Program studiów

I. PODSTAWOWE DANE O STUDIACH

1.	Nazwa wydziału:	Wydział Elektroniki i Technik Informacyjnych
2.	Nazwa kierunku:	Cyberbezpieczeństwo
3.	Poziom studiów:	studia drugiego stopnia
4.	Profil studiów:	ogólnoakademicki
5.	Forma studiów:	studia stacjonarne
6.	Język prowadzenia studiów:	polski
7.	Dyscypliny naukowe, do których przypisany jest kierunek:	Informatyka techniczna i telekomunikacja – 100%
8.	W przypadku zawodu, o którym mowa w art. 68 Ustawy, standardy kształcenia, na podstawie których będą prowadzone studia:	nie dotyczy
9.	Liczba semestrów studiów:	trzy
10.	Tytuł zawodowy uzyskiwany przez absolwenta:	magister inżynier

II. OKREŚLENIE EFEKTÓW UCZENIA SIĘ

1. Tabela odniesień efektów uczenia się dla programu studiów do:

- uniwersalnych charakterystyk pierwszego stopnia PRK, na poziomie 7, określonych w załączniku do ustawy o Zintegrowanym Systemie Kwalifikacji (Dz. U. z 2020 r., poz. 226) – „Odniesienie-symbol”,
- charakterystyk drugiego stopnia PRK na poziomie 7, określonych przez rozporządzenie w sprawie charakterystyk drugiego stopnia dla kwalifikacji na poziomach 6–8 Polskiej Ramy Kwalifikacji (Dz. U. z 2018 r. poz. 2218); z uwzględnieniem charakterystyk drugiego stopnia inżynierskich (dla studiów kończących się nadaniem tytułu zawodowego inżyniera albo magistra inżyniera) – „Odniesienie – symbol I/III”.

Lp.	Symbol efektu uczenia się dla programu studiów	Efekt uczenia się	Odniesienie – symbol I/III	Odniesienie – symbol
1	*2*	*3*	*4*	*5*
Wiedza				
		Absolwent		
1.	W_01	Zna i rozumie główne tendencje rozwojowe informatyki technicznej i telekomunikacji, także w szerszym, społecznym kontekście.	I.P7S_WG.o	P7U_W
2.	W_02	Zna i rozumie podstawowe procesy zachodzące w systemach teleinformatycznych, istotne dla zapewnienia bezpiecznego funkcjonowania takich systemów.	I.P7S_WG.o III.P7S_WG	P7U_W
3.	W_03	Zna metodologiczne podstawy prowadzenia badań naukowych; ma wiedzę dotyczącą metodyki prowadzenia prac o charakterze badawczym w dziedzinie nauk inżynieryjno-technicznych, w szczególności związanych z badaniami z zakresu cyberbezpieczeństwa.	I.P7S_WG.o	P7U_W
4.	W_04	Zna zaawansowane narzędzia informatyczne niezbędne do analizy wyników badań.	I.P7S_WG.o	P7U_W
5.	W_05	Ma zaawansowaną wiedzę z zakresu matematyki, obejmującą m.in.: - metody i algorytmy algebry liniowej, - podstawy logiki temporalnej, - algorytmy kodowania i dekodowania dla liniowych kodów korekcyjnych, - podstawy teorii krat, - podstawy teoretyczne rozpoznawania wzorców, tworzącą podstawy do identyfikowania problemów i formułowania specyfikacji złożonych i nietypowych zadań inżynierskich oraz problemów badawczych, związanych z zapewnieniem cyberbezpieczeństwa oraz ich innowacyjnego rozwiązywania, dotyczących w szczególności analizy danych, weryfikacji formalnej i kryptografii postkwantowej.	I.P7S_WG.o	P7U_W
6.	W_06	W pogłębionym stopniu zna i rozumie wybrane fakty, teorie i metody, stanowiące zaawansowaną wiedzę z zakresu analizy danych w kontekście jej zastosowań w rozwiązywaniu problemów dotyczących cyberbezpieczeństwa.	I.P7S_WG.o	P7U_W

Lp.	Symbol efektu uczenia się dla programu studiów	Efekt uczenia się	Odniesienie – symbol I/III	Odniesienie – symbol
1	*2*	*3*	*4*	*5*
7.	W_07	W pogłębionym stopniu zna i rozumie wybrane fakty, teorie i metody, stanowiące zaawansowaną wiedzę z zakresu zapewniania bezpieczeństwa systemów Internetu Rzeczy.	I.P7S_WG.o	P7U_W
8.	W_08	W pogłębionym stopniu zna i rozumie wybrane fakty, teorie i metody, stanowiące zaawansowaną wiedzę z zakresu wybranych aspektów cyberbezpieczeństwa, w tym: - bezpieczeństwa rozwiązań sprzętowych, - bezpieczeństwa komunikacji opartej na najnowszych standardach sieci bezprzewodowych.	I.P7S_WG.o	P7U_W
9.	W_09	Zna i rozumie procesy zachodzące w cyklu życia systemów teleinformatycznych, zwłaszcza związane z zapewnieniem bezpieczeństwa tych systemów.	I.P7S_WG.o	P7U_W
10.	W_10	Rozumie fundamentalne dylematy współczesnej cywilizacji, związane z rozwojem nauk inżynieryjno-technicznych, a zwłaszcza informatyki technicznej i telekomunikacji, oraz wykorzystaniem najnowszych osiągnięć nauki i techniki i wynikającymi z tego zagrożeniami, w szczególności osobiste i społeczne dylematy będące następstwem działań zagrażających bezpieczeństwu systemów teleinformatycznych.	I.P7S_WK	P7U_W
11.	W_11	ma podstawową wiedzę niezbędną do rozumienia pozatechnicznych (prawnych, ekonomicznych, etycznych i innych) uwarunkowań działalności zawodowej w zakresie bezpośrednio lub pośrednio związanym z cyberbezpieczeństwem.	I.P7S_WK	P7U_W
12.	W_12	ma podstawową wiedzę w zakresie ochrony własności intelektualnej, w tym ochrony własności przemysłowej i prawa autorskiego, zwłaszcza w zakresie bezpośrednio lub pośrednio związanym z cyberbezpieczeństwem.	I.P7S_WK	P7U_W
13.	W_13	zna i rozumie podstawowe zasady tworzenia i rozwoju różnych form indywidualnej przedsiębiorczości, w tym związane przedsiębiorczością startupową.	I.P7S_WK III.P7S_WK	P7U_W
Umiejętności				
		Absolwent		
14.	U_01	Potrafi pozyskiwać informacje z właściwie dobranych źródeł, dokonywać ich krytycznej oceny, analizy, syntezy i twórczej interpretacji, wyciągać wnioski i wyczerpująco je uzasadniać.	I.P7S_UW.o	P7U_U
15.	U_02	Potrafi przeprowadzić krytyczną analizę sposobu funkcjonowania istniejących rozwiązań technicznych z zakresu bezpieczeństwa systemów teleinformatycznych i oceniać te rozwiązania.	I.P7S_UW.o III.P7S_UW.o	P7U_U
16.	U_03	Potrafi planować i przeprowadzać eksperymenty / badania, w tym symulacje komputerowe dotyczące bezpieczeństwa systemów teleinformatycznych, oraz interpretować uzyskane wyniki.	I.P7S_UW.o III.P7S_UW.o	P7U_U

Lp.	Symbol efektu uczenia się dla programu studiów	Efekt uczenia się	Odniesienie – symbol I/III	Odniesienie – symbol
1	*2*	*3*	*4*	*5*
17.	U_04	Potrafi wykorzystać zaawansowane narzędzia informatyczne niezbędne do przeprowadzenia eksperymentów/badań związanych z zagadnieniami cyberbezpieczeństwa i analizy ich wyników.	I.P7S_UW.o	P7U_U
18.	U_05	Potrafi formułować i testować hipotezy związane z prostymi problemami badawczymi dotyczącymi m.in. zapewnienia bezpieczeństwa systemów teleinformatycznych.	I.P7S_UW.o	P7U_U
19.	U_06	Potrafi dokonać identyfikacji i sformułować specyfikację złożonych zadań dotyczących cyberbezpieczeństwa, a w szczególności: - analizy danych w kontekście jej zastosowań w rozwiązywaniu problemów związanych z zapewnieniem bezpieczeństwa systemów teleinformatycznych, - zapewniania bezpieczeństwa sieci bezprzewodowych najnowszych generacji i systemów Internetu Rzeczy.	I.P7S_UW.o	P7U_U
20.	U_07	Potrafi zaprojektować – zgodnie z zadaną specyfikacją, używając właściwie dobranych metod i narzędzi – rozwiązanie zawierające elementy innowacyjności, związane z zapewnieniem bezpieczeństwa systemów teleinformatycznych, a także zweryfikować jego poprawność.	I.P7S_UW.o III.P7S_UW.o	P7U_U
21.	U_08	Potrafi przy identyfikacji i formułowaniu specyfikacji złożonych zadań dotyczących bezpieczeństwa systemów teleinformatycznych oraz ich rozwiązywaniu: - dostrzegać ich aspekty systemowe i pozatechniczne, w tym aspekty etyczne, - oceniać aspekty ekonomiczne proponowanych rozwiązań i podejmowanych działań; Potrafi wnieść wkład w opracowanie strategii zarządzania bezpieczeństwem na poziomie instytucjonalnym.	I.P7S_UW.o III.P7S_UW.o	P7U_U
22.	U_09	Potrafi – w pracach badawczych oraz przy rozwiązywaniu zadań dotyczących zapewnienia bezpieczeństwa systemów teleinformatycznych: - wykorzystywać metody analityczne, symulacyjne i eksperymentalne, - dokonać wyboru oraz zastosować właściwe metody, techniki i narzędzia, w tym zaawansowane techniki informacyjno-komunikacyjne, - przystosować istniejące lub opracować nowe metody i narzędzia.	I.P7S_UW.o III.P7S_UW.o	P7U_U
23.	U_10	Potrafi przygotować opracowanie i przedstawić prezentację ustną, dotyczącą w szczególności zagadnień z zakresu cyberbezpieczeństwa, potrafi przygotować krótkie doniesienie naukowe.	I.P7S_UK	P7U_U
24.	U_11	Potrafi komunikować się przy użyciu różnych technik w środowisku zawodowym oraz w innych środowiskach; potrafi prowadzić debatę.	I.P7S_UK	P7U_U

Lp.	Symbol efektu uczenia się dla programu studiów	Efekt uczenia się	Odniesienie – symbol I/III	Odniesienie – symbol
1	*2*	*3*	*4*	*5*
25.	U_12	Potrafi posługiwać się językiem angielskim na poziomie B2+ Europejskiego Systemu Opisu Kształcenia Językowego.	I.P7S_UK	P7U_U
26.	U_13	Potrafi pracować indywidualnie oraz współdziałać z innymi osobami w ramach prac zespołowych; potrafi kierować pracą zespołu.	I.P7S_UO	P7U_U
27.	U_14	Potrafi określić kierunki dalszego uczenia się, zaplanować i zrealizować proces samokształcenia, a także ukierunkowywać innych w tym zakresie.	I.P7S_UU	P7U_U
Kompetencje społeczne				
		Absolwent		
28.	K_01	Jest gotów do krytycznej oceny posiadanej wiedzy i odbieranych treści oraz do uznawania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu; jest gotów do stałego aktualizowania i wzbogacania posiadanej wiedzy.	I.P7S_KK	P7U_K
29.	K_02	Jest gotów do wypełniania zobowiązań społecznych, inspirowania i organizowania działalności na rzecz środowiska społecznego oraz interesu publicznego, a zwłaszcza formułowania i przekazywania społeczeństwu – m.in. poprzez środki masowego przekazu – informacji i opinii dotyczących zagrożeń związanych z cyberbezpieczeństwem i sposobów przeciwdziałania tym zagrożeniom; podejmuje starania, aby przekazać takie informacje i opinie w sposób powszechnie zrozumiały.	I.P7S_KO	P7U_K
30.	K_03	Jest gotów do myślenia i działania w sposób przedsiębiorczy, przewodzenia grupie i ponoszenia odpowiedzialności za nią.	I.P7S_KO	P7U_K
31.	K_04	Jest gotów do odpowiedzialnego pełnienia ról zawodowych, z uwzględnieniem zmieniających się potrzeb społecznych, w tym: - rozwijania dorobku zawodu, - podtrzymywanie etosu zawodu, - przestrzegania etyki zawodowej oraz działania na rzecz przestrzegania tych zasad.	I.P7S_KR	P7U_K

Kod składnika charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji, określony w uchwale Senatu PW w sprawie przyjęcia przez Politechnikę Warszawską kodu składnika charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji dla kwalifikacji uzyskiwanych w ramach szkolnictwa wyższego.

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

W zestawie przedmiotów/modułów zajęć tworzących program studiów wykorzystane są m.in. następujące formy prowadzenia zajęć:

- wykłady,
- ćwiczenia,
- projekty i zajęcia laboratoryjne, realizowane indywidualnie i w zespołach,
- moduły zajęć typu PBL (project-based learning), prowadzone zgodnie z koncepcją „design thinking", wymagające formułowania i rozwiązywania problemów „otwartych",
- samodzielne uczenie się studentów i prezentacja wyników tego samokształcenia na zajęciach grupowych.

Zróżnicowanym formom prowadzenia zajęć odpowiadają zróżnicowane formy weryfikacji i oceny efektów uczenia się. Stosowane są niemal wszystkie wymienione w aktach prawa wewnętrznego PW formy sprawdzania efektów uczenia się, tj. egzamin pisemny, egzamin ustny, kolokwium, laboratorium + sprawozdanie pisemne z realizacji zajęć, projekt + sprawozdanie pisemne z realizacji zadania, prezentacja indywidualna/zespołowa, praca domowa, ocena aktywności podczas zajęć.

Weryfikacja i oceny efektów uczenia się osiągniętych przez studenta w trakcie całego cyklu uczenia się (całego programu studiów) odbywa się przede wszystkim na poziomie poszczególnych przedmiotów (w sposób uwidoczniony w sylabusach). Pełne pokrycie efektów uczenia się zdefiniowanych dla programu studiów przez efekty uczenia się zdefiniowane (i weryfikowane) dla przedmiotów tworzących ten program zapewnia weryfikację efektów kierunkowych (efektów uczenia się osiągniętych przez studenta w trakcie całego cyklu uczenia się).

III. REALIZACJA PROGRAMU STUDIÓW

Łączna liczba godzin zajęć:	900 godz
Liczba punktów ECTS konieczna do ukończenia studiów:	90 ECTS
Procentowy udział liczby punktów ECTS w liczbie punktów ECTS koniecznej do ukończenia studiów ze wskazaniem **dyscypliny wiodącej:** Informatyka techniczna i telekomunikacja	78.9%
Liczba punktów ECTS, którą student musi uzyskać na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich lub innych osób prowadzących zajęcia	46 ECTS tj. 51.1%
Liczba punktów ECTS jaką student musi uzyskać w ramach zajęć z dziedziny nauk humanistycznych lub nauk społecznych, w przypadku kierunków studiów przyporządkowanych do dyscyplin w ramach dziedzin innych niż dziedziny nauk humanistycznych lub nauk społecznych:	5 ECTS
Liczba godzin zajęć z wychowania fizycznego na studiach prowadzonych w formie stacjonarnej:	nie dotyczy
Łączna liczba punktów ECTS, którą student musi uzyskać w ramach zajęć podlegających wyborowi przez studenta *(w wymiarze nie mniejszym niż 30% liczby punktów ECTS koniecznych do ukończenia studiów na danym poziomie)*:	40 ECTS tj. 44.4%
Dla studiów o profilu praktycznym: Łączna liczba punktów ECTS, którą student musi uzyskać w ramach przedmiotów/zajęć kształtujących umiejętności praktyczne (*w wymiarze większym niż 50% liczby punktów ECTS koniecznych do ukończenia studiów na danym poziomie)*:	nie dotyczy
Dla studiów o profilu ogólnoakademickim: Łączna liczba punktów ECTS, którą student musi uzyskać w ramach zajęć związanych z prowadzoną w Uczelni działalnością naukową w dyscyplinie lub dyscyplinach, do których przyporządkowany jest kierunek studiów *(w wymiarze większym niż 50% liczby punktów ECTS wymaganej do ukończenia studiów na danym poziomie)*, z uwzględnieniem udziału studentów w zajęciach przygotowujących do prowadzenia działalności naukowej lub udziału w tej działalności:	71 ECTS tj. 78.9%
Liczba punktów ECTS, jaka może być uzyskana w ramach kształcenia z wykorzystaniem metod i technik kształcenia na odległość: *(liczba punktów ECTS nie może być większa niż 50% liczby punktów ECTS koniecznej do ukończenia studiów – w przypadku studiów o profilu praktycznym albo 75% liczby punktów ECTS koniecznej do ukończenia studiów – w przypadku studiów o profilu ogólnoakademickim).*	0 ECTS[1] tj. 0%

[1] Zakłada się, że w warunkach „normalnych" wszystkie zajęcia objęte programem studiów są realizowane na Uczelni. Organizacja zajęć umożliwia – w razie potrzeby – ich realizację z wykorzystaniem metod i technik kształcenia na odległość.

Łączna liczba godzin oraz punktów ECTS z matematyki	60 godz. 4 ECTS Zgodnie z uchwałą Senatu PW nr 58/L/2020 z dnia 25 listopada 2020 r. *w sprawie ustalania programów studiów w Politechnice Warszawskiej* wymagane godziny i punkty ECTS zrealizowano na studiach pierwszego stopnia.
Łączna liczba godzin oraz punktów ECTS z fizyki	Zgodnie z uchwałą Senatu PW nr 58/L/2020 z dnia 25 listopada 2020 r. *w sprawie ustalania programów studiów w Politechnice Warszawskiej* wymagane godziny i punkty ECTS zrealizowano na studiach pierwszego stopnia.
Łączna liczba godzin oraz punktów ECTS języków obcych	120 godz. 8 ECTS Zgodnie z uchwałą Senatu PW nr 58/L/2020 z dnia 25 listopada 2020 r. *w sprawie ustalania programów studiów w Politechnice* Warszawskiej realizacja poprzez prowadzenie przedmiotów w języku angielskim na poziomie B2+.
Liczba punktów ECTS za pracę dyplomową	20 ECTS

IV. WYMIAR, ZASADY, FORMA PRAKTYK ZAWODOWYCH

Program studiów nie obejmuje praktyki zawodowej

V. SYLABUSY

Program studiów obejmuje następujące klasy programowe (grupy przedmiotów):

PRZEDMIOTY HUMANISTYCZNO-SPOŁECZNE (5 ECTS)
- Przedsiębiorczość startupowa,
- Cyberprzestępczość.

PODSTAWY TEORETYCZNE CYBERBEZPIECZEŃSTWA (8 ECTS)
- Metody matematyczne w cyberbezpieczeństwie,
- Rozpoznawanie wzorców **(**Pattern Recognition),
- Techniki i technologie Big Data.

CYBERBEZPIECZEŃSTWO – MODUŁY PBL (20 ECTS)
- PBL1: Analiza danych w cyberbezpieczeństwie,
- PBL2: Bezpieczeństwo Internetu Rzeczy.

CYBERBEZPIECZEŃSTWO (13 ECTS)
- Bezpieczne systemy cyfrowe,
- Bezpieczeństwo sieci 5G i 6G,
- Pozatechniczne aspekty cyberbezpieczeństwa (Non-technical dimensions of cybersecurity).

PRZEDMIOTY OBIERALNE: CYBERBEZPIECZEŃSTWO/TELEINFORMATYKA (min. 8 ECTS)

PRZEDMIOTY OBIERALNE TECHNICZNE (min. 4 ECTS)

PROWADZENIE BADAŃ I DYPLOMOWANIE (32 ECTS)
- Metodologiczne i etyczne problemy badań technonaukowych (Methodological and ethical issues of technoscientific research),
- Pracownia problemowa,
- Pracownia dyplomowa,
- Seminarium dyplomowe,
- Przygotowanie pracy dyplomowej,
- Redakcja i edycja pracy dyplomowej.

Oferta przedmiotów w klasie PRZEDMIOTY OBIERALNE: CYBERBEZPIECZEŃSTWO/ TELEINFORMATYKA obejmuje przedmioty prowadzone obecnie na Wydziale oraz przedmioty opracowane specjalnie na potrzeby nowego programu. Realizując wymagania związane z uzyskaniem odpowiedniej liczby punktów ECTS w tej klasie, student będzie mógł korzystać z przedmiotów z zakresu cyberbezpieczeństwa, a zwłaszcza teleinformatyki o odpowiednim poziomie zaawansowania (studia drugiego stopnia), prowadzonych na Wydziale na potrzeby innych kierunków studiów (informatyka, telekomunikacja, inżynieria internetu rzeczy), oraz – za zgodą Dziekana wydaną na podstawie opinii kierownika kierunku – przedmiotów prowadzonych na innych wydziałach PW i innych uczelniach. Planowane jest ponadto uruchomienie m.in. następujących przedmiotów, opracowanych specjalnie na potrzeby nowego programu:
- Współczesne problemy cyberbezpieczeństwa,
- CyberBioBezpieczeństwo,
- Ukrywanie informacji w sieciach.

Ostateczna postać tej oferty (nowych przedmiotów) przedłożona studentom będzie uwzględniać rozwój tematyki badań związanych z cyberbezpieczeństwem oraz rozwój kadry akademickiej związanej ze studiami w tym obszarze (na Wydziale i poza Wydziałem). Student w tej klasie przedmiotów obieralnych musi uzyskać co najmniej 8 ECTS.

W klasie przedmiotów OBIERALNYCH TECHNICZNYCH student będzie mógł korzystać z oferty przedmiotów o odpowiednim poziomie zaawansowania (studia drugiego stopnia), prowadzonych na Wydziale oraz – za zgodą Dziekana wydaną na podstawie opinii kierownika kierunku – przedmiotów prowadzonych na innych wydziałach PW i innych uczelniach. Student w tej klasie przedmiotów obieralnych musi uzyskać co najmniej 4 ECTS.

W dalszej części tego punktu przedstawiono opis przedmiotów tworzących „trzon" studiów drugiego stopnia, tzn. przedmiotów obejmujących zajęcia grupowe w klasach programowych:

PRZEDMIOTY HUMANISTYCZNO-SPOŁECZNE

PODSTAWY TEORETYCZNE CYBERBEZPIECZEŃSTWA

CYBERBEZPIECZEŃSTWO – MODUŁY PBL
CYBERBEZPIECZEŃSTWO
PROWADZENE BADAŃ I DYPLOMOWANIE

PRZEDSIĘBIORCZOŚĆ STARTUPOWA

rodzaj zajęć/liczba godzin	wykład	10
	ćwiczenia	0
	laboratorium	0
	projekt	20
	zajęcia zintegrowane (warsztaty)	0
liczba punktów ECTS	3	
status przedmiotu	obowiązkowy	

Treści kształcenia

WYKŁAD

Zdobycie wiedzy na temat specyfiki przedsiębiorczości startupowej oraz w zakresie metodyki zarządzania startupem: Lean Startup.

W1: Innowacje. Przedsiębiorczość innowacyjna a inne formy przedsiębiorczości. Startupy jako szczególne formy organizacji aktywności przedsiębiorczej,
W2: Lean Startup jako metodyka zarządzania startupem i jej składowe: zwinny rozwój produktu (agile development), odkrywanie klienta (customer development) i modelowanie biznesowe; triada: klient-problem- rozwiązanie (CPS),
W3: Modelowanie biznesowe na bazie kanwy modelu biznesowego oraz kanwy propozycji wartości wg Osterwaldera; struktura modelu i formułowanie hipotez biznesowych,
W4: Weryfikowanie hipotez biznesowych w procesie modelowania biznesowego; odkrywanie klienta – zasady projektowania i przeprowadzania wywiadów z interesariuszami projektu; prototypowanie, koncepcja MVP,
W5: Model biznesowy jako narzędzie wdrażania zmian i innowacji w przedsiębiorstwie.

PROJEKT

Praca nad projektem startupu – co najmniej zakończenie etapu Customer Discovery – na projekcie własnym (w grupach).

P0: Selekcja pomysłów na projekty, elementy debaty
P1: Sformułowanie hipotez biznesowych: CPS i archetypu klienta (tworzenie persony)
P2-P3: Kanwa propozycji wartości i kanwa modelu biznesowego – warsztaty projektowe w grupach
P4: Zaprojektowanie wywiadów i przeprowadzenie ich
P5: Weryfikacja hipotez biznesowych, analiza konkurencji
P6: Zajęcia mentoringowe, zajęcia z gościem i/lub w inkubatorze i akceleratorze innowacji PW
P7: Zasady prawidłowego „pitcha" projektu, prezentacji pomysłu i pracy nad jego weryfikacją i rozwojem
P8-P9: Prezentacja końcowa projektu (w obecności gości spoza uczelni – inwestorzy, przedsiębiorcy, eksperci)

Efekty uczenia się dla przedmiotu

Symbol efektu uczenia się dla przedmiotu	Opis efektów uczenia się	Symbole efektów uczenia się dla programu studiów	Sposób weryfikacji
	Student		
WIEDZA			
W01	Zna i rozumie podstawowe zasady tworzenia i rozwoju różnych form indywidualnej przedsiębiorczości, a zwłaszcza innowacyjnych, ambitnych i dynamicznych form organizacji typu startup.	W_13	Aktywność na zajęciach, kolokwium
W02	Ma podstawową wiedzę w zakresie ochrony własności intelektualnej w kontekście tworzenia i rozwijania startupów – innowacyjnych form przedsiębiorczości.	W_12	Kolokwium
UMIEJĘTNOŚCI			
U01	Potrafi przygotować opracowanie i przedstawić prezentację ustną (w języku polskim lub w języku angielskim), tzw. prezentację inwestorską: „pitch" na temat tworzonego startupu i jego modelu biznesowego.	U_10	Projekt zespołowy – prace cząstkowe prezentowane i omawiane na kolejnych zajęciach, prezentacja końcowa
U02	Potrafi komunikować się przy użyciu różnych technik multimedialnych w środowisku zawodowym oraz w innych środowiskach (w języku polskim lub w języku angielskim) w zakresie tworzenia i walidacji startupu i modelu biznesowego.	U_11	Prezentacja końcowa
U03	Potrafi pracować indywidualnie oraz współdziałać z innymi osobami w ramach prac zespołowych nad tworzeniem i walidacją koncepcji startupu.	U_13	Projekt zespołowy – prace cząstkowe prezentowane i omawiane na kolejnych zajęciach
U04	Potrafi określić kierunki dalszego uczenia się, zaplanować i zrealizować proces samokształcenia, a także ukierunkowywać innych w tym zakresie – w ramach prac nad tworzeniem startupu.	U_14	Projekt zespołowy – prace cząstkowe prezentowane i omawiane na kolejnych zajęciach, prezentacja końcowa
KOMPETENCJE SPOŁECZNE			
K01	Jest gotów do myślenia i działania w sposób innowacyjny i przedsiębiorczy, przewodzenia grupie i ponoszenia odpowiedzialności za nią.	K_03	Projekt zespołowy – prace cząstkowe prezentowane i omawiane na kolejnych zajęciach, prezentacja końcowa

CYBERPRZESTĘPCZOŚĆ

rodzaj zajęć/liczba godzin	wykład	0
	ćwiczenia	10
	laboratorium	0
	projekt	6
	zajęcia zintegrowane (warsztaty)	14
liczba punktów ECTS	2	
status przedmiotu	obowiązkowy	

Treści kształcenia

Przedmiot opiera się na założeniu, że praca zawodowa oraz prowadzenie działalności gospodarczej w sektorze informatycznym wymaga znajomości podstawowych koncepcji prawnych oraz ryzyka prawnego związanego z obszarem cyberprzestępczości.

Podczas zajęć omówione zostaną teoretyczne i praktyczne aspekty zwalczania i zapobiegania cyberprzestępczości przy wykorzystaniu narzędzi prawnych oraz współpracy z wymiarem sprawiedliwości, w tym organami ścigania. Studenci zapoznają się także z tendencjami rozwojowymi prawa i procesu karnego w obszarze cyberprzestępczości.

Przedmiot ma na celu dostarczenie wiedzy oraz kształtowanie umiejętności praktycznych i kompetencji społecznych w tym zakresie. Zamierzone cele dydaktyczne można podzielić na dwie grupy – merytoryczne (opanowanie kluczowych pojęć, zrozumienie instytucji prawnych i zasad prawa karnego materialnego i procesu karnego, prawne aspekty prowadzenia audytów bezpieczeństwa informatycznego) oraz osiągnięcie określonych umiejętności praktycznych (identyfikowanie ryzyka prawnego w obszarze cyberprzestępczości, identyfikowanie ryzyka niezgodności z prawem prowadzonej działalności gospodarczej lub zawodowej, dokonywanie wykładni przepisów w zakresie prawa karnego materialnego i postępowania karnego umożliwiające ich poprawne zastosowanie w praktyce, umiejętność opracowania rozwiązań prawnych sytuacji kryzysowych związanych z cyberprzestępczością).

Podczas zajęć studenci zostaną zapoznani z zagrożeniami wynikającymi z wykorzystywania rozwoju telekomunikacji przez pojedynczych przestępców i zorganizowane grupy przestępcze.

Uczestnicy zajęć zostaną podzieleni na grupy projektowe, w których każdemu z uczestników zostanie przydzielona odrębna rola i zadanie. Studenci w ramach wyznaczonego zadania projektowego (kazusu dotyczącego cyberprzestępstwa), przygotują memorandum (raport) identyfikujące:
- ryzyka prawne i pozaprawne odnoszące się do przedstawionego problemu;
- kwalifikację prawną cyberprzestępstwa wraz z identyfikacją jego znamion i potrzebami dowodowym w tym zakresie;
- propozycje kroków prawnych, jakie należy podjąć w reakcji na zidentyfikowany problem;
- propozycje rozwiązań ograniczających ryzyko wiktymizacji omawianym cyberprzestępstwem.

Zadania w ramach grupy projektowej zostaną zaprojektowane i rozdzielone w taki sposób, aby ocenić indywidualny wkład każdego z uczestników w projekt oraz pracę zespołową w projekcie. Projekty będą prezentowane przez uczestników podczas zajęć, a sposób przedstawienia projektu także będzie podlegał ocenie.

Niezależnie od ww. pracy projektowej w toku zajęć (w ramach bloków I i II) ich uczestnicy będą dzieleni na grupy pracujące nad kazusami prawnymi przedstawionymi podczas zajęć w oparciu o materiały zapewnione przez prowadzącego. Aktywność podczas rozwiązywania kazusów, sposób prowadzenia argumentacji i prawidłowość prezentowanych wniosków będą podlegały ocenie.

ĆWICZENIA (zajęcia w tygodniach 1-5)

Blok tematyczny I: Kluczowe zagadnienia procesu karnego w sprawach cyberprzestępstw.

1. Wstęp do prawa karnego i procesu karnego w obszarze cyberprzestępstw:
   - statystyczne i socjologiczne ujęcie problemu cyberprzestępczości,
   - pojęcie przestępstwa i cyberprzestępstwa,
   - podstawy odpowiedzialności karnej za cyberprzestępstwo
   - model postępowania dotyczącego odpowiedzialności karnej za cyberprzestępstwo
   - etyka, moralność a cyberprzestępczość.
2. Prawne narzędzia reagowania na incydenty bezpieczeństwa:
   - audyt bezpieczeństwa informatycznego i ryzyka prawne z nim związane,
   - gromadzenie dowodów niezbędnych dla postępowania karnego,
   - zawiadomienie o możliwości popełnienia przestępstwa – skuteczny sposób redagowania,
   - reprezentacja pokrzywdzonego w postępowaniu,
   - obowiązki audytora w procesie karnym.
3. Postępowania przygotowawcze dotyczące cyberprzestępstw:
   - organy ścigania i instytucje państwa powołane do zwalczania cyberprzestępczości i reagowania na incydenty dot. bezpieczeństwa informatycznego,
   - czynności związane ze śledztwami w sprawach cyberprzestępstw,
   - przeszukanie i inne czynności procesowe,
   - działalność biegłych.
4. Postępowania sądowe dotyczące cyberprzestępstw:
   - kluczowe prawa i obowiązki stron postępowania,
   - reprezentacja pokrzywdzonego (ze szczególnym uwzględnieniem osób prawnych, w tym przedsiębiorstw lub instytucji).
5. Obrona w sprawach dotyczących cyberprzestępczości:
   - unikanie ryzyka popełnienia cyberprzestępstwa i pociągnięcia do odpowiedzialności karnej za cyberprzestępstwo,
   - ograniczanie ryzyka prawnego w obszarach ryzykownych z perspektywy cyberprzestępczości,
   - prawo do obrony w postępowaniu karnym dot. cyberprzestępczości,
   - ochrona praw i wolności oskarżonego o popełnienie cyberprzestępstwa.

ZAJĘCIA ZINTEGROWANE (zajęcia w tygodniach 6-12).

Blok tematyczny II: Typologia cyberprzestępstw oraz case studies.

6. Komputery i sieci jako narzędzia popełniania przestępstw:
   - spam (spam na portalach społecznościowych, spam nigeryjski itd.),
   - kradzież tożsamości,
   - phishing,
   - darknet,
   - nielegalny hazard.
7. Komputery i sieci jako narzędzia popełniania przestępstw:
   - tzw. fałszerstwa komputerowe,
   - hate crimes,
   - false advertising,
   - przetwarzanie i rozpowszechnianie treści zabronionych (treści pornograficzne z udziałem małoletniego, publiczne znieważanie grupy ludności albo poszczególnej osoby, treści mogące ułatwić popełnienie przestępstwa o charakterze terrorystycznym).
8. Cyberprzestępstwa przeciw poufności, integralności i dostępności danych:
   - malware,
   - dDoS,
   - hacking,
   - pharming,
   - podsłuch,
   - nielegalna ingerencja w dane lub w funkcjonowanie systemu,
   - wyłudzenia danych osobowych,
   - wytwarzanie, sprzedaż, oferowanie, posiadanie urządzeń służących do popełniania cyberprzestępstw.

9. Cyberprzestępstwa w obszarze własności intelektualnej:
   - plagiat,
   - tzw. piractwo internetowe,
   - problematyka streamingu i sharingu a cyberprzestępczość,
   - wykorzystywanie sieci do naruszeń własności przemysłowej.
10. Cyberprzestępstwa w obszarze e-commerce:
   - oszustwa na aukcjach internetowych,
   - oszustwa telekomunikacyjne,
   - wyłudzenia w obszarze cyberprzestępczości.
11. Cyberprzestępstwa w obszarze bankowości elektronicznej i usług finansowych:
   - pranie pieniędzy i finansowanie terroryzmu,
   - kryptowaluty a cyberprzestępczość,
   - przestępcze wykorzystanie płatności anonimowych,
   - carding.
12. Cyberterroryzm:
   - aktywizm i haktywizm,
   - cyberwarfare,
   - cyberprzestępczość a finansowanie terroryzmu i typowa działalność terrorystyczna,
   - cyberprzestępczość a przestępczość zorganizowana,
   - cyberprzestępczość a szpiegostwo.

PROJEKT (zajęcia w tygodniach 13-15).

Ostatni blok zajęć zostanie poświęcony prezentacji projektów przygotowanych przez studentów w ramach pracy w grupach projektowych. Uczestnicy zajęć przedstawią grupie case-study, które opracowali jako grupa projektowa oraz zaproponują rozwiązanie napotkanych problemów z zakresu cyberprzestępczości. Po prezentacji każdej z grup projektowych przewidziana jest dyskusja oraz sesja pytań i odpowiedzi (Q&A), podczas której grupa projektowa będzie odpowiadać na pytania uczestników zajęć i prowadzącego

Efekty uczenia się dla przedmiotu

symbol efektu uczenia się dla przedmiotu	opis efektów uczenia się	symbole efektów uczenia się dla programu studiów	sposób weryfikacji
	Student		
WIEDZA			
W01	Zna i rozumie problemy prawne związane z cyberprzestępczością, jej wykrywaniem i zwalczaniem.	W_01 W_10	Memorandum (raport) z projektu, praca projektowa w trakcie zajęć
W02	Posiada podstawową wiedzę o narzędziach prawnych służących do dochodzenia odpowiedzialności sprawców cyberprzestępstw.	W_01 W_10 W_11	Memorandum (raport) z projektu
W03	Rozumie etyczne, prawne i społeczny aspekty zwalczania cyberprzestępczości.	W_10 W_11	Memorandum (raport) z projektu, praca projektowa w trakcie zajęć
W04	Posiada wiedzę na temat ryzyka prawnego związanego z bezprawnym lub nieprawidłowym przetwarzaniem danych.	W_01 W_10 W_11	Memorandum (raport) z projektu
W05	Posiada wiedzę na temat ryzyka prawnego związanego z naruszeniem prawa w zakresie ochrony własności intelektualnej, własności przemysłowej oraz z czynami nieuczciwej konkurencji.	W_12	Memorandum (raport) z projektu
UMIEJĘTNOŚCI			
U01	Potrafi interpretować normy prawne w stopniu umożliwiającym identyfikację ryzyka prawnego w obszarze cyberbezpieczeństwa.	U_01	Praca projektowa w trakcie zajęć
U02	Potrafi przygotować opracowanie i przedstawić prezentację ustną przedstawiającą praktyczne aspekty postępowania zgodnie z przepisami prawa w sytuacjach ryzyka prawnego w obszarze cyberbezpieczeństwa.	U_10	Memorandum (raport) z projektu
U03	Potrafi ocenić aspekty etyczne i prawne odnoszące się do zjawiska cyberprzestępczości i uwzględnić czynniki społeczne w zapobieganiu cyberprzestępczości.	U_08	Memorandum (raport) z projektu
U04	Potrafi zidentyfikować aktualne problemy prawne odnoszące się do zjawiska cyberprzestępczości oraz uwzględnić ryzyka prawne w tym zakresie w przyszłej działalności zawodowej.	U_08 U_13	Memorandum (raport) z projektu, prezentacja memorandum
KOMPETENCJE SPOŁECZNE			
K01	Umie w zrozumiały sposób prezentować rozwiązania i strategie cyberbezpieczeństwa odbiorcom nietechnicznym z uwzględnieniem podstawowych aspektów prawnych.	K_02	Praca projektowa w trakcie zajęć
K02	Potrafi planować rozwój swoich kompetencji zawodowych, oraz przewidywać i rozwijać nowe trendy z zakresu cyberbezpieczeństwa, biorąc pod uwagę ich aspekty prawne i etyczne.	K_03	Memorandum (raport) z projektu, prezentacja memorandum

METODY MATEMATYCZNE W CYBERBEZPIECZEŃSTWIE

rodzaj zajęć/liczba godzin	wykład	15
	ćwiczenia	15
	laboratorium	0
	projekt	30
	zajęcia zintegrowane (warsztaty)	0
liczba punktów ECTS	4	
status przedmiotu	obowiązkowy	

Treści kształcenia

WYKŁAD

1. Faktoryzacja macierzy (4 godz.).

Nieujemna i dodatnia określoność macierzy kwadratowej, związek z wartościami własnymi.
Rozkłady macierzy: QR, LU, SVD (wg wartości osobliwych), rozkład spektralny macierzy. Normy macierzowe.

2. Wprowadzenie do logik temporalnych (4 godz.).

Elementy logiki modalnej. Podstawy logiki temporalnej: aspekty syntaktyki oraz semantyka (np. modele Kripkego). Postać normalna formuł. Reguły wnioskowania i równoważność formuł. Automaty Büchi a logika temporalna. Logiki temporalne z liniową strukturą czasu (LTL) oraz z rozgałęzioną strukturą czasu (CTL). Przykładowe modele.

3. Kody korekcyjne (4 godz.).

Kody liniowe nad dowolnymi ciałami skończonymi. Kody BCH jako kody poprawiające błędy wielokrotne. Niebinarne kody Reeda-Solomona. Uogólnione kody RS. Kody alternujące.

4. Kraty stosowane w kryptografii (3 godz.).

Wprowadzenie podstawowych pojęć dotyczących krat, kraty q-arne, wyznacznik kraty. Istnienie niezerowych wektorów o minimalnej długości. Twierdzenie Blichfeldta, twierdzenia Minkowskiego.

ĆWICZENIA

Ćwiczenia audytoryjne będą ilustracją problemów poruszanych na wykładach. Ponadto będą stanowiły uzupełnienie wykładów o następujące zagadnienia:

1. Funkcje macierzy. Eksponenta macierzy.
2. Operatory sprzężone i unitarne. Macierze Householdera.
3. Własności ciał skończonych. Wielomiany nad ciałami skończonymi.
4. Kody Goppa w kryptografii. System McEliece z kluczem publicznym.
5. Zredukowana baza w 2-wymiarowej kracie. Uogólniony algorytm Gaussa.

PROJEKT

W ramach projektu kilkuosobowe zespoły będą opracowywać prezentacje zastosowań praktycznych zagadnień omawianych na wykładach lub na ćwiczeniach. W zakres tematyki projektów będą wchodziły między innymi:

1. Metody numeryczne znajdywania wartości własnych.
2. Wybrane implementacje i zastosowania algorytmów rozkładu macierzy do zagadnień związanych z cyberbezpieczeństwem.
3. Rozwiązywanie układów równań z wykorzystaniem faktoryzacji macierzy.
4. Metody formalne analizy bezpieczeństwa protokołów z wykorzystaniem logiki temporalnej.
5. Zastosowanie wybranych metod kodowania korekcyjnego w praktyce.
6. Przykładowe techniki kryptoanalizy dla systemów kryptograficznych opartych na kodach liniowych (np. atak Sidelnikov-Shestakov).
7. Wybrane algorytmy aproksymacyjne problemów kratowych: problem najkrótszego wektora w kracie (SVP), problem najbliższego wektora w kracie (CVP), problem najkrótszych wektorów liniowo niezależnych (SIVP).
8. Zastosowanie metody Coppersmitha znajdowania rozwiązań równań wielomianowych do ataków na system RSA.

Ponadto elementem projektu będzie przygotowanie materiałów z danego zakresu dla studentów z pozostałych grup projektowych

Efekty uczenia się dla przedmiotu

symbol efektu uczenia się dla przedmiotu	opis efektów uczenia się	symbole efektów uczenia się dla programu studiów	sposób weryfikacji
	Student		
WIEDZA			
W01	Ma wiedzę ogólną w zakresie metod i algorytmów stosowanych w algebrze liniowej.	W_05	Kolokwium pisemne, aktywność podczas zajęć; projekt #1,3
W02	Zna podstawy logiki temporalnej.	W_05	Kolokwium pisemne, aktywność podczas zajęć
W03	Zna algorytmy kodowania i dekodowania dla wybranych liniowych kodów korekcyjnych.	W_05	Kolokwium pisemne, aktywność podczas zajęć
W04	Zna podstawowe zagadnienia dotyczące krat.	W_05	Kolokwium pisemne, aktywność podczas zajęć
UMIEJĘTNOŚCI			
U01	Potrafi wykorzystać nabytą wiedzę z algebry liniowej do zagadnień z zakresu analizy danych.	U_01 U_11 U_13	Kolokwium pisemne, aktywność podczas zajęć; projekt #2
U02	Potrafi wykorzystać metody logiki temporalnej do weryfikacji własności prostych systemów zmiennych w czasie.	U_01 U_10	Kolokwium pisemne, aktywność podczas zajęć; projekt #4
U03	Posiada umiejętność zastosowania krat oraz kodów korekcyjnych w kryptografii postkwantowej.	U_01 U_10 U_13	Aktywność podczas zajęć; projekt #5-8
KOMPETENCJE SPOŁECZNE			
K01	Rozumie przydatność nabytej wiedzy i umiejętności obliczeniowych do stawiania hipotez oraz ich weryfikacji w możliwych zastosowaniach.	K_01	Samoocena
K02	Umie współpracować w grupie.	K_03	Projekty: współpraca i aktywność podczas zajęć

ROZPOZNAWANIE WZORCÓW

przedmiot prowadzony w języku angielskim
PATTERN RECOGNITION

rodzaj zajęć/liczba godzin	wykład	30
	ćwiczenia	0
	laboratorium	0
	projekt	0
	zajęcia zintegrowane (warsztaty)	0
liczba punktów ECTS	2	
status przedmiotu	obowiązkowy	

Treści kształcenia

WYKŁAD

Wprowadzenie: elementy systemu rozpoznawania obrazu; cykl projektowy tworzenia klasyfikatora; metody oceny jakości klasyfikatorów i systemów klasyfikacji.
Optymalna klasyfikacja Bayesa: rola informacji a priori; postać funkcji gęstości prawdopodobieństwa; optymalny klasyfikator Bayesa; ryzyko/strata decyzji klasyfikacyjnej; granice decyzyjne klasyfikatorów; zgodność rozkładu danych z przyjętym modelem gęstości prawdopodobieństwa.
Metody najbliższego sąsiedztwa: dopasowanie wzorców; klasyfikatory minimalno-odległościowe; metryki; klasyfikatory k-NN; metody wyszukiwania najbliższych sąsiadów; przyspieszanie poszukiwania najbliższego sąsiada; edycja i redukcja zestawu treningowego.
Klasyfikacja liniowa: liniowe funkcje decyzyjne; przestrzeń jednorodna; wyznaczanie granicy decyzyjnej; agregacja wyników klasyfikacji dla więcej niż dwóch klas; metoda wektorów nośnych; sekwencyjny minimalny algorytm optymalizacji.
Redukcja wymiarowości: analiza składowych głównych (PCA); liniowa klasyfikacja Fishera; wielowymiarowa analiza dyskryminacyjna (MDA).
Grupowanie: sformułowanie problemu grupowania; ocena podobieństwa grupowania; algorytmy typu k-średnich; grupowanie wstępujące; algorytmy grafowe.
Sieci neuronowe: podstawowy model neuronu; algorytmy uczenia pojedynczego neuronu; interpretacja działania pojedynczego neuronu; sieci neuronowe; algorytm wstecznej propagacji błędów; sieci splotowe i ze sprzężeniami zwrotnymi; przykłady zastosowań poza klasyfikacją wzorców.
Modele Markowa: dyskretne procesy Markowa; ukryty proces Markowa; algorytm Viterbiego; algorytm Bauma-Welsha do wyznaczania parametrów modelu Markowa; problemy wykorzystania modeli Markowa w klasyfikacji.
Wyszukiwanie tekstu: problem dokładnego i przybliżonego wyszukiwania tekstu; algorytm Boyera-Moora; odległość edycyjna; analiza tekstu z wykorzystaniem automatów niedeterministycznych i deterministycznych; drzewo i tablica przyrostków; algorytm Ukkonena do konstruowania drzewa przyrostków; przybliżone wyszukiwanie z drzewami przyrostkowymi; generowanie sąsiedztwa do wyszukiwania z błędami; funkcje skrótu do szybkiego wyszukiwania.
Drzewa decyzyjne: konstruowanie drzew decyzyjnych - podstawowy algorytm CART; ocena niejednorodności węzłów drzewa; kryteria zatrzymania podziału węzła podczas budowania drzewa; efekt horyzontu; algorytmy przycinania drzew.
Poprawa jakości klasyfikacji: podstawowe problemy projektowania metaklasyfikatorów; schematy głosowania; kwestia niezależności klasyfikatorów; głosowanie z wagami; wyznaczanie wag; Bayesowskie metody komponowania wyników klasyfikatorów; przestrzeń wiedza-zachowanie; metody konstruowania zbiorów słabych klasyfikatorów (algorytm AdaBoost); wykorzystanie informacji kontekstowych w klasyfikacji; kontekst w systemach OCR; korzystanie ze słowników i trigramów.

LECTURES

Introduction: components of the image recognition system; design cycle of creating a classifier; methods of quality assessment of classifiers and classification systems.

Optimal Bayesian Classification: the role of a priori information; the form of the probability density function; optimal Bayes classifier; the risk / loss of the classification decision; decision boundaries of classifiers; compliance of the data distribution with the adopted theoretical distribution.
Nearest Neighbour Methods: Template Matching; minimum distance classifiers; metrics; k-NN classifiers; nearest neighbour search methods; speeding up the search for the nearest neighbour; editing and reduction of the training set.
Linear Classification: linear decision functions; homogeneous space; learning the decision boundary; assembling of individual classifiers' results for more than two classes; support vector method; sequential minimal optimization algorithm.
Dimensionality Reduction: Principal Component Analysis; Fisher's linear classification; multivariate discriminant analysis (MDA).
Clustering: clustering problem; assessment of clustering similarity; k-means class algorithms; bottom-up clustering; graph algorithms.
Neural Networks: basic model of the neuron; single neuron learning algorithms; interpretation of the operation of a single neuron; neural networks; error backpropagation algorithm; convolutional and feedback networks; application examples beyond image recognition.
Markov Models: discrete Markov processes; hidden Markov process; Viterbi's algorithm; Baum-Welsh algorithm for determining the parameters of the Markov system; problems of using Markov models in classification.
Text Searching: the problem of exact and approximate text search; Boyer-Moor algorithm; edit distance; text analysis with the use of nondeterministic and deterministic automata; tree and table of suffixes; Ukkonen's algorithm for constructing a suffix tree; approximate search with suffix trees; neighbourhood generation for search with errors; hash functions for quick searches.
Decision Trees: constructing decision trees - basic CART algorithm; assessment of tree node heterogeneity; stop criteria when building a tree; horizon effect; tree pruning algorithms.
Quality of Classification Improvement: basic problems of designing meta-classifiers; voting schemes; the issue of the independence of classifiers; voting with weights; determination of weights; Bayesian methods of composing the results of classifiers; Behaviour-Knowledge space; methods of constructing sets of weak classifiers (AdaBoost algorithm); use of contextual information in classification; context in OCR systems; use of dictionaries and trigrams.

Efekty uczenia się dla przedmiotu

Symbol efektu uczenia się dla przedmiotu	Opis efektów uczenia się	Symbole efektów uczenia się dla programu studiów	Sposób weryfikacji
	Student		
WIEDZA			
W01	Zna podstawowe metody klasyfikacji wzorców.	W_05 W_06	Sprawdziany
W02	Zna metody wstępnej analizy danych oraz ich grupowania.	W_05	Sprawdziany
W03	Zna podstawowe metody konstruowania zespołów klasyfikatorów.	W_05	Sprawdziany
UMIEJĘTNOŚCI			
U01	Potrafi krytycznie ocenić rozwiązanie problemu klasyfikacji i zaproponować jego usprawnienia.	U_01 U_09 U_12	Sprawdziany
U02	Potrafi porozumiewać się w języku angielskim, w szczególności w kwestiach związanych z rozpoznawaniem wzorców.	U_12	Sprawdziany
KOMPETENCJE SPOŁECZNE			
-	-	-	-

TECHNIKI I TECHNOLOGIE BIG DATA

rodzaj zajęć/liczba godzin	wykład	30
	ćwiczenia	0
	laboratorium	0
	projekt	0
	zajęcia zintegrowane (warsztaty)	0
liczba punktów ECTS	2	
status przedmiotu	obowiązkowy	

Treści kształcenia

WYKŁAD

1. Wprowadzenie do zagadnień przetwarzania Big Data. Wprowadzenie do przedmiotu, omówienie spraw organizacyjnych, cele zajęć oraz ich program. Omówienie przyczyn zmian w podejściu do retencji danych. Przedstawienie rysu historycznego metod składowania oraz analizy dużych zbiorów danych. Omówienie najważniejszych zagadnień związanych z Big Data: architektura lambda, przetwarzanie strumieniowe vs przetwarzanie batchowe, orkiestracja, serializacja i deserializacja danych, bazy NoSQL. Przedstawienie czołowych projektów z obszaru Big Data: Hadoop, Spark, Cassandra. (2 godziny).
2. Podstawowe komponenty ekosystemu Hadoop: wprowadzenie do YARN i HDFS. (2 godziny).
3. Sposób organizacji danych: pojęcie jeziora danych (data lake), analityka oraz bazy klucz-wartość, serializacja i deserializacja danych, formaty (ORC, Parquet), Cassandra, HBase, pojęcie schematu danych i ewolucji na przykładzie Avro, wsparcie dla ACID na przykładzie DeltaLake czy Iceberg. Porównanie wydajności różnych konfiguracji dla rzeczywistych przypadków użycia, pochodzących z projektów badawczych. (4 godziny).
4. Apache Spark. Omówienie koncepcji i zastosowań RDD (historycznie) i DataFrame. Architektura Spark (cluster manager, executor'y). Porównanie przetwarzania z Hadoop MapReduce oraz dyskusja dotycząca optymalizacji. Powiązanie z platformą Hadoop poprzez Resource Manger'a oraz wersja standalone (local). Omówienie API na podstawie przykładowego job'a. (4 godziny).
5. Analityka Big Data - SQL w środowisku Big Data (na przykładzie SparkSQL, Hive). Analiza danych z Hadoop za pomocą R i innych środowisk analitycznych (pyspark + jupyter). Przykłady potoków przetwarzania wykorzystywanych w projektach badawczych prowadzonych przez prowadzących. (4 godziny).
6. Wizualizacja danych – środowisko R/Python + narzędzia D3, Leaflet, Vega, deck.gl. Omówienie podstawowych pojęć i strategii wizualizacji danych z uwzględnieniem przede wszystkim danych ilościowych i danych geograficznych. (2 godziny).
7. Przetwarzanie strumieniowe. Wprowadzenie do narzędzi służących przetwarzaniu strumieni danych: Kafka, Spark Streaming, Apache Flink, Apache Beam. Przykład algorytmu strumieniowego z wykorzystaniem struktur danych takich jak: count min sketch, bloom filter. (4 godziny).
8. Big Data w chmurze. Przedstawienie architektur chmurowych, wirtualizacji i kontenerów, systemów zarządzania chmurą (OpenShift, K8S), Przykładowe osadzenie projektu big data w chmurze. Przedstawienie heterogenicznych środowisk obliczeniowych i zarządzania zasobami oraz ich izolacji za pomocą konteneryzacji. (2 godziny).
9. Zapewnienie bezpieczeństwa w środowisku rozproszonym – uwierzytelnienie (Kerberos) oraz scentralizowana autoryzacja dostępu do zasobów (Apache Ranger. Integracja z istniejącymi systemami bezpieczeństa, wykorzystanie impersonacji uzytkowników, bezpieczeństwo w środowisku kontenerowym. (2 godziny).
10. Uczenie maszynowe w środowiskach rozproszonych z wykorzystaniem bilbiotek TensorFlow. Wprowadzenie do uczenia maszynowego na przykładzie sieci neuronowych oraz głębokich sieci neuronowych. Wprowadzenie do TensorFlow oraz przykłady implementacji rozproszonej m.in. w oparciu o rozwiązania chmurowe. (4 godziny).

Efekty uczenia się dla przedmiotu

Symbol efektu uczenia się dla przedmiotu	Opis efektów uczenia się	Symbole efektów uczenia się dla programu studiów	Sposób weryfikacji
	Student		
WIEDZA			
W01	Zna mechanizmy zapewnienia bezpieczeństwa w systemach rozproszonych.	W_02	Kolokwia pisemne
W02	Zna metody stosowane w implementacji rozproszonych narzędzi wykorzystujących metody uczenia maszynowego.	W_06	Kolokwia pisemne
W03	zna sposoby organizacji danych w systemach Big Data, w tym formaty i silniki zapytań stosowane w rozproszonych bazach danych.	W_06	Kolokwia pisemne
W04	Zna metody stosowane w analityce Big Data, w tym metody integracji potoków przetwarzania danych.	W_06	Kolokwia pisemne
W05	Zna podstawowe architektury stosowane w systemach chmur obliczeniowych, sposoby konteneryzacji oraz systemy zarządzania chmurą.	W_06	Kolokwia pisemne
W06	Zna podstawowe komponenty ekosystemu Hadoop.	W_06	Kolokwia pisemne
W07	Zna koncepcję przetwarzania w Apache Spark, w tym stosowane struktury danych RDD, dataframe.	W_06	Kolokwia pisemne
W08	Zna metody stosowane do wizualizacji danych Big Data.	W_06	Kolokwia pisemne
W09	Zna koncepcje i metody stosowane do przetwarzania strumieniowego w systemach Big Data.	W_06	Kolokwia pisemne
UMIEJĘTNOŚCI			
-	-	-	-
KOMPETENCJE SPOŁECZNE			
-	-	-	-

ANALIZA DANYCH W CYBERBEZPIECZEŃSTWIE (PBL1)

rodzaj zajęć/liczba godzin	wykład	0
	ćwiczenia	0
	laboratorium	0
	projekt	30
	zajęcia zintegrowane (warsztaty)	90
liczba punktów ECTS	8	
status przedmiotu	obowiązkowy	

Treści kształcenia

PROJEKT

Projekt będzie wykonywany w zespołach 3-5 osobowych. Zajęcia związane z realizacją projektu odbywają w wymiarze 2 godz. w każdym tygodniu w formie konsultacji poszczególnych zespołów z opiekunami.

Zakłada się sześć etapów projektu, każdy z etapów będzie dotyczył kolejnego etapu procesu analizy danych w zastosowaniach w różnych obszarach cyberbezpieczeństwa. Wykonanie każdego etapu będzie potwierdzone napisaniem krótkiego raportu cząstkowego, zaś raporty cząstkowe będą stanowiły kolejne rozdziały raportu finalnego. Raport finalny będzie prezentował wyniki całego projektu w ramach przedmiotu. Zakłada się następujące etapy projektu:

1. Analiza literatury dotyczącej: wybranego problemu/zagadnienia, sposobów analizy danych, narzędzi do analizy danych i ich zastosowania w różnych obszarach cyberbezpieczeństwa;
2. Stawianie hipotez dotyczących problemu np. możliwość lokalizacji/momentu nieuprawnionego dostępu do zasobów;
3. Badanie zależności między podzbiorami danych a hipotezami;
4. Budowa modeli informacyjnych dotyczących testowania i weryfikacji hipotez;
5. Testowanie i weryfikacja poprawności hipotez; ocena stosowalności opracowanych rozwiązań w praktyce cyberbezpieczeństwa;
6. Synteza wyników.

Ze względu na charakter badawczy projektu, studenci będą stawiali kolejne hipotezy („prototypy"), testowali je, a następnie ulepszali je bądź ponownie formułowali. Powyższe etapy nie będą realizowane liniowo i możliwe będą nawroty. Wymagane będzie przeprowadzenie co najmniej jednego nawrotu. Zakłada się, że na każdy etap będzie przeznaczone około 2-3 tygodni.
Każdy ze studentów będzie oceniany indywidualnie (za wykonaną pracę indywidualną) oraz za wyniki pracy całego zespołu projektowego. Wyraźny podział zadań między członków zespołu będzie jednym z zadań projektowych. Część zespołowa będzie oceniać: wykonaną pracę, wyniki, współpracę nad poszczególnymi elementami raportu i jego spójność.
Synteza wyników projektu zostanie opublikowana w wybranej sieci społecznościowej i będzie stanowiła integralną część raportu.

ZAJĘCIA ZINTEGROWANE

Zajęcia zintegrowane uzupełniają tworzenie projektu przez studentów. Zajęcia te będą odbywały się co tydzień. Ich celem jest przedyskutowanie bieżącej pracy studentów, dostarczenie im wiedzy i wskazówek dotyczącej prowadzonego projektu. Na wybranych zajęciach zintegrowanych studenci otrzymają pracę domową, którą będą musieli zrealizować na kolejne zajęcia.

Zgodnie z zasadami PBL na pierwszych zajęciach studenci otrzymają informacje na temat dostępnych zbiorów danych odnoszących się do różnych obszarów cyberbezpieczeństwa i zestaw niedookreślonych zagadnień/problemów, potencjalnie możliwych do rozwiązania przy pomocy tych zbiorów.

Harmonogram zajęć zintegrowanych:

1. Zajęcia wstępne, podział studentów na zespoły, praca nad tematami projektów wybraną metodą. z zakresu analizy danych.
2. Prowadzenie badań literaturowych dotyczących wybranego problemu/zagadnienia oraz metod analizy danych w różnych obszarach cyberbezpieczeństwa, wybór obiecujących rozwiązań. Zebranie potencjalnych metod na rozwiązanie problemu.
3. Burza mózgów dotycząca potencjalnych metod rozwiązania zredefiniowanego problemu, wybór obiecujących rozwiązań, postawienie pierwszych hipotez dotyczących analizy danych.
4. Zajęcia w formie demonstracyjno-dyskusyjnej z naciskiem na zaangażowanie studentów (mikro prezentacje problemów cząstkowych, przygotowywanie schematów, (info)grafik, map myśli wraz z omówieniem): źródła, struktury danych, metody pozyskania i agregacja danych, przegląd algorytmów w kontekście postawionego problemu badawczego.
5. Zajęcia w formie demonstracyjno-dyskusyjnej z naciskiem na zaangażowanie studentów (mikro prezentacje problemów cząstkowych, przygotowywanie schematów, (info)grafik, map myśli wraz z omówieniem): preprocessing, techniki manipulacji na dużych zbiorach danych i modelowanie zbiorów danych na potrzeby np. uczenia maszynowego,
6. Zajęcia w formie demonstracyjno-dyskusyjnej z naciskiem na zaangażowanie studentów (mikro prezentacje problemów cząstkowych, przygotowywanie schematów, (info)grafik, map myśli wraz z omówieniem): budowa, specyfikacja i implementacja modeli w odniesieniu do wypracowanej hipotezy.
7. Zajęcia w formule otwartych prezentacji, na których studenci przedstawiają: charakterystykę analizowanych danych, problem do rozwiązania, sformułowane hipotezy i sformułowanie dalszych kroków.
8. Zajęcia w formule otwartych prezentacji: wstępny rekonesans opracowanych rozwiązań, weryfikacja założeń względem osiągniętych wyników.
9. Remodelowanie rozwiązań, rozszerzenie badań literaturowych.
10. Zajęcia w formule demonstracyjno-dyskusyjnej z naciskiem na zaangażowanie studentów (mikro prezentacje problemów cząstkowych, przygotowywanie schematów, (info)grafik, map myśli wraz z omówieniem): trening, parametryzacja modeli.
11. Zajęcia w formule demonstracyjno-dyskusyjnej z naciskiem na zaangażowanie studentów (mikro prezentacje problemów cząstkowych, przygotowywanie schematów, (info)grafik, map myśli wraz z omówieniem): modelowanie testowania oraz technik weryfikacyjnych.
12. Zajęcia otwarte w formie prezentacji: prezentacja wyników uzyskanych do tego etapu projektu, omówienie problemów, kwestii technicznych, metodycznych itd.
13. Zajęcia w formule demonstracyjno-dyskusyjnej z naciskiem na zaangażowanie studentów (mikro prezentacje problemów cząstkowych, przygotowywanie schematów, (info)grafik, map myśli wraz z omówieniem): poprawa modeli, omówienie toku realizacji projektu tj. retrospekcja działań, możliwe kroki, które usprawniłyby pracę itd.
14. Zajęcia w formie demonstracyjno-dyskusyjnej: synteza wyników, tworzenie dokumentacji.
15. Zajęcia otwarte w formie prezentacji, podczas których studenci przedstawiają wyniki swojej pracy, wyniki swoich eksperymentów i wnioski.

Efekty uczenia się dla przedmiotu

Symbol efektu uczenia się dla przedmiotu	Opis efektów uczenia się	Symbole efektów uczenia się dla programu studiów	Sposób weryfikacji
	Student		
WIEDZA			
W01	Zna i potrafi poprawