezpieczeństwa. Przeprowadzenie przykładowego mini-szkolenia lub prezentacji uświadamiającej

Metody dydaktyczne	
1	wykład informacyjny
2	analiza przypadków
3	metoda projektu
4	dyskusja dydaktyczna
5	przygotowanie prezentacji

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena aktywności w trakcie zajęć	51%
O3	ocena przygotowanego projektu	51%
O4	ocena przygotowanej prezentacji	51%

Literatura podstawowa	
1	Brzostek, Agnieszka, i in., Cyberbezpieczeństwo w Polsce i na świecie. Towarzystwo Wiedzy Obronnej, 2024.
2	Oleksiewicz, Izabela, Transformacja polityki cyberbezpieczeństwa RP w XXI wieku. Elipsa Dom Wydawniczy, 2021.
3	Norma PN-EN ISO/IEC 27001:2023-08. Systemy zarządzania bezpieczeństwem informacji.
4	Norma ISO 19011 – Wytyczne dotyczące audytowania systemów zarządzania.
5	Krawiec, Jerzy, Cyberbezpieczeństwo. Podejście systemowe. Oficyna Wydawnicza Politechniki Warszawskiej, 2020.
6	Karpiuk, Mirosław, Audyt, kontrola i nadzór w sferze bezpieczeństwa. Wydawnictwo: Akademia Sztuki Wojennej, 2024.

Literatura uzupełniająca	
1	Ustawa z dnia 5 lipca 2018 r.o krajowym systemie cyberbezpieczeństwa. Dz.U. 2018 poz. 1560.
2	Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.
3	Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii.
4	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych.
5	Marczyk, Maciej, Cyberbezpieczeństwo w teorii i praktyce. Wybrane aspekty. Wydawnictwo: Akademia Sztuki Wojennej, 2023.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	60
Udział w wykładach:	30
Udział w zajęciach projektowych:	30
Praca własna studenta, w tym:	40
Studiowanie tematyki wykładów, przygotowanie do egzaminu:	25
Przygotowanie projektu:	15
Łączny czas pracy studenta	100
Sumaryczna liczba punktów ECTS dla przedmiotu	4

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W13+++ CB1A_W14+++	C1, C2	W1 – W10	1, 2	O1
EK 2	CB1A_W13+++ CB1A_W02+	C1, C2	W1 – W10	1, 2	O1
EK 3	CB1A_W13+++	C1, C2	W4 – W10	1, 2	O1

	CB1A_W15++				
EK 4	CB1A_U09++ CB1A_U20+++	C4	P1, P2, P7	2 - 5	O3, O4
EK 5	CB1A_U18+++ CB1A_U05+++	C3	P3 - P6	2 - 4	O3
EK 6	CB1A_U07++ CB1A_U05+++	C1 - C4	P7	4, 5	O2, O4
EK 7	CB1A_K03+++	C1 - C3	W1 - W10, P1 - P7	1 - 5	O1 - O3

Autor programu:	dr inż. Joanna Szulżyk-Cieplak; mgr inż. Jacek Zaborko
Adres e-mail:	j.szulzyk-cieplak@pollub.pl; j.zaborko@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Technicznej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Programowalne zarządzanie infrastrukturą i siecią (DevNet)
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C603
Rok:	III
Semestr:	6
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	60
Wykład	30
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	4
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zrozumienie koncepcji programowalnego zarządzania infrastrukturą sieciową
C2	Nabycie umiejętności tworzenia i wdrażania skryptów automatyzujących zadania sieciowe
C3	Rozwinięcie umiejętności monitorowania i optymalizacji infrastruktury sieciowej

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Znajomość podstaw działania sieci komputerowych
2	Znajomość podstaw działania komunikacji webowej

Efekty uczenia się	
	W zakresie wiedzy:
EK1	wyjaśnia podstawowe koncepcje programowalnego zarządzania infrastrukturą i siecią, w tym infrastrukturę jako kod, automatyzację sieci i rolę DevOps w zarządzaniu IT
EK2	zna kluczowe protokoły i standardy stosowane w programowalnym zarządzaniu sieciami, takie jak REST API i YANG
EK3	identyfikuje narzędzia i technologie wykorzystywane w środowiskach DevNet
	W zakresie umiejętności:
EK4	tworzy skrypty automatyzujące zadania sieciowe
EK5	wdraża procesy automatyzacji konfiguracji urządzeń sieciowych
EK6	implementuje praktyki monitorowania sieci z wykorzystaniem programowalnych mechanizmów i narzędzi analitycznych

	W zakresie kompetencji społecznych:
EK7	jest gotów do wykazania się umiejętnością dostosowania narzędzi i technologii do potrzeb organizacji, uwzględniając ich specyficzne wymagania biznesowe i techniczne

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Środowisko rozwojowe DevNet
W2	Główne koncepcje rozwoju i wdrażania oprogramowania
W3	Zastosowania i wykorzystanie interfejsów programistycznych aplikacji
W4	Wdrażanie aplikacji w sposób bezpieczny
W5	Automatyzacja zarządzania infrastrukturą
Forma zajęć - laboratoria	
	Treści programowe
L1	Instalacja i konfiguracja środowiska deweloperskiego
L2	Konfiguracja projektu DevNet oraz integracja z popularnymi narzędziami
L3	Wykorzystanie DevNet sandbox do testowania aplikacji i usług
L4	Wprowadzenie do cyklu życia oprogramowania w podejściu DevOps (CI/CD)
L5	Wdrażanie aplikacji na środowisku testowym z wykorzystaniem kontenerów Docker
L6	Tworzenie skryptów wykorzystujących RESTful API do automatyzacji konfiguracji urządzeń sieciowych
L7	Wdrażanie aplikacji z uwzględnieniem praktyk bezpieczeństwa: szyfrowanie danych, kontrola dostępu
L8	Automatyzacja konfiguracji urządzeń sieciowych przy użyciu Ansible: tworzenie playbooków i zarządzanie konfiguracją urządzeń
L9	Definiowanie infrastruktury jako kodu (IaC)

Metody dydaktyczne	
1	wykład informacyjny
2	analiza przypadków
3	ćwiczenia laboratoryjne

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51 %
O2	ocena wykonanych ćwiczeń laboratoryjnych	51 %

Literatura podstawowa	
1	Oh, Daniel, i in. Ansible 2 w praktyce : automatyzacja infrastruktury, zarządzanie konfiguracją i wdrażanie aplikacji. Helion, 2021.

2	Chou E., Zaawansowana inżynieria sieci w Pythonie. Automatyzacja, monitorowanie i zarządzanie chmurą., Helion, 2024.
3	Krief, M., DevOps w praktyce. Wdrażanie narzędzi Terraform, Azure DevOps, Kubernetes i Jenkins. Helion. 2023.

Literatura uzupełniająca	
1	John F. S., Jenkins: The Definitive Guide. Continuous Integration for the Masses., : O'Reilly Media.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	60
Udział w wykładach:	30
Udział w zajęciach laboratoryjnych:	30
Praca własna studenta, w tym:	40
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	20
Przygotowanie do zajęć laboratoryjnych:	20
Łączny czas pracy studenta	100
Sumaryczna liczba punktów ECTS dla przedmiotu	4

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W12++ CB1A_W09++	C1, C2	W1, W2	1	O1
EK 2	CB1A_W12++ CB1A_W09++	C2	W1, W2	1	O1
EK 3	CB1A_W12++ CB1A_W09++	C1, C2	W2, W4, W5	1	O1
EK 4	CB1A_U24++	C1, C2	L4 - L9	2, 3	O2
EK 5	CB1A_U18++	C1, C2, C3	L7, L8, L9	2, 3	O2
EK 6	CB1A_U18++	C1, C2, C3	L1 - L9	2, 3	O2
EK 7	CB1A_K04++	C1, C2, C3	L1 - L9	2, 3	O1, O2

Autor programu:	dr Rafał Stęgiński
Adres e-mail:	r.stegierski@pollub.pl
Jednostka organizacyjna:	Katedra Inteligencji Obliczeniowej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Projekt zespołowy z obszaru bezpieczeństwa aplikacji mobilnych i webowych
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C604.1
Rok:	III
Semestr:	6
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	30
Wykład	
Ćwiczenia	
Laboratorium	
Projekt	30
Liczba punktów ECTS:	6
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Rozwinięcie umiejętności pracy zespołowej w kontekście projektowania i wdrażania rozwiązań z zakresu cyberbezpieczeństwa
C2	Rozwinięcie umiejętności praktycznych w zakresie projektowania, wdrażania i testowania rozwiązań zabezpieczających w aplikacjach mobilnych i webowych
C3	Rozwinięcie umiejętności analitycznych i inżynierskich w zakresie tworzenia kompleksowych rozwiązań bezpieczeństwa IT, z uwzględnieniem specyfiki środowisk mobilnych i webowych

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Znajomość podstawowych zagrożeń bezpieczeństwa cyfrowego oraz metod ich identyfikacji i przeciwdziałania im
2	Znajomość problematyki tworzenia aplikacji mobilnych i internetowych
3	Umiejętność pracy w zespole

Efekty uczenia się	
	W zakresie umiejętności:
EK1	potrafi zaprojektować, wdrożyć i przetestować rozwiązania zabezpieczające dla aplikacji mobilnych i webowych, uwzględniając konkretne zagrożenia i wymagania bezpieczeństwa
EK2	potrafi efektywnie współpracować z członkami zespołu, planować zadania, prowadzić dyskusje i dzielić się obowiązkami, w celu realizacji złożonych projektów z obszaru cyberbezpieczeństwa

EK3	potrafi przygotować dokumentację projektową, przedstawić wyniki pracy zespołowej oraz ocenić skuteczność wdrożonych rozwiązań
	W zakresie kompetencji społecznych:
EK4	jest gotów do odpowiedzialnego pełnienia roli zawodowej specjalisty ds. cyberbezpieczeństwa dbając o terminową realizację powierzonych zadań
EK5	jest gotów do krytycznej analizy efektywności działań zespołowych, dążąc do ciągłego doskonalenia realizowanego projektu

Treści programowe przedmiotu	
Forma zajęć - projekt	
	Treści programowe
P1	Rola pracy zespołowej w kontekście projektów cyberbezpieczeństwa. Przykłady projektów związanych z bezpiecz. aplikacji mobilnych i webowych
P2	Planowanie projektu. Określenie celów i zakresu projektu. Analiza wymagań użytkowników oraz bezpieczeństwa. Opracowanie harmonogramu działań oraz przydzielanie zadań członkom zespołu
P3	Zaprojektowanie aplikacji o wybranej tematyce. Implementacja aplikacji z uwzględnieniem podstawowych funkcjonalności
P4	Analiza zagrożeń i ocena ryzyka. Identyfikacja potencjalnych zagrożeń w aplikacji. Ocena ryzyka i identyfikacja krytycznych punktów w architekturze aplikacji. Wykorzystanie narzędzi i technik do analizy zagrożeń
P5	Implementacja mechanizmów bezpieczeństwa. Projektowanie interfejsów użytkownika z uwzględnieniem zasad bezpieczeństwa
P6	Wdrożenie zaprojektowanych rozwiązań. Testowanie zabezpieczeń. Ocena skuteczności zastosowanych rozwiązań
P7	Przygotowanie i przedstawienie raportu z wynikami projektu

Metody dydaktyczne	
1	analiza przypadków
2	metoda projektu
3	praca wykonywana w grupach

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena przygotowanego projektu	51%
O2	ocena obrony projektu	51%

Literatura podstawowa	
1	Stallings, William i in. Bezpieczeństwo systemów informatycznych : zasady i praktyka. T. 1 i 2. Wyd. Helion, 2019.
2	Jakubiak, Marek i in., Współczesne trendy cyberzagrożeń społeczeństwa informacyjnego. Oficyna Wydawnicza Politechniki Warszawskiej, 2023.

3	Hoffman, Andrew, i in., Bezpieczeństwo nowoczesnych aplikacji internetowych : przewodnik po zabezpieczeniach. Wyd. Helion, 2021.
---	--

Literatura uzupełniająca	
1	Anderson, Ross, Inżyniera zabezpieczeń. Tom I. Przewodnik po budowaniu niezawodnych systemów rozproszonych. Wyd. Naukowe PWN, 2024.
2	Mitnick, Kevin i in. Duch w sieci : moje przygody jako najbardziej poszukiwanego hakera wszech czasów. Wyd. Helion, 2019.
3	Aleks, Nick i in. Black Hat GraphQL : bezpieczeństwo API dla hakerów i pentesterów. Wyd. Helion, 2024.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	30
Udział w zajęciach projektowych:	30
Praca własna studenta, w tym:	120
Przygotowanie projektu:	120
Łączny czas pracy studenta	150
Sumaryczna liczba punktów ECTS dla przedmiotu	6

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_U04+++	C1 - C3	P2 – P6	1 - 3	O1, O2
EK 2	CB1A_U07+++	C1 - C3	P1 – P7	2, 3	O1, O2
EK 3	CB1A_U05+++	C1 - C3	P7	2	O1, O2
EK 4	CB1A_K05++	C1 - C3	P1 – P7	1 - 3	O1, O2
EK 5	CB1A_K01+	C1 - C3	P1 – P7	1 - 3	O1, O2

Autor programu:	dr inż. Joanna Szulżyk-Cieplak; mgr inż. Jacek Zaborko
Adres e-mail:	j.szulzyk-cieplak@pollub.pl; j.zaborko@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Technicznej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Projekt zespołowy z obszaru bezpieczeństwa systemów sieciowych
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C604.2
Rok:	III
Semestr:	6
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	30
Wykład	
Ćwiczenia	
Laboratorium	
Projekt	30
Liczba punktów ECTS:	6
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Rozwinięcie umiejętności pracy zespołowej w kontekście projektowania i wdrażania rozwiązań z zakresu cyberbezpieczeństwa
C2	Rozwinięcie umiejętności praktycznych związanych z projektowaniem, wdrażaniem i testowaniem zabezpieczeń w systemach sieciowych
C3	Rozwinięcie umiejętności analitycznych i inżynierskich w zakresie tworzenia kompleksowych rozwiązań bezpieczeństwa w systemach sieciowych

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Znajomość podstawowych zagrożeń bezpieczeństwa cyfrowego oraz metod ich identyfikacji i przeciwdziałania im
2	Umiejętność pracy w zespole

Efekty uczenia się	
	W zakresie umiejętności:
EK1	projektuje, wdraża i testuje rozwiązania zabezpieczające dla systemów sieciowych, uwzględniając konkretne zagrożenia i wymagania bezpieczeństwa
EK2	potrafi współpracować z członkami zespołu, efektywnie dzieląc zadania i prowadząc dyskusje w celu realizacji projektu
EK3	potrafi przygotować dokumentację projektową oraz przedstawić wyniki pracy zespołowej, w tym zastosowane rozwiązania i uzyskane efekty
	W zakresie kompetencji społecznych:
EK4	jest gotów do odpowiedzialnego pełnienia roli zawodowej specjalisty ds. cyberbezpieczeństwa dbając o terminową realizację powierzonych zadań

EK5	jest gotów do krytycznej analizy efektywność działań zespołowych, dążąc do ciągłego doskonalenia realizowanego projektu
------------	---

Treści programowe przedmiotu	
Forma zajęć - projekt	
	Treści programowe
P1	Przykłady projektów zespołowych z zakresu bezpieczeństwa systemów sieciowych i przemysłowych
P2	Planowanie projektu. Określenie celów i zakresu projektu. Analiza wymagań. Opracowanie harmonogramu działań i podział zadań w zespole
P3	Tworzenie środowiska testowego w wirtualnej sieci
P4	Ocena ryzyka i określenie krytycznych punktów w architekturze sieciowej. Wykorzystanie narzędzi i technik do analizy zagrożeń. Dokumentacja luk w zabezpieczeniach
P5	Tworzenie strategii bezpieczeństwa dla systemów sieciowych. Opracowanie i wdrożenie mechanizmów obronnych. Testowanie skuteczności zabezpieczeń za pomocą symulacji ataków. Analiza wyników testów i wprowadzanie usprawnień
P6	Przygotowanie i przedstawienie raportu z wynikami projektu

Metody dydaktyczne	
1	analiza przypadków
2	metoda projektu
3	praca wykonywana w grupach

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena przygotowanego projektu	51%
O2	ocena obrony projektu	51%

Literatura podstawowa	
1	Stallings, William i in. Bezpieczeństwo systemów informatycznych : zasady i praktyka. T. 1 i 2. Wyd. Helion, 2019.
2	Szymaniec, Sławomir, i in., Utrzymanie ruchu w przemyśle : informatyka i cyberbezpieczeństwo : diagnostyka przemysłowa : praktyka. Wydanie I. Wyd. Naukowe PWN, 2021.
3	Jakubiak, Marek i in., Współczesne trendy cyberzagrożeń społeczeństwa informacyjnego. Oficyna Wydawnicza Politechniki Warszawskiej, 2023.
4	Bravo, Cesar i in. Cyberbezpieczeństwo dla zaawansowanych : skuteczne zabezpieczenia systemu Windows, Linux, IoT i infrastruktury w chmurze. Wyd. Helion, 2023.
5	Kaim, Marcin i in., Bezpieczeństwo w sieci - Jak skutecznie chronić się przed atakami. Wyd. ITSTART, 2020.

Literatura uzupełniająca	
1	Anderson, Ross, Inżyniera zabezpieczeń. Tom I. Przewodnik po budowaniu niezawodnych systemów rozproszonych. Wyd. Naukowe PWN, 2024.
2	Mitnick, Kevin i in. Duch w sieci : moje przygody jako najbardziej poszukiwanego hakera wszech czasów. Wyd. Helion, 2019.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	30
Udział w zajęciach projektowych:	30
Praca własna studenta, w tym:	120
Przygotowanie projektu:	120
Łączny czas pracy studenta	150
Sumaryczna liczba punktów ECTS dla przedmiotu	6

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_U04+++	C1 - C3	P2 - P5	1 - 3	O1, O2
EK 2	CB1A_U07+++	C1 - C3	P1 - P6	2, 3	O1, O2
EK 3	CB1A_U05+++	C1 - C3	P6	2	O1, O2
EK 4	CB1A_K05++	C1 - C3	P1 - P6	1 - 3	O1, O2
EK 5	CB1A_K01+	C1 - C3	P1 - P6	1 - 3	O1, O2

Autor programu:	dr hab. Arkadiusz Syta, profesor uczelni; mgr inż. Jacek Zaborko
Adres e-mail:	a.syta@pollub.pl; j.zaborko@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Technicznej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Analiza deepfake
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C605.1
Rok:	III
Semestr:	6
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	60
Wykład	30
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	4
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zapoznanie z technikami używanymi do generowania deepfake oraz zagrożeń, które one ze sobą niosą
C2	Poznanie metod wykorzystywanych do badania obrazów oraz plików wideo i audio pod kątem ich wiarygodności
C3	Umiejętność doboru algorytmów wykorzystujących uczenie maszynowe i sieci neuronowe, w zastosowaniu do rozpoznawania i identyfikowania deepfake

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Podstawy uczenia maszynowego
2	Podstawy programowania

Efekty uczenia się	
	W zakresie wiedzy:
EK1	wskazuje zastosowanie sieci generatywnych do manipulowania obrazem i dźwiękiem w celu tworzenia fałszywych treści
EK2	charakteryzuje techniki rozpoznawania fałszywych treści
	W zakresie umiejętności:
EK3	opracowuje proste sieci generatywne i wykorzystuje je do tworzenia fikcyjnych treści
EK4	identyfikuje treści wygenerowane przez sztuczną inteligencję w obrazach i nagraniach audio
	W zakresie kompetencji społecznych:
EK5	jest gotów do krytycznej oceny treści cyfrowych oraz propagowania wiedzy o etycznych aspektach związanych z technologiami deepfake

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Wprowadzenie do problematyki pozyskiwania i analizy danych
W2	Przegląd AI Search Engines
W3	Geneza i rozwój wywiadu gospodarczego
W4	Eksploracja cyfrowych śmieci
W5	Wykrywanie fałszerstw fotografii i porównywanie plików graficznych
W6	Techniki analizy plików audio
W7	Techniki analizy plików video
Forma zajęć - laboratoria	
	Treści programowe
L1	Techniki generowania deepfake
L2	Podstawowe techniki detekcji deepfake
L3	Analiza plików graficznych
L4	Analiza plików dźwiękowych
L5	Analiza plików video
L6	Techniki głębokie do wykrywania deepfake

Metody dydaktyczne	
1	wykład informacyjny
2	ćwiczenia laboratoryjne

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena wykonanych ćwiczeń laboratoryjnych	51%

Literatura podstawowa	
1	Foster, D., i in.: Deep learning i modelowanie generatywne : jak nauczyć komputer malowania, pisanie, komponowania i grania. Gliwice: Helion SA, 2021.
2	Marcin Szeliga. Praktyczne uczenie maszynowe. 1. wyd. Warszawa: Wyd. Naukowe PWN, 2019.

Literatura uzupełniająca	
1	Garreta R., Guillermo M.: Learning Scikit-Learn: Machine Learning in Python. 1st ed. Birmingham: Packt Publishing, Limited, 2013.
2	Goodfellow I., i in.: Deep Learning. Cambridge, MA ; The MIT Press, 2017.

3	Shanmugamani R.: Deep Learning for Computer Vision : Expert Techniques to Train Advanced Neural Networks Using TensorFlow and Keras. 1st edition. Birmingham, England: Paths International Ltd, 2018.
---	---

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	60
Udział w wykładach:	30
Udział w zajęciach laboratoryjnych:	30
Praca własna studenta, w tym:	40
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	20
Przygotowanie do zajęć laboratoryjnych:	20
Łączny czas pracy studenta	100
Sumaryczna liczba punktów ECTS dla przedmiotu	4

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W18++	C1	W1-W7	1	O1
EK 2	CB1A_W11+++	C2, C3	W1-W7	1	O1
EK 3	CB1A_U09++ CB1A_U12++	C1	L1-L6	2	O2
EK 4	CB1A_U09++ CB1A_U12++	C2, C3	L1-L6	2	O2
EK 5	CB1A_K03+	C1, C2, C3	W1- W7 L1-L6	1,2	O1,O2

Autor programu:	dr Adam Kiersztyn; mgr Krystyna Kiersztyn; mgr inż. Albert Rachwał
Adres e-mail:	a.kiersztyn@pollub.pl; k.kiersztyn@pollub.pl; a.rachwal@pollub.pl
Jednostka organizacyjna:	Katedra Inteligencji Obliczeniowej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Detekcja anomalii w strumieniach danych
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C605.2
Rok:	III
Semestr:	6
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	60
Wykład	30
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	4
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zapoznanie z wybranymi metodami wykrywania anomalii i danych odstających
C2	Wykształcenie umiejętności stosowania technik wykrywania anomalii w praktycznych przykładach

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Znajomość podstaw matematyki
2	Umiejętność programowania w dowolnym języku

Efekty uczenia się	
	W zakresie wiedzy:
EK1	zna techniki wykrywania anomalii i danych odstających
EK2	opisuje strumień danych za pomocą szeregów czasowych
	W zakresie umiejętności:
EK3	stosuje techniki wykrywania anomalii i danych odstających
EK4	dobiera techniki wykrywania anomalii do konkretnych problemów
	W zakresie kompetencji społecznych:
EK5	jest gotów do podejmowania wyzwań związanych z wykorzystaniem technik wykrywania anomalii i danych odstających w rzeczywistych zagadnieniach

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Pojęcie i przykłady szeregów czasowych

W2	Badanie integralności szeregów czasowych
W3	Wykrywanie outlierów w szeregach czasowych
W4	Wykrywanie anomalii w szeregach czasowych
W5	Szereg czasowy a strumień danych
W6	Przegląd technik wykrywania anomalii w strumieniach danych
W7	Porównanie efektywności metod wykrywania anomalii

Forma zajęć - laboratoria

	Treści programowe
L1	Metody opisu szeregów czasowych
L2	Analiza własności szeregów czasowych
L3	Analiza integralności szeregów czasowych
L4	Wykrywanie wartości odstających w szeregach czasowych
L5	Wykrywanie anomalii w szeregach czasowych
L6	Reprezentacja strumienia danych za pomocą szeregów czasowych
L7	Wizualizacja wybranych własności strumieni danych
L8	Wykrywanie anomalii w strumieniach danych

Metody dydaktyczne

1	wykład informacyjny
2	ćwiczenia laboratoryjne

Metody i kryteria oceny

Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51 %
O2	ocena wykonanych ćwiczeń laboratoryjnych	51 %

Literatura podstawowa

1	Kozłowski, Edward. Analiza i identyfikacja szeregów czasowych. Politechnika Lubelska, 2015.
----------	---

Literatura uzupełniająca

1	Milo, Władysław, Analiza szeregów czasowych, Uniwersytet Łódzki, 1983.
2	Kiersztyn, Adam, Karczmarek, Paweł, Kiersztyn, Krystyna, Pedrycz, Witold, Detection and Classification of Anomalies in Large Datasets on the Basis of Information Granules, IEEE Transactions on Fuzzy Systems, 2022-08, Vol.30 (8), p.2850-2860.
3	Karczmarek, Paweł, Kiersztyn, Adam, Pedrycz, Witold, AI, Ebru, K-Means-based isolation forest, Knowledge-based systems, 2020-05, Vol.195, p.105659,.
4	Kiersztyn, Krystyna, Kiersztyn, Adam, Fuzzy Rule-based Outlier Detector, 2022 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), 2022, p.1-7.

Obciążenie pracą studenta

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	60
Udział w wykładach:	30
Udział w zajęciach laboratoryjnych:	30
Praca własna studenta, w tym:	40
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	20
Przygotowanie do zajęć laboratoryjnych:	20
Łączny czas pracy studenta	100
Sumaryczna liczba punktów ECTS dla przedmiotu	4

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W18++ CB1A_W11+++	C2	W3-W7	1	O1
EK 2	CB1A_W18++ CB1A_W11+++	C1	W1, W5	1	O1
EK 3	CB1A_U12++ CB1A_U14++	C1,C2	L1,L2,L6,L7	2	O2
EK 4	CB1A_U14++	C1,C2	L7,L8	2	O2
EK 5	CB1A_K05+	C1,C2	W1-W7 L1-L8	1,2	O1,O2

Autor programu:	dr Adam Kiersztyn; mgr Krystyna Kiersztyn
Adres e-mail:	a.kiersztyn@pollub.pl; k.kiersztyn@pollub.pl
Jednostka organizacyjna:	Katedra Inteligencji Obliczeniowej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Technika cyfrowa i systemy SOC
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C606.1
Rok:	III
Semestr:	6
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	60
Wykład	30
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	4
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu

C1	Zdobycie wiedzy na temat kluczowych wyzwań i problemów, przed jakimi stoją usługi SOC
C2	Zdobycie umiejętności rozpoznawania i reagowania na incydenty bezpieczeństwa, w tym identyfikacji cyberataków oraz zrozumienia, jak SOC reaguje na incydenty, takie jak włamania czy ataki z użyciem złośliwego oprogramowania
C3	Zrozumienie, w jaki sposób SOC analizuje dane i opracowuje raporty dotyczące zagrożeń

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1	Podstawowa wiedza z obszaru sieci komputerowych
2	Znajomość podstawowych zagadnień z zakresu cyberbezpieczeństwa, takich jak firewalle, antywirusy, szyfrowanie, uwierzytelnianie i autoryzacja
3	Umiejętność analitycznego myślenia oraz zdolności do myślenia w sposób logiczny i przyczynowo-skutkowy

Efekty uczenia się

	W zakresie wiedzy:
EK1	zna podstawowe pojęcia i zasady działania technik cyfrowych oraz ich zastosowanie w systemach SOC
EK2	rozumie strukturę, funkcje oraz zadania SOC w monitorowaniu i ochronie systemów IT oraz zna narzędzia i technologie wykorzystywane w SOC do wykrywania, analizy i reagowania na incydenty bezpieczeństwa
EK3	ma wiedzę na temat zagrożeń i rodzajów cyberataków oraz metod ich wykrywania i zapobiegania im

	W zakresie umiejętności:
EK4	potrafi monitorować ruch sieciowy i analizować dzienniki systemowe w celu wykrywania zagrożeń i podejrzanych aktywności
EK5	rozpoznaje i klasyfikuje incydenty bezpieczeństwa oraz podejmuje odpowiednie działania naprawcze
	W zakresie kompetencji społecznych:
EK6	jest gotów do odpowiedzialnego pełnienia ról zawodowych w obszarze cyberbezpieczeństwa, wykazując się dbałością o bezpieczeństwo cyfrowe i przestrzeganiem zasad etyki zawodowej

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Pamięci cyfrowe, rodzaje pamięci, RAM, ROM, Flash i ich zastosowanie w systemach cyfrowych
W2	Systemy mikroprocesorowe i mikrokontrolery, zasada działania mikroprocesorów i mikrokontrolerów w systemach cyfrowych
W3	Architektura komputerów cyfrowych, opis działania jednostek centralnych, magistrali danych i pamięci
W4	Podstawowe zagrożenia cyberbezpieczeństwa, przegląd rodzajów ataków
W5	Wprowadzenie do Security Operations Center (SOC), zadania i struktura SOC oraz jego rola w zabezpieczeniach
W6	Systemy SIEM (Security Information and Event Management)
W7	Narzędzia i techniki stosowane w SOC do monitorowania sieci i wykrywania zagrożeń
W8	Wykrywanie zagrożeń i incydentów bezpieczeństwa
W9	Procesy i procedury stosowane w SOC do szybkiego i skutecznego reagowania na incydenty
W10	Podstawy kryptografii, szyfrowania danych i ich rola w zabezpieczaniu informacji
W11	Zarządzania incydentami, w tym komunikacja, raportowanie i analiza post-mortem
W12	Zastosowanie narzędzi automatyzacji w procesie wykrywania zagrożeń i reakcji na incydenty
W13	Systemy IDS/IPS (Intrusion Detection/Prevention Systems)
Forma zajęć - laboratoria	
	Treści programowe
L1	Praca z interfejsami; I2C, SPI i UART
L2	Analiza logów systemowych i sieciowych, w tym ruchu sieciowego i aktywności użytkowników
L3	Monitorowanie ruchu sieciowego z Wireshark
L4	Przeprowadzanie skanowania podatności systemów IT z wykorzystaniem skanera Nessus oraz analiza wyników
L5	Analizowaniu logów systemowych i wykrywanie nieautoryzowanych działań

L6	Praca z zaporami sieciowymi – konfiguracja reguł i analiza ruchu sieciowego, który jest blokowany lub dozwolony
L7	Zarządzanie kontami użytkowników i kontrola dostępu
L8	Szyfrowanie danych i zarządzanie kluczami
L9	Konfigurowanie systemu IDS/IPS (Intrusion Detection/Prevention System)
L10	Symulacja i testowanie zabezpieczeń w sieciach bezprzewodowych
L11	Konfigurowanie źródeł logów i tworzenie reguł detekcji incydentów w systemach SIEM
L12	Analiza zagrożeń w urządzeniach IoT i zabezpieczanie sieci IoT przed atakami, takimi jak przejęcie kontroli nad urządzeniami
L13	Monitoring sieci i wykrywanie nietypowego ruchu

Metody dydaktyczne	
1	wykład informacyjny
2	ćwiczenia laboratoryjne
3	metoda symulacji

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena odpowiedzi ustnej	51%
O2	ocena wykonanych ćwiczeń laboratoryjnych	51%
O3	ocena wykonanych symulacji	51%

Literatura podstawowa	
1	Banasiński, Cezary, i in. Cyberbezpieczeństwo. Wolters Kluwer, 2020.
2	Joseph Steinberg, Cyberbezpieczeństwo dla bystrzaków. Wydanie II, 2023, Wydawnictwo: Helion.
3	Marek Górka, Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku, ISBN: 9788379303342, 2014.

Literatura uzupełniająca	
1	Pisarewicz, Piotr, and Jerzy Podlewski. "Cyberbezpieczeństwo Polskiego Sektora Ubezpieczeniowego w Kontekście Krajowych i Unijnych Regulacji Prawnych." Bank i Kredyt, vol. 54, no. No. 5, 2023, pp. 557–76, https://doi.org/10.5604/01.3001.0054.5716 .
2	Magdalena Molendowska, Rafał Miernik, Bezpieczeństwo w cyberprzestrzeni - wybrane zagadnienia, ISBN: 9788381804158, 2020.
3	Wojciech Brzeziński, Agata Kaźmierska, Strefy cyberwojny, Wydawco Oficyna 4eM, 2021.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności

Godziny kontaktowe z wykładowcą, w tym:	60
Udział w wykładach:	30
Udział w zajęciach laboratoryjnych:	30
Praca własna studenta, w tym:	40
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	20
Przygotowanie do zajęć laboratoryjnych:	20
Łączny czas pracy studenta	100
Sumaryczna liczba punktów ECTS dla przedmiotu	4

Macierz efektów uczenia się					
Symbol przedmiotowe go efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W03++	C1 - C3	W1 - W3, W7, W12	1, 2	O1
EK 2	CB1A_W03++ CB1A_W15++	C1 - C3	W5 - W13	1, 2	O1
EK 3	CB1A_W15++	C1 - C3	W4, W7, W8, W10 - W13	1, 2	O1
EK 4	CB1A_U12++ CB1A_U16++	C1 - C3	L1 - L13	3, 4	O2, O3
EK 5	CB1A_U12++ CB1A_U16++	C1 - C3	L1 - L13	3, 4	O2, O3
EK 6	CB1A_K05+	C1 - C3	W1 - W13 L1 - L13	1 - 4	O1, O2, O3

Autor programu:	dr hab. Ernest Gnapowski, profesor uczelni
Adres e-mail:	e.gnapowski@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Stosowanej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Steganografia i cyfrowe znaki wodne
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C606.2
Rok:	III
Semestr:	6
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	60
Wykład	30
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	4
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu

C1	Zapoznanie z podstawowymi technikami steganografii i cyfrowych znaków wodnych
C2	Wyszkolenie umiejętności stosowania cyfrowych znaków wodnych i steganografii do zabezpieczania informacji

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1	Znajomość podstaw programowania
2	Umiejętność pracy z dokumentacją techniczną

Efekty uczenia się

	W zakresie wiedzy:
EK 1	rozdziela podstawowe pojęcia steganografii i cyfrowych znaków wodnych
EK 2	charakteryzuje różne techniki zabezpieczeń treści cyfrowych
	W zakresie umiejętności:
EK3	stosuje techniki steganografii i cyfrowych znaków wodnych w praktycznych zastosowaniach
EK4	opracowuje cyfrowe znaki wodne i steganograficzne struktury do ochrony treści
	W zakresie kompetencji społecznych:
EK5	jest gotów do uznawania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych związanych ze steganografią i cyfrowymi znakami wodnymi, doceniając rolę ciągłego uczenia się i dzielenia się doświadczeniami w kontekście zapewniania bezpieczeństwa cyfrowego

Treści programowe przedmiotu

Forma zajęć - wykłady	
	Treści programowe
W1	Wprowadzenie do steganografii
W2	Klasyfikacja metod steganografii
W3	Techniki ukrywania danych
W4	Narzędzia steganograficzne
W5	Techniki ukrywania danych w protokołach sieciowych
W6	Cyfrowe znaki wodne
W7	Cechy cyfrowych znaków wodnych
W8	Stegoanaliza
W9	Steganografia i znakowanie wodne stosowane przy zabezpieczaniu danych
W10	Kierunki rozwoju steganografii

Forma zajęć - laboratoria	
	Treści programowe
L1	Ukrywanie informacji w obrazach
L2	Ukrywanie informacji w plikach multimedialnych
L3	Cyfrowe znaki wodne
L4	Cyfrowe znaki wodne odporne na kompresję i transformacje
L5	Wykrywanie i ekstrakcja znaków wodnych
L6	Ukrywanie danych w protokołach sieciowych
L7	Ocena odporności technik steganografii
L8	Oprogramowanie steganograficzne

Metody dydaktyczne	
1	wykład informacyjny
2	dyskusja dydaktyczna
3	praca wykonywana indywidualnie
4	ćwiczenia laboratoryjne

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena wykonanych ćwiczeń laboratoryjnych	51%
O3	ocena aktywności w trakcie zajęć	51%

Literatura podstawowa	
1	Mosorov, Volodymyr. Steganografia cyfrowa : sztuka ukrywania informacji. Wyd. Uniwersytetu Łódzkiego, 2013.

Literatura uzupełniająca

1	Yahya, Abid. Steganography Techniques for Digital Images. 1st ed. 2019. Springer International Publishing, 2019.
2	Cox, I. J. (Ingemar J.). Digital Watermarking and Steganography. 2nd ed. Morgan Kaufmann Publishers, 2008.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	60
Udział w wykładach:	30
Udział w zajęciach laboratoryjnych:	30
Praca własna studenta, w tym:	40
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	20
Przygotowanie do zajęć laboratoryjnych:	20
Łączny czas pracy studenta	100
Sumaryczna liczba punktów ECTS dla przedmiotu	4

Macierz efektów uczenia się					
Symbol przedmiotowe go efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W11++	C1	W1-W10	1, 2	O1
EK 2	CB1A_W07++	C1	W1-W10	1, 2	O1
EK 3	CB1A_U19++	C2	L1-L8	3, 4	O2, O3
EK 4	CB1A_U15+++	C2	L1-L8	3, 4	O2, O3
EK 5	CB1A_K02+	C1	W1-W10	1, 2	O1

Autor programu:	dr hab. Paweł Karczmarek, profesor uczelni; dr inż. Łukasz Gałka
Adres e-mail:	p.karczmarek@pollub.pl; l.galka@pollub.pl
Jednostka organizacyjna:	Katedra Inteligencji Obliczeniowej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Najnowsze trendy w cyberbezpieczeństwie
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C607.1
Rok:	III
Semestr:	6
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	30
Wykład	30
Ćwiczenia	
Laboratorium	
Projekt	
Liczba punktów ECTS:	2
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zapoznanie z najnowszymi technologiami i narzędziami stosowanymi w zabezpieczaniu sieci, systemów oraz danych
C2	Zrozumienie najnowszych typów zagrożeń cyfrowych wykorzystywanych przez cyberprzestępców
C3	Poznanie najnowszych technologii i narzędzi stosowanych w zabezpieczaniu sieci, systemów i danych

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Znajomość podstawowych zagadnień związanych z architekturą komputerów, systemami operacyjnymi, sieciami komputerowymi oraz protokołami komunikacyjnymi
2	Znajomość zasad działania internetu, DNS, sieci VPN, protokołów komunikacyjnych, adresowania IP oraz zasad działania aplikacji webowych
3	Znajomość podstawowych zasad ochrony systemów komputerowych

Efekty uczenia się	
	W zakresie wiedzy:
EK1	zna i rozumie nowoczesne technologie i narzędzia stosowane w ochronie danych, takie jak kryptografia, systemy IDS/IPS, firewalle, oraz techniki związane z zabezpieczaniem chmur obliczeniowych
EK2	ma wiedzę na temat najnowszych zagrożeń w cyberprzestrzeni
	W zakresie kompetencji społecznych:

EK3	jest gotów do wypełniania zobowiązań społecznych oraz inicjowania działań na rzecz środowiska społecznego związanych z podnoszeniem świadomości na temat cyberzagrożeń
------------	--

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Wprowadzenie do cyberbezpieczeństwa, kluczowe pojęcia, zagrożenia i cele
W2	Sztuczna inteligencja i uczenie maszynowe w cyberbezpieczeństwie
W3	Cyberbezpieczeństwo w kontekście Internetu Rzeczy (IoT)
W4	Zagrożenia wynikające z rozwoju technologii 5G
W5	Bezpieczeństwo w chmurze obliczeniowej
W6	Ransomware jako rosnące zagrożenie dla przedsiębiorstw i instytucji
W7	Ataki z wykorzystaniem sztucznej inteligencji
W8	Phishing i jego zaawansowane formy
W9	Rozwój narzędzi SIEM (Security Information and Event Management)
W10	Bezpieczeństwo systemów autonomicznych i pojazdów
W11	Ataki na systemy operacyjne i firmware
W12	Bezpieczeństwo aplikacji mobilnych
W13	Technologie blockchain i ich wpływ na bezpieczeństwo
W14	Cyberbezpieczeństwo w przemyśle 4.0

Metody dydaktyczne	
1	wykład informacyjny
2	dyskusja dydaktyczna

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena odpowiedzi ustnej	51%

Literatura podstawowa	
1	Wojciech Brzeziński, Agata Kaźmierska, Strefy cyberwojny, Wydawco Oficyna 4eM, 2021.
2	Joseph Steinberg, Cyberbezpieczeństwo dla bystrzaków. Wydanie II, 2023, Wydawnictwo: Helion.
3	Marek Górka, Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku, ISBN: 9788379303342, 2014.

Literatura uzupełniająca	
1	Magdalena Molendowska, Rafał Miernik, Bezpieczeństwo w cyberprzestrzeni - wybrane zagadnienia, ISBN: 9788381804158, 2020.

2	Pisarewicz, Piotr, and Jerzy Podlewski. "Cyberbezpieczeństwo Polskiego Sektora Ubezpieczeniowego w Kontekście Krajowych i Unijnych Regulacji Prawnych." Bank i Kredyt, vol. 54, no. No. 5, 2023, pp. 557-76, https://doi.org/10.5604/01.3001.0054.5 .
3	William Stallings, Lawrie Brown, Bezpieczeństwo systemów informatycznych. Zasady i praktyka. Wydanie IV. Tom 1, 2023, Wydawnictwo: Helion.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	30
Udział w wykładach:	30
Praca własna studenta, w tym:	20
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	20
Łączny czas pracy studenta	50
Sumaryczna liczba punktów ECTS dla przedmiotu	2

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W18++	C1 - C3	W1 - W14	1, 2	O1
EK 2	CB1A_W02++	C1 - C3	W1 - W14	1, 2	O1
EK 3	CB1A_K03+	C1 - C3	W1 - W14	1, 2	O1

Autor programu:	dr hab. Ernest Gnapowski, profesor uczelni
Adres e-mail:	e.gnapowski@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Stosowanej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Zaawansowane technologie w cyberbezpieczeństwie
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C607.2
Rok:	III
Semestr:	6
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	30
Wykład	30
Ćwiczenia	
Laboratorium	
Projekt	
Liczba punktów ECTS:	2
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język angielski/język niemiecki

Cele przedmiotu	
C1	Zapoznanie z najważniejszymi problemami i wyzwaniami współczesnego cyberbezpieczeństwa
C2	Rozwijanie krytycznego myślenia w ocenie skuteczności nowych rozwiązań w ochronie systemów informatycznych
C3	Przygotowanie do wdrażania innowacyjnych praktyk i narzędzi z obszaru cyberbezpieczeństwa w środowisku zawodowym

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Podstawowa znajomość zagadnień z zakresu cyberbezpieczeństwa i sieci komputerowych
2	Umiejętność analitycznego myślenia i pracy z informacjami z różnych źródeł

Efekty uczenia się	
	W zakresie wiedzy:
EK1	zna i rozumie najnowsze trendy i technologie stosowane w bezpieczeństwie cyfrowym
EK2	rozumie wyzwania związane z implementacją nowych technologii w kontekście cyberbezpieczeństwa
	W zakresie kompetencji społecznych:
EK3	jest gotów do krytycznej analizy dostępnych rozwiązań i rekomendowania najlepszych praktyk w obszarze cyberbezpieczeństwa

Treści programowe przedmiotu

Forma zajęć - wykłady	
	Treści programowe
W1	Ewolucja cyberbezpieczeństwa. Zmieniające się środowisko zagrożeń cybernetycznych
W2	Ewolucja cyberzagrożeń i nowe wektory ataków. Analiza najnowszych technik ataków. Case study: analiza ostatnich incydentów bezpieczeństwa
W3	Rola innowacji technologicznych w cyberbezpieczeństwie
W4	Najnowsze trendy w cyberbezpieczeństwie
W5	Wpływ przepisów prawnych i regulacji na strategię cyberbezpieczeństwa
W6	Etyka w cyberbezpieczeństwie i odpowiedzialność społeczna

Metody dydaktyczne	
1	wykład informacyjny
2	analiza przypadków

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena odpowiedzi ustnej	51%

Literatura podstawowa	
1	Audun, Jøsang, Cybersecurity: Technology and Governance. Wyd. Springer, 2024.
2	Gonzalez, Joaquin, i in., Cybersecurity : Current Writings on Threats and Protection. McFarland & Company, Inc., Publishers, 2019.
3	Brooks, Chuck, Inside Cyber. Wiley, 2024.

Literatura uzupełniająca	
1	Jakobsen, Adam, Practical Cyber Intelligence. Wiley, 2024.
2	Nour, El Madhoun, i in. Building Cybersecurity Applications with Blockchain and Smart Contracts. Springer International Publishing AG, 2024.
3	Cochran, Kodi, Cybersecurity Essentials: Practical Tools for Today's Digital Defenders. Berkeley, CA: Apress L. P, 2024.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	30
Udział w wykładach:	30
Praca własna studenta, w tym:	20
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	20

Łączny czas pracy studenta	50
Sumaryczna liczba punktów ECTS dla przedmiotu	2

Macierz efektów uczenia się					
Symbol przedmiotowe go efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W02++	C1 - C3	W1 - W6	1, 2	O1
EK 2	CB1A_W18++	C1 - C3	W1 - W6	1, 2	O1
EK 3	CB1A_K01+	C1 - C3	W1 - W6	1, 2	O1

Autor programu:	dr hab. Ernest Gnapowski, profesor uczelni
Adres e-mail:	e.gnapowski@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Stosowanej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Biały wywiad
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	CB-1-S-C701
Rok:	IV
Semestr:	7
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	30
Wykład	15
Ćwiczenia	
Laboratorium	15
Projekt	
Liczba punktów ECTS:	2
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zapoznanie z podstawowymi metodami białego wywiadu (OSINT) oraz jego znaczeniem w kontekście cyberbezpieczeństwa
C2	Przekazanie wiedzy na temat źródeł informacji dostępnych publicznie i metod ich pozyskiwania
C3	Rozwinięcie umiejętności praktycznego wykorzystywania narzędzi OSINT do analizy informacji i identyfikacji zagrożeń
C4	Ukształtowanie świadomości etycznej i prawnej związanej z pozyskiwaniem informacji z otwartych źródeł

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Znajomość kluczowych zagadnień z zakresu cyberbezpieczeństwa
2	Ogólna wiedza na temat sieci komputerowych
3	Zdolność analitycznego myślenia i interpretacji dokumentów normatywnych
4	Podstawowa znajomość narzędzi wyszukiwania informacji w Internecie

Efekty uczenia się	
	W zakresie wiedzy:
EK1	zna podstawowe pojęcia, metody i narzędzia związane z białym wywiadem
EK2	rozumie możliwości i ograniczenia wykorzystywania informacji z otwartych źródeł w analizie zagrożeń
EK3	zna podstawy prawne i etyczne związane z prowadzeniem działań OSINT
	W zakresie umiejętności:
EK4	potrafi zastosować narzędzia i techniki OSINT do pozyskiwania i analizy danych

EK5	potrafi ocenić wiarygodność i relewantność informacji znalezionych w otwartych źródłach
EK6	potrafi przygotować prosty raport OSINT z zastosowaniem odpowiednich metod i technik
	W zakresie kompetencji społecznych:
EK7	jest gotów do przestrzegania norm prawnych i etycznych w zakresie pozyskiwania i przetwarzania informacji

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Wprowadzenie do OSINT: definicje, kontekst, zastosowania w cyberbezpieczeństwie
W2	Kategorie źródeł informacji: media społecznościowe, fora, bazy danych, rejestry, WHOIS
W3	Metody wyszukiwania informacji i analiza powiązań
W4	Prawne i etyczne aspekty OSINT
W5	Przegląd narzędzi wspomagających OSINT
W6	Studium przypadków: OSINT w praktyce (incydenty, analiza celów, przeciwdziałanie dezinformacji)
W7	Raportowanie i prezentacja wyników OSINT
Forma zajęć - laboratoria	
	Treści programowe
L1	Konfiguracja narzędzi OSINT i środowisk pracy
L2	Wyszukiwanie danych personalnych i technicznych (IP, DNS, metadane)
L3	Analiza aktywności w mediach społecznościowych i forach
L4	Tworzenie map powiązań i zależności
L5	Użycie wyszukiwarek specjalistycznych i technik eksploracji
L6	Ocena wiarygodności i filtrowanie informacji
L7	Opracowanie mini-raportu OSINT

Metody dydaktyczne	
1	wykład informacyjny
2	analiza przypadków
3	ćwiczenia laboratoryjne
4	przygotowanie sprawozdania
5	praca wykonywana w grupach

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena wykonanych ćwiczeń laboratoryjnych	51%

O3	ocena wykonanych sprawozdań laboratoryjnych	51%
----	---	-----

Literatura podstawowa	
1	Kuciel, Dawid, OSINT. Sztuka zdobywania informacji. Wydawnictwo DK Group Dawid Kuciel, 2023.
2	Wosiński, Krzysztof, Bezpieczeństwo osób i systemów IT z wykorzystaniem białego wywiadu : OSINT. Wydanie I. Wydawnictwo Naukowe PWN SA, 2024.

Literatura uzupełniająca	
1	Baker, Rae, Prawdziwa głębia OSINT. Odkryj wartość danych Open Source Intelligence. Wydawnictwo Helion, 2024.
2	Wosiński, Krzysztof, OSINT: nowy wymiar poszukiwań w sieci. Wydawnictwo: Securitum, 2024.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	30
Udział w wykładach:	15
Udział w zajęciach projektowych:	15
Praca własna studenta, w tym:	20
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	10
Przygotowanie projektu:	10
Łączny czas pracy studenta	50
Sumaryczna liczba punktów ECTS dla przedmiotu	2

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W04+++	C1, C2	W1 – W7	1, 2	O1
EK 2	CB1A_W04+++ CB1A_W15++	C1, C2	W1 – W6	1, 2	O1
EK 3	CB1A_W13+++	C1, C2	W5	1	O1
EK 4	CB1A_U01+++ CB1A_U21+++	C3, C4	L1 – L5	3 - 5	O2, O3

EK 5	CB1A_U01+++ CB1A_U21+++	C3, C4	L6	3 - 5	O2, O3
EK 6	CB1A_U05++ CB1A_U03++	C3, C4	L7	3 - 5	O2, O3
EK 7	CB1A_K05+++	C1 - C4	W1 - W7, L1 - L7	1 - 4	O1 - O3

Autor programu:	dr inż. Joanna Szulżyk-Cieplak
Adres e-mail:	j.szulzyk-cieplak@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Technicznej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Praktyczne aspekty cyberwojny
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C702.1
Rok:	IV
Semestr:	7
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	60
Wykład	15
Ćwiczenia	
Laboratorium	45
Projekt	
Liczba punktów ECTS:	4
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zrozumienie technik i narzędzi cyberataków oraz metod ochrony i zabezpieczeń
C2	Rozwijanie umiejętności analizy i reagowania na niepożądane incydenty w cyberprzestrzeni
C3	Poznanie aspektów prawnych i etycznych związanych z cyberwojną i cyberprzestępczością

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Posiada umiejętność identyfikowania problemów i szukania skutecznych rozwiązań
2	Posiada wiedzę dotyczącą konfiguracji sieci lokalnej i obsługa narzędzi
3	Ma gotowość do pracy w środowisku dynamicznie zmieniających się technologii i zagrożeń

Efekty uczenia się	
	W zakresie wiedzy:
EK1	zna i rozumie podstawy działania cyberprzestępczości
EK2	definiuje i wskazuje zastosowania technologii stosowanych w cyberświecie i związane z nimi zagrożenia
EK3	zna typy ataków na różnego rodzaju sieci i instytucje oraz możliwości ich ograniczenia oraz rozumie cykl życia ataku cybernetycznego
	W zakresie umiejętności:
EK4	potrafi posługiwać się dedykowanymi narzędziami do rozpoznawania i ograniczania cyberataków
EK5	potrafi zabezpieczyć dane przed cyberprzestępczością

EK6	potrafi planować i przeprowadzać symulacje komputerowe dotyczące bezpieczeństwa sieci i danych
	W zakresie kompetencji społecznych:
EK5	jest gotów do działań na rzecz szerzenia świadomości stosowania zabezpieczeń danych

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Cyberwojny od pierwszych ataków do współczesnych konfliktów
W2	Cyberwojna, a wojna informacyjna, manipulacja i dezinformacja
W3	Praktyczne aspekty prowadzenia operacji ofensywnych w cyberprzestrzeni
W4	Prawo i etyka w cyberwojnie
W5	Cyberwojna hybrydowa, połączenie działań cyfrowych i fizycznych
W6	Cyberszpiegostwo w sieci i życiu codziennym
W7	Ewolucja narzędzi cyberwojny od malware do zaawansowanych exploitów
W8	Budowanie narodowych strategii cyberbezpieczeństwa
W9	Cyfrowe ślady i ich wykorzystanie
W10	Rola "dark webu" i kryptowalut w finansowaniu cyberataków
W11	Psychocybernetyka - jak cyberataki wpływają na psychologię społeczeństw i jednostek
W12	Rola chmur obliczeniowych w cyberkonfliktach
W13	Blockchain jako narzędzie w cyberkonfliktach
W14	Cyberwojna i ochrona danych
Forma zajęć - laboratoria	
	Treści programowe
L1	Analiza i wykrywanie złośliwego oprogramowania
L2	Wykrywanie i neutralizacja ataków phishingowych
L3	Budowa i obrona infrastruktury serwerowej w warunkach symulowanego cyberataku
L4	Forensyka cyfrowa, odzyskiwanie danych i analiza incydentów
L5	Ataki na infrastrukturę Wi-Fi i jej zabezpieczenie
L6	Tworzenie fałszywych informacji i analiza ich wpływu na opinię publiczną
L7	Testowanie infrastruktury chmurowej pod kątem bezpieczeństwa
L8	Monitoring sieci i wykrywanie nietypowego ruchu
L9	Zarządzanie incydentami bezpieczeństwa w symulowanym środowisku
L10	Cyberryzyko w systemach IoT i urządzeniach wbudowanych
L11	Cyberbezpieczeństwo w sieciach 5G, szanse i zagrożenia w czasach konfliktów
L12	Automatyczne wykrywanie anomalii w logach sieciowych
L13	Analiza technik antywłamaniowych w nowoczesnych systemach operacyjnych
L14	Zastosowanie wirtualizacji do izolacji zagrożeń

Metody dydaktyczne	
1	wykład informacyjny
2	dyskusja dydaktyczna
3	ćwiczenia laboratoryjne
4	metoda symulacji

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena odpowiedzi ustnej	51%
O2	ocena wykonanych ćwiczeń laboratoryjnych	51%
O3	ocena wykonanych symulacji	51%

Literatura podstawowa	
1	Klimburg, Alexander, The Darkening Web: The War for Cyberspace, Penguin Press, New York 2017.
2	Marek, Górka, Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku, ISBN: 9788379303342, 2014.
3	Wojciech, Brzeziński, Agata, Kaźmierska, Strefy cyberwojny, Wydawco Oficyna 4eM, 2021.

Literatura uzupełniająca	
1	Buchanan, Ben, The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations, Oxford University Press, New York 2017.
2	Pisarewicz, Piotr, and Jerzy Podlewski. "Cyberbezpieczeństwo Polskiego Sektora Ubezpieczeniowego w Kontekście Krajowych i Unijnych Regulacji Prawnych." Bank i Kredyt, vol. 54, no. No. 5, 2023, pp. 557–76, https://doi.org/10.5604/01.3001.0054.5716 .
3	Magdalena Molendowska, Rafał Miernik, Bezpieczeństwo w cyberprzestrzeni - wybrane zagrożenia, ISBN: 9788381804158, 2020.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	60
Udział w wykładach:	15
Udział w zajęciach laboratoryjnych:	45
Praca własna studenta, w tym:	40
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	10
Przygotowanie do zajęć laboratoryjnych:	30
Łączny czas pracy studenta	100

Sumaryczna liczba punktów ECTS dla przedmiotu	4
---	---

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W02++ CB1A_W15++	C1 - C3	W1 - W15	1	O1
EK 2	CB1A_W02++	C1 - C3	W5, W7, W10, W12, W13	1	O1
EK 3	CB1A_W21++	C1 - C3	W5 - W14	1	O1
EK 4	CB1A_U06+++	C1 - C3	L1 - L14	2, 3, 4	O2, O3
EK 5	CB1A_U06++	C1 - C3	L1 - L14	2, 3, 4	O2, O3
EK 6	CB1A_U06+++ CB1A_U11++	C1 - C3	L1 - L14	2, 3, 4	O2, O3
EK 7	CB1A_K03++	C1 - C3	W1 - W14 L1 - L14	1 - 4	O1, O2, O3

Autor programu:	dr inż. Sebastian Gnapowski
Adres e-mail:	s.gnapowski@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Stosowanej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	AI w cyberbezpieczeństwie
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C702.2
Rok:	IV
Semestr:	7
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	75
Wykład	30
Ćwiczenia	
Laboratorium	45
Projekt	
Liczba punktów ECTS:	5
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zapoznanie z zaawansowanymi modelami sztucznej inteligencji na potrzeby cyberbezpieczeństwa
C2	Nabycie praktycznej wiedzy z zakresu zaawansowanych metod uczenia maszynowego i sztucznej inteligencji w celu stosowania w cyberbezpieczeństwie
C3	Nabycie umiejętności w zakresie projektowania i implementowania rozwiązań AI zabezpieczających systemy informatyczne

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Znajomość podstawowych modeli uczenia maszynowego
2	Podstawowe umiejętności programowania w wybranym języku programowania wysokiego poziomu
3	Znajomość algebry liniowej, analizy matematycznej oraz statystyki
4	Znajomość sieci komputerowych i systemów operacyjnych

Efekty uczenia się	
	W zakresie wiedzy:
EK 1	rozpoznaje zróżnicowane zagrożenia cybernetyczne w systemach informatycznych
EK 2	identyfikuje metody monitorowania, zapobiegania i reakcji na incydenty bezpieczeństwa z zastosowaniem AI
	W zakresie umiejętności:
EK3	implementuje zaawansowane modele lub systemy AI na potrzeby zabezpieczania systemów informatycznych

EK4	projektuje bezpieczne systemy oparte na AI w kontekście zapewnienia cyberbezpieczeństwa
	W zakresie kompetencji społecznych:
EK5	jest gotów do podejmowania wyzwań związanych z wykorzystaniem nowoczesnych technik AI i krytycznej oceny tych technik

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Wykrywanie zagrożeń w czasie rzeczywistym
W2	Automatyczna klasyfikacja zagrożeń
W3	Analiza behawioralna użytkowników
W4	Sztuczna inteligencja w analizie logów
W5	Predykcja zagrożeń cybernetycznych
W6	Zaawansowane systemy antywirusowe
W7	Uczenie maszynowe w zaporach ogniowych
W8	Rozpoznawanie i ochrona przed atakami
W9	AI w analizie socjotechniki i phishingu
W10	Analiza danych telemetrycznych
W11	Zarządzanie lukami w zabezpieczeniach
W12	Personalizowane systemy ostrzegania
W13	Deepfake i wykrywanie manipulacji treści
Forma zajęć - laboratoria	
	Treści programowe
L1	Wykrywanie anomalii w ruchu sieciowym przy użyciu algorytmów klasteryzacji
L2	Wykrywanie phishingu z użyciem klasyfikatorów AI
L3	Predykcja zagrożeń cybernetycznych
L4	Analiza złośliwego oprogramowania za pomocą AI
L5	Wykrywanie ataków brute force na podstawie analizy logów
L6	Wykrywanie ataków z wykorzystaniem AI
L7	Systemy detekcji luk w zabezpieczeniach
L8	Wykrywanie ataków socjotechnicznych z użyciem AI
L9	Wykrywanie nietypowych zachowań użytkowników
L10	Analiza logów systemowych przy pomocy algorytmów AI
L11	Analiza danych telemetrycznych z wykorzystaniem AI
L12	Rozpoznawanie deepfake i manipulacji obrazami
Metody dydaktyczne	
1	wykład informacyjny
2	ćwiczenia laboratoryjne

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena odpowiedzi ustnej	51%
O3	ocena wykonanych ćwiczeń laboratoryjnych	51%

Literatura podstawowa	
1	Banasiński, Cezary, i in. Cyberbezpieczeństwo. Wolters Kluwer, 2020.
2	Surma, Jerzy, i in. Hakowanie sztucznej inteligencji. Wydanie I., Wyd. Naukowe PWN SA, 2020.
3	Hurbans, Rishal. Algorytmy sztucznej inteligencji: ilustrowany przewodnik. Helion SA, 2021.
4	Kaplan, Jerry. Sztuczna inteligencja: co każdy powinien wiedzieć. Wydanie I., Wyd. Naukowe PWN, 2019.

Literatura uzupełniająca	
1	Żulicki, Remigiusz. Data science: najseksowniejszy zawód XXI wieku w Polsce. Wyd. Uniwersytetu Łódzkiego, 2022. katalog.pollub.pl, https://doi.org/10.18778/8331-110-4 .
2	Parol, Mirosław, i in. Sztuczna inteligencja w praktyce: laboratorium : praca zbiorowa. Oficyna Wydawnicza Politechniki Warszawskiej, 2008.
3	Sztuczna inteligencja w praktyce : laboratorium : praca zbiorowa - Politechnika Lubelska.
4	Ponteves, Hadelin de. Sztuczna inteligencja: błyskawiczne wprowadzenie do uczenia maszynowego, uczenia ze wzmocnieniem i uczenia głębokiego. Helion, 2021.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	75
Udział w wykładach:	30
Udział w zajęciach laboratoryjnych:	45
Praca własna studenta, w tym:	50
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	20
Przygotowanie do zajęć laboratoryjnych:	30
Łączny czas pracy studenta	125
Sumaryczna liczba punktów ECTS dla przedmiotu	5

Macierz efektów uczenia się					
Symbol przedmiotowe	Odniesienie przedmiotowego	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny

go efektu uczenia się	efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania				
EK 1	CB1A_W02++ CB1A_W15++	C1,C3	W1-W13	1	O1, O2
EK 2	CB1A_W15++ CB1A_W19++	C1,C2	W1-W13	1	O1, O2
EK 3	CB1A_U01++ CB1A_U22+++	C1, C2, C3	L1-L12	2	O3
EK 4	CB1A_U01++ CB1A_U22+++	C1, C2, C3	L1-L12	2	O3
EK 5	CB1A_K01+	C2	W1-W13	1	O1, O2

Autor programu:	dr hab. inż. Michał Wydra, profesor uczelni
Adres e-mail:	m.wydra@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Stosowanej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Blockchain i kryptowaluty
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C703.1
Rok:	IV
Semestr:	7
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	45
Wykład	15
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	3
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zapoznanie się z metodami i regułami funkcjonowania kryptowalut
C2	Zapoznanie z podstawowymi zasadami działania technologii blockchain oraz jej zastosowaniami, w szczególności w kryptowalutach
C3	Przedstawienie potencjalnych zagrożeń i wyzwań związanych z bezpieczeństwem systemów opartych na blockchain

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Podstawowa znajomość kryptografii i zasad działania systemów rozproszonych
2	Znajomość zagadnień związanych z cyberbezpieczeństwem i ochroną danych

Efekty uczenia się	
	W zakresie wiedzy:
EK1	definiuje teoretyczne podstawy działania rejestrów rozproszonych i kryptowalut
EK2	definiuje i potrafi wskazać zastosowania technologii rejestrów rozproszonych oraz jej ograniczenia i związane z nią zagrożenia
EK3	rozumie wyzwania związane z bezpieczeństwem systemów opartych na blockchain oraz kryptowalut
	W zakresie umiejętności:
EK4	potrafi efektywnie korzystać z różnych wariantów rejestrów rozproszonych
EK5	potrafi zaprojektować strukturę blockchain oraz wykorzystać ją w konkretnym zastosowaniu
EK6	potrafi posługiwać się dedykowanymi narzędziami do tworzenia aplikacji rozproszonych

	W zakresie kompetencji społecznych:
EK7	docenia znaczenie wiedzy związanej z najnowocześniejszymi osiągnięciami technologicznymi i jest świadomy konieczności jej ciągłego uzupełniania

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Wprowadzenie do technologii blockchain i kryptowalut
W2	Blockchain bezpieczeństwo i ograniczenia
W3	Ekonomiczne aspekty kryptowalut i ich bezpieczeństwo i zabezpieczenia
W4	Wybrane kryptowaluty i mechanizmy ich bezpiecznego funkcjonowania
W5	Platformy wykorzystywane w implementacjach
W6	Tworzenie tokenów, a tworzenie kryptowalut
W7	Hot wallet czy cold wallet - bezpieczeństwo
W8	Proof of Work (PoW), Proof of Stake (PoS), Delegated PoS, Proof of Authority
W9	Mechanizm działania Bitcoina: transakcje, mining, halving
W10	Tokeny NFT, tokeny użytkowe, token bezpieczeństwa
W11	Bezpieczeństwo portfeli i zarządzanie kluczami prywatnymi
W12	Mechanizmy bezpieczeństwa w blockchain
W13	Połączenie blockchain z AI
W14	Wyzwania i przyszłość blockchain
W15	Prawne aspekty rejestrów rozproszonych, kryptowalut i inteligentnych kontraktów
Forma zajęć - laboratoria	
	Treści programowe
L1	Tworzenie tokenów
L2	Tworzenie kryptowalut
L3	Konfiguracja portfeli software'owych
L4	Przechowywanie kluczy prywatnych i tworzenie kopii zapasowych (seed phrase)
L5	Portfele zimne - cold wallet
L6	Wizualizacja przepływu kryptowalut
L7	Analiza ataków, phishingu i exploitów inteligentnych kontraktów
L8	Wykorzystanie narzędzi do audytu inteligentnych kontraktów
L9	Generowanie kluczy publicznych i prywatnych
L10	Analiza bezpieczeństwa transakcji w sieci Bitcoin lub Ethereum
L11	Analiza transakcji za pomocą eksploratora bloków
L12	Wykorzystanie eksploratora bloków w celu analizy transakcji, hashy bloków i adresów
L13	Kopanie kryptowalut i ich bezpieczeństwo
L14	Tworzenie whitepaper do nowego crypto

Metody dydaktyczne

1	wykład informacyjny
2	dyskusja dydaktyczna
3	ćwiczenia laboratoryjne
4	metoda symulacji

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena odpowiedzi ustnej	51%
O2	ocena wykonanych ćwiczeń laboratoryjnych	51%
O3	ocena wykonanych symulacji	51%

Literatura podstawowa	
1	David L. Shrier, Blockchain Basics. Springer 2017.
2	Kądziołka Kinga, Inwestycje w internecie: bitcoin i inne kryptowaluty, Rozpisani.pl, 2016.
3	Song J., Zrozumieć Bitcoin. Programowanie kryptowalut od podstaw, Helion, 2020.

Literatura uzupełniająca	
1	Gilder George, Standard złota w epoce pieniądza cyfrowego: informacyjna teoria pieniądza i kredytu, Fijorr Publishing, 2015.
2	Ward Beullens, Jan-Piete D'Anvers, Andreas HÅNulsing, Tanja Lange, Lorenz Panny, Cyprien de Saint Guilhem, and Nigel P. Smart., Post-quantum cryptography - current state and quantum mitigation, 2022.
3	Dhillon V., Metcalf D., Hooper M., Zastosowania technologii Blockchain, PWN, 2018.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	45
Udział w wykładach:	15
Udział w zajęciach laboratoryjnych:	30
Praca własna studenta, w tym:	30
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	10
Przygotowanie do zajęć laboratoryjnych:	20
Łączny czas pracy studenta	75
Sumaryczna liczba punktów ECTS dla przedmiotu	3

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W06++	C1 - C3	W1 - W15	1, 2	O1
EK 2	CB1A_W15+ CB1A_W06++	C1 - C3	W1 - W15	1, 2	O1
EK 3	CB1A_W02++ CB1A_W15+	C1 - C3	W1 - W15	1, 2	O1
EK 4	CB1A_U19++	C1 - C3	L1 - L14	3, 4	O2, O3
EK 5	CB1A_U16++ CB1A_U19++	C1 - C3	L1 - L14	3, 4	O2, O3
EK 6	CB1A_U16++ CB1A_U19++	C1 - C3	L1 - L14	3, 4	O2, O3
EK 7	CB1A_K02+	C1 - C3	W1 - W15, L1 - L14	1 - 4	O1, O2, O3

Autor programu:	dr inż. Sebastian Gnapowski
Adres e-mail:	s.gnapowski@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Stosowanej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Hurtownie danych i analiza OLAP
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C703.2
Rok:	IV
Semestr:	7
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	45
Wykład	15
Ćwiczenia	
Laboratorium	
Projekt	30
Liczba punktów ECTS:	3
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zdobycie wiedzy na temat hurtowni danych
C2	Opanowanie umiejętności projektowania hurtowni danych
C3	Rozwinięcie praktycznych umiejętności analizy danych z wykorzystaniem OLAP
C4	Przygotowanie do pracy z nowoczesnymi technologiami zarządzania danymi

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Podstawy programowania

Efekty uczenia się	
	W zakresie wiedzy:
EK1	formułuje teoretyczne podstawy hurtowni danych i analizy wielowymiarowej
EK2	charakteryzuje zasady projektowania i implementacji hurtowni danych
EK3	opisuje najnowsze trendy w hurtowniach danych i ich integracji z technologiami Big Data
	W zakresie umiejętności:
EK4	tworzy modele hurtowni danych
EK5	przeprowadza proces ETL
	W zakresie kompetencji społecznych:
EK6	jest gotów do podejmowania wyzwań związanych z wykorzystaniem hurtowni danych i ich krytycznej oceny

Treści programowe przedmiotu	
Forma zajęć - wykłady	

	Treści programowe
W1	Definicja i rola hurtowni danych w organizacjach
W2	Porównanie systemów zarządzania danymi OLTP i OLAP
W3	Architektura hurtowni danych: warstwy i komponenty
W4	Schematy danych: gwiazda, płatek śniegu i konstelacja
W5	Fakty i wymiary: charakterystyka i typy
W6	Proces modelowania wymiarowego
W7	Kluczowe etapy procesu ETL
W8	Podstawy analizy OLAP, wielowymiarowe struktury danych
W9	Operacje OLAP: drill-down, roll-up, slice, dice, pivot
W10	Tworzenie i wykonywanie zapytań wielowymiarowych
W11	Hurtownie danych a Big Data: podobieństwa i różnice
W12	Rola hurtowni danych w eksploracji danych
W13	Predykcja i modele statystyczne oparte na danych hurtowni

Forma zajęć - projekt

	Treści programowe
P1	Analiza wymiarów
P2	Analiza faktów
P3	Budowa modeli hurtowni danych (biznesowy, logiczny, fizyczny)
P4	Proces ETL
P5	ROLAP vs. MOLAP
P6	Prezentacja projektów zaliczeniowych

Metody dydaktyczne

1	wykład informacyjny
2	metoda projektu

Metody i kryteria oceny

Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena przygotowanego projektu	51%

Literatura podstawowa

1	Imasri, Ramez A., Navathe, Shamkant B. Wprowadzenie do systemów baz danych. Wyd. Helion, 2019.
2	Chodkowska-Gyurics, A., Hurtownie danych: teoria i praktyka, Wyd. Naukowe PWN, 2014.

Literatura uzupełniająca

1	Surma, J., Business Intelligence: systemy wspomaganie decyzji biznesowych, Wyd. Naukowe PWN, 2009.
---	--

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	45
Udział w wykładach:	15
Udział w zajęciach projektowych:	30
Praca własna studenta, w tym:	30
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	10
Przygotowanie projektu:	20
Łączny czas pracy studenta	75
Sumaryczna liczba punktów ECTS dla przedmiotu	3

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W06++	C1, C4	W1-W13	1	O1
EK 2	CB1A_W06++	C1, C4	W1-W13	1	O1
EK 3	CB1A_W06++ CB1A_W02++	C1, C4	W1-W13	1	O1
EK 4	CB1A_U19++ CB1A_U17+++	C2, C3, C4	P1-P6	2	O2
EK 5	CB1A_U12++ CB1A_U19++ CB1A_U17+++	C2, C3, C4	P1-P6	2	O2
EK 6	CB1A_K01+	C4	W1-W13, P1-P6	1,2	O1, O2

Autor programu:	dr Rafał Stęgiński; dr Adam Kiersztyn; dr Konrad Smoliński
Adres e-mail:	r.stegierski@pollub.pl; a.kiersztyn@pollub.pl; k.smolinski@pollub.pl
Jednostka organizacyjna:	Katedra Inteligencji Obliczeniowej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Wybrane zagadnienia z analizy obrazów cyfrowych i biometrii
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C704.1
Rok:	IV
Semestr:	7
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	60
Wykład	30
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	4
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zapoznanie z podstawowymi pojęciami i metodami analizy obrazów cyfrowych oraz ich zastosowaniami w biometrii, umożliwiające zrozumienie procesów przetwarzania i interpretacji obrazów
C2	Nabycie umiejętności projektowania, implementacji i trenowania modeli uczenia maszynowego i sztucznej inteligencji do zadań przetwarzania obrazu
C3	Rozwinięcie zdolności krytycznej analizy i oceny algorytmów oraz technologii stosowanych w przetwarzaniu obrazów i biometrii, z uwzględnieniem aktualnych trendów i osiągnięć w tej dziedzinie

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Znajomość algorytmów i struktur danych
2	Podstawy uczenia maszynowego i statystyki
3	Znajomość programowania

Efekty uczenia się	
	W zakresie wiedzy:
EK 1	rozpoznaje podstawowe pojęcia i metody analizy obrazów cyfrowych oraz biometrii
EK 2	rozdziela modele uczenia maszynowego wykorzystywane w analizie obrazów oraz do przetwarzania danych biometrycznych
	W zakresie umiejętności:
EK3	opracowuje różne algorytmy przetwarzania i analizy obrazów cyfrowych oraz danych biometrycznych

EK4	dobiera modele uczenia maszynowego do rozważanego problemu
	W zakresie kompetencji społecznych:
EK5	jest gotów do uznawania znaczenia wiedzy z zakresu analizy obrazu i biometrii jako elementu w rozwiązywaniu problemów w obszarze cyberbezpieczeństwa, wykazując otwartość na jej ciągle poszerzanie oraz stosowanie w praktycznych rozwiązaniach

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Wprowadzenie do analizy obrazu cyfrowego
W2	Transformacje i przetwarzanie obrazów
W3	Podstawy uczenia maszynowego i głębokiego
W4	Zaawansowane metody głębokiego uczenia w przetwarzaniu obrazów, wybrane architektury sieci neuronowych, techniki optymalizacji modeli
W5	Techniki klasyfikacji obrazów
W6	Metody segmentacji obrazów. Techniki podziału obrazu na regiony o podobnych cechach
W7	Algorytmy wykrywania i śledzenia obiektów
W8	Wprowadzenie do biometrii. Przegląd cech biometrycznych wykorzystywanych w identyfikacji osób
W9	Zastosowania biometrii w systemach bezpieczeństwa. Wyzwania i aspekty bezpieczeństwa w biometrii
W10	Techniki ekstrakcji cech z obrazów biometrycznych
W11	Klasyfikacja w biometrii. Metody rozpoznawania i weryfikacji tożsamości na podstawie danych biometrycznych
Forma zajęć - laboratoria	
	Treści programowe
L1	Wprowadzenie do analizy obrazów. Podstawowe operacje na obrazach
L2	Transformacje cyfrowe obrazów
L3	Zastosowanie modeli uczenia maszynowego na zbiorach danych zawierających obrazy
L4	Sieci konwolucyjne w klasyfikacji obrazów
L5	Odszumianie obrazów
L6	Segmentacja obrazów
L7	Wykrywanie obiektów na obrazie
L8	Analiza danych biometrycznych. Ekstrakcja cech biometrycznych
L9	Klasyfikacja w biometrii

Metody dydaktyczne	
1	wykład informacyjny
2	metoda programowania z użyciem komputera

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena wykonanych programów komputerowych	51%

Literatura podstawowa	
1	Aurélien Géron, Uczenie maszynowe z użyciem Scikit-Learn, Keras i TensorFlow.
2	K. Ślot, Wybrane zagadnienia biometrii, WKŁ, 2008.
3	Francois Chollet, J. J. Allaire, Deep Learning. Praca z językiem R i biblioteką Keras.

Literatura uzupełniająca	
1	Szeliski, Richard. Computer Vision: Algorithms and Applications. 1st ed. London: Springer Nature, 2010. Web.
2	Wilhelm Burger, Mark J. Burge, Digital Image Processing: An Algorithmic Introduction Using Java. Springer, 2016.
3	David Zhang, Guangming Lu, Lei Zhang, Advanced Biometrics. Springer, 2018.
4	Cichosz, Paweł, Systemy uczące się. Wyd. 2. Warszawa: Wydawnictwa Naukowo-Techniczne, 2007. Print.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	60
Udział w wykładach:	30
Udział w zajęciach laboratoryjnych:	30
Praca własna studenta, w tym:	40
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	20
Przygotowanie do zajęć laboratoryjnych:	20
Łączny czas pracy studenta	100
Sumaryczna liczba punktów ECTS dla przedmiotu	4

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny

EK 1	CB1A_W11+++	C1	W1 - W11	1	O1
EK 2	CB1A_W11+++	C1	W1 - W11	1	O1
EK 3	CB1A_U12++ CB1A_U14++	C2	L1 - L9	2	O1, O2
EK 4	CB1A_U12++ CB1A_U14++	C2	L1 - L9	2	O1, O2
EK 5	CB1A_K02+	C3	L1 - L9, W1 - W11	1, 2	O1, O2

Autor programu:	dr hab. Paweł Karczmarek, profesor uczelni; dr Rafał Stęgiński; mgr inż. Albert Rachwał; mgr Alicja Żmudzińska; dr inż. Łukasz Gałka
Adres e-mail:	p.karczmarek@pollub.pl; r.stegierski@pollub.pl; a.rachwal@pollub.pl; a.zmudzinska@pollub.pl; l.galka@pollub.pl
Jednostka organizacyjna:	Katedra Inteligencji Obliczeniowej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Automatyzacja i orkiestracja bezpieczeństwa systemów komputerowych
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C704.2
Rok:	IV
Semestr:	7
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	60
Wykład	30
Ćwiczenia	
Laboratorium	30
Projekt	
Liczba punktów ECTS:	4
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Rozwinięcie umiejętności projektowania i wdrażania procesów automatyzacji w celu poprawy efektywności i skuteczności działań związanych z bezpieczeństwem systemów komputerowych
C2	Wykształcenie zdolności analizy i oceny ryzyka związanego z zagrożeniami w cyberprzestrzeni, ze szczególnym uwzględnieniem technik monitorowania, wykrywania i reagowania na incydenty bezpieczeństwa
C3	Przygotowanie do samodzielnego wykorzystania zaawansowanych narzędzi i technologii, w tym sztucznej inteligencji, w celu zapewnienia ciągłości działania systemów komputerowych i ochrony przed zagrożeniami

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Podstawowa znajomość podstawowych pojęć i zagadnień związanych z bezpieczeństwem systemów komputerowych, w tym podstawowych metod ochrony danych oraz analizy ryzyka
2	Znajomość zasad działania sieci komputerowych
3	Umiejętność programowania na poziomie podstawowym
4	Znajomość podstawowych metod uczenia maszynowego i ich potencjalnego zastosowania w analizie i wykrywaniu cyberzagrożeń

Efekty uczenia się	
	W zakresie wiedzy:
EK 1	definiuje podstawowe pojęcia związane z automatyzacją i orkiestracją w cyberbezpieczeństwie oraz rozpoznaje główne rodzaje cyberzagrożeń

EK 2	zna zaawansowane technologie, w tym wykorzystanie sztucznej inteligencji w identyfikacji i zapobieganiu zagrożeniom bezpieczeństwa systemów komputerowych
	W zakresie umiejętności:
EK3	stosuje narzędzia automatyzacji do monitorowania sieci, analizy logów oraz reagowania na incydenty bezpieczeństwa
EK4	projektuje i wdraża polityki bezpieczeństwa oraz modele automatyzacji procesów w celu ochrony systemów komputerowych
	W zakresie kompetencji społecznych:
EK5	jest gotów do krytycznej oceny posiadanej wiedzy oraz podejmowania decyzji w złożonych sytuacjach technicznych

Treści programowe przedmiotu	
Forma zajęć - wykłady	
	Treści programowe
W1	Wprowadzenie do automatyzacji i orkiestracji w cyberbezpieczeństwie
W2	Architektura systemów do automatyzacji bezpieczeństwa. Monitorowanie i analiza zagrożeń
W3	Reagowanie na incydenty bezpieczeństwa. Reagowanie na incydenty bezpieczeństwa. Automatyzacja w wykrywaniu zagrożeń
W4	Tworzenie polityk bezpieczeństwa. Analiza przypadków: Incydenty bezpieczeństwa i ich automatyzacja
W5	Automatyzacja zarządzania podatnościami. Automatyzacja ochrony danych i zgodności z regulacjami
W6	Zabezpieczanie środowisk chmurowych
W7	Audyt i raportowanie w automatyzacji bezpieczeństwa
W8	Wyzwania w automatyzacji bezpieczeństwa. Przyszłość automatyzacji i orkiestracji w cyberbezpieczeństwie
Forma zajęć - laboratoria	
	Treści programowe
L1	Wprowadzenie do narzędzi automatyzacji. Tworzenie reguł automatyzacji
L2	Monitorowanie aktywności w sieci. Analiza logów i zdarzeń
L3	Automatyzacja reakcji na incydenty. Wykorzystanie sztucznej inteligencji w wykrywaniu zagrożeń. Orkiestracja procesów między narzędziami
L4	Zarządzanie podatnościami. Automatyzacja ochrony danych
L5	Zabezpieczenie środowisk chmurowych. Analiza przypadków incydentów bezpieczeństwa. Automatyzacja raportowania
L6	Testowanie i optymalizacja polityk bezpieczeństwa. Rozwiązywanie problemów implementacyjnych
L7	Podsumowanie i prezentacja projektów końcowych

Metody dydaktyczne	
1	wykład problemowy
2	analiza przypadków

3	ćwiczenia laboratoryjne
4	metoda projektu

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena pracy pisemnej	51%
O2	ocena wykonanych ćwiczeń laboratoryjnych	51%
O3	ocena przygotowanego projektu	51%

Literatura podstawowa	
1	Agarwal, Gaurav, Modern Devops Practices : Implement and Secure devOps in the Public Cloud with Cutting-Edge Tools, Tips, Tricks, and Techniques. Packt, 2021.
2	Beyer, Betsy i in. Site reliability engineering : jak Google zarządza systemami produkcyjnymi. Wyd. Helion, 2018.

Literatura uzupełniająca	
1	Collin, Michael, Network Security Through Data Analysis, O'Reilly Media, 2017.
2	Troncone, Paul, i in., Cyberbezpieczeństwo w bashu : jak za pomocą wiersza poleceń prowadzić działania zaczepne i obronne. Wyd. Helion , 2022.
3	Sanders, Chris, i in., Applied Network Security Monitoring : Collection, Detection, and Analysis. Waltham, MA: Syngress, 2014.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	60
Udział w wykładach:	30
Udział w zajęciach laboratoryjnych:	30
Praca własna studenta, w tym:	40
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	20
Przygotowanie do zajęć laboratoryjnych:	20
Łączny czas pracy studenta	100
Sumaryczna liczba punktów ECTS dla przedmiotu	4

Macierz efektów uczenia się					
Symbol przedmiotowe go efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny

	zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania				
EK 1	CB1A_W04++ CB1A_W15++	C1	W1 - W8	1	O1
EK 2	CB1A_W19++	C2	W3, W4	1, 2	O1
EK 3	CB1A_U12++	C3	L1 - L7	3	O2
EK 4	CB1A_U22++	C2	L1 - L7	2, 3, 4	O3
EK 5	CB1A_K01+	C1, C3	W1 - W8, L1 - L7	1 - 4	O1, O2, O3

Autor programu:	mgr inż. Dariusz Głuchowski; dr hab. inż. Dariusz Czerwiński, profesor uczelni
Adres e-mail:	d.głuchowski@pollub.pl; d.czerwinski@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Stosowanej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Seminarium dyplomowe
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C705
Rok:	IV
Semestr:	7
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	30
Wykład	
Ćwiczenia	30
Laboratorium	
Projekt	
Liczba punktów ECTS:	2
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Zapoznanie ze sposobami formułowania tematu, określaniem celów, dobieraniem odpowiednich metod analizy uzyskanych wyników
C2	Kształtowanie zdolności do samodzielnego prowadzenia badań, analizy literatury oraz krytycznego myślenia
C3	Zapoznanie z metodami prezentacji wyników badań oraz obrony pracy dyplomowej

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Podstawowa umiejętności z zakresu edycji dokumentów
2	Podstawowe umiejętności z zakresu tworzenia prezentacji

Efekty uczenia się	
	W zakresie umiejętności:
EK1	wyszukuje dostępne informacje z wybranego obszaru tematycznego dotyczącego cyberbezpieczeństwa
EK2	analizuje dostępną wiedzę z wybranego obszaru tematycznego z zakresu cyberbezpieczeństwa
EK3	potrafi opracować dokumentację oraz przedstawić prezentację wyników badań lub projektu inżynierskiego na wybrany temat z zakresu cyberbezpieczeństwa
EK4	potrafi uczestniczyć w dyskusjach oraz prowadzić merytoryczne konsultacje z profesjonalistami w celu opracowywania skutecznych rozwiązań problemów związanych z bezpieczeństwem w cyberprzestrzeni
	W zakresie kompetencji społecznych:

EK5	jest gotów do krytycznej oceny posiadanej wiedzy oraz podnoszenia swoich kompetencji i konsultacji z ekspertami
------------	---

Treści programowe przedmiotu	
Forma zajęć - ćwiczenia	
	Treści programowe
ĆW1	Omówienie zasad realizacji pracy dyplomowej. Wymogi formalne i strukturalne pracy inżynierskiej
ĆW2	Zaawansowana edycja dokumentów i zarządzanie wersjami
ĆW3	Metody opracowywania bibliografii i wykorzystywania referencji
ĆW4	Przygotowanie do realizacji pracy dyplomowej: formułowanie problemu badawczego, wyznaczanie celów i zakresu pracy oraz określenie metodyki badań
ĆW5	Analiza literatury oraz przegląd istniejących rozwiązań i technologii
ĆW6	Tworzenie i wdrażanie nowych pomysłów w wybranym obszarze
ĆW7	Opracowywanie części praktycznej pracy. Realizacja projektu inżynierskiego lub badań w obszarze cyberbezpieczeństw
ĆW8	Prezentacja wyników - metody wizualizacji danych
ĆW9	Wyciąganie wniosków oraz krytyczna analiza uzyskanych wyników

Metody dydaktyczne	
1	wykład informacyjny
2	przygotowanie prezentacji
3	dyskusja dydaktyczna

Metody i kryteria oceny		
Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	ocena przygotowanej prezentacji	51%
O2	ocena aktywności w trakcie zajęć	51%

Literatura podstawowa	
1	Banasiński, Cezary, i in. Cyberbezpieczeństwo. Wolters Kluwer, 2020.
2	Żulicki, Remigiusz. Data science: najseksowniejszy zawód XXI wieku w Polsce. Wyd. Uniwersytetu Łódzkiego, 2022. katalog.pollub.pl, https://doi.org/10.18778/8331-110-4 .
3	Bravo, Cesar. Cyberbezpieczeństwo dla zaawansowanych: skuteczne zabezpieczenia systemu Windows, Linux, IoT i infrastruktury w chmurze. Helion, 2023.

Literatura uzupełniająca	
1	Surma, Jerzy, i in. Hakowanie sztucznej inteligencji. Wydanie I., Wyd. Naukowe PWN SA, 2020.
2	Hurbans, Rishal. Algorytmy sztucznej inteligencji: ilustrowany przewodnik. Helion SA, 2021.

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z wykładowcą, w tym:	30
Udział w ćwiczeniach:	30
Praca własna studenta, w tym:	20
Studiowanie tematyki wykładów, przygotowanie do kolokwium:	0
Przygotowanie do ćwiczeń:	20
Łączny czas pracy studenta	50
Sumaryczna liczba punktów ECTS dla przedmiotu	2

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_U01+++	C1, C2	ĆW1 - ĆW9	1,2	1
EK 2	CB1A_U01+++ CB1A_U04+++	C1, C3	ĆW1 - ĆW9	1,2, 3	1, 2
EK 3	CB1A_U04+++	C2, C3	ĆW3 - ĆW9	1,2	1
EK 4	CB1A_U07+++	C1, C2, C3	ĆW1 - ĆW9	3	2
EK 5	CB1A_K01++ CB1A_K02++	C1, C2, C3	ĆW9	2	1

Autor programu:	dr hab. inż. Michał Wydra, profesor uczelni
Adres e-mail:	m.wydra@pollub.pl
Jednostka organizacyjna:	Katedra Informatyki Stosowanej

Karta (sylabus) modułu (przedmiotu)
Kierunek studiów: Cyberbezpieczeństwo
Studia pierwszego stopnia

Przedmiot:	Praca dyplomowa
Rodzaj przedmiotu:	obieralny
Kod przedmiotu:	CB-1-S-C706
Rok:	IV
Semestr:	7
Forma studiów:	studia stacjonarne
Rodzaj zajęć i liczba godzin w semestrze:	0
Wykład	
Ćwiczenia	
Laboratorium	
Projekt	
Liczba punktów ECTS:	15
Sposób zaliczenia:	zaliczenie
Język wykładowy:	język polski

Cele przedmiotu	
C1	Nabycie umiejętności wykorzystania nabytej w toku studiów wiedzy w rozwiązaniu problemu/ zagadnienia z wybranego zakresu z obszaru cyberbezpieczeństwa
C2	Rozwinięcie umiejętności prowadzenia samodzielnych badań, analizy i interpretacji wyników oraz prezentacji osiągnięć w formie zwięzłego opracowania
C3	Doskonalenie zdolności prezentacji oraz obrony własnych koncepcji w obszarze cyberbezpieczeństwa

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Wiedza i umiejętności ze wszystkich przedmiotów przewidzianych programem kształcenia na poziomie studiów inżynierskich dla kierunku cyberbezpieczeństwo
2	Umiejętność analizy literatury specjalistycznej oraz interpretacji danych
3	Wiedza z zakresu przedmiotów kierunkowych, szczególnie dotyczących zagadnień związanych z cyberbezpieczeństwem

Efekty uczenia się	
	W zakresie wiedzy:
EK 1	ma wiedzę w wybranych dziedzinach z zakresu kierunku studiów związanych z tematyką pracy dyplomowej
	W zakresie umiejętności:
EK2	korzysta z literatury naukowej, norm, standardów i innych źródeł, ocenia wiarygodność i przydatność tych źródeł, oraz wybiera najważniejsze dla rozwiązania problematyki zawartej w pracy dyplomowej

EK3	wykorzystuje wiedzę z toku studiów do rozwiązania problemu projektowego lub badawczego postawionego w pracy dyplomowej oraz potrafi zastosować odpowiednie techniki i narzędzia do jej realizacji
EK4	potrafi efektywnie planować i organizować zadania w trakcie przygotowania pracy dyplomowej, w tym komunikować się i współdziałać z uczestnikami procesu badawczego lub projektowego, wyjaśniając w sposób zrozumiały swoje poglądy i przyjmując argumenty
EK5	potrafi samodzielnie identyfikować własne potrzeby rozwojowe, planować i realizować działania prowadzące do pogłębiania wiedzy oraz doskonalenia umiejętności w obszarze cyberbezpieczeństwa
	W zakresie kompetencji społecznych:
EK6	jest gotów do inicjowania działań związanych z formułowaniem i przekazywaniem informacji oraz współdziałaniem w społeczeństwie w obszarze objętym tokiem studiów, a także ma świadomość potrzeby zachowywania się w sposób profesjonalny oraz przestrzegania zasad etyki zawodowej

Treści programowe przedmiotu

1	Treść konsultacji związana z tematem pracy inżynierskiej uzależniona od potrzeb studenta
----------	--

Metody dydaktyczne

1	konsultacje z promotorem pracy dyplomowej
----------	---

Metody i kryteria oceny

Symbol metody oceny	Opis metody oceny	Próg zaliczeniowy
O1	przygotowanie pracy dyplomowej	51%

Literatura podstawowa

1	Urban S., Ładoński W.: Jak napisać dobrą pracę magisterską. Wyd. piąte, uzup. Wrocław: Wyd. Akademii Ekonomicznej im. O. Łangego we Wrocławiu, 2003.
2	Taranenko W., Świć A., Zubrzycki J., Opielak M.: Metodyka opracowania prac inżynierskich i magisterskich, Wyd. Politechniki Lubelskiej, Lublin 2007.
3	Wojcik K.: Piszę pracę magisterską – poradnik dla autorów akademickich prac promocyjnych (licencjackich, magisterskich, doktorskich), Warszawa: Oficyna Wyd. SGH, 2002.

Literatura uzupełniająca

P1	Literatura związana z tematem pracy dyplomowej.
-----------	---

Obciążenie pracą studenta

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
------------------	---

Godziny kontaktowe z wykładowcą, w tym:	0
Praca własna studenta, w tym:	375
Łączny czas pracy studenta	375
Sumaryczna liczba punktów ECTS dla przedmiotu	15

Macierz efektów uczenia się					
Symbol przedmiotowego efektu uczenia się	Odniesienie przedmiotowego efektu uczenia się do efektów zdefiniowanych dla kierunku studiów wraz z określeniem stopnia powiązania	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Metody oceny
EK 1	CB1A_W03++ CB1A_W05++ CB1A_W06++ CB1A_W09++ CB1A_W12++ CB1A_W13++ CB1A_W14++ CB1A_W15++ CB1A_W18++ CB1A_W19++	C1	P1	1	O1
EK 2	CB1A_U01+++	C2	P1	1	O1
EK 3	CB1A_U04+++ CB1A_U05+++ CB1A_U06++ CB1A_U11++ CB1A_U12++ CB1A_U13++ CB1A_U14++ CB1A_U16++ CB1A_U17++ CB1A_U18++ CB1A_U19++ CB1A_U21++ CB1A_U22++ CB1A_U23++ CB1A_U24++	C1 - C3	P1	1	O1
EK 4	CB1A_U07+++	C2, C3	P1	1	O1
EK 5	CB1A_U08+++	C2, C3	P1	1	O1
EK 6	CB1A_K03++ CB1A_K05++	C1 - C3	P1	1	O1

Autor programu:	dr hab. Paweł Karczmarek, profesor uczelni
Adres e-mail:	p.karczmarek@pollub.pl
Jednostka organizacyjna:	Katedra Inteligencji Obliczeniowej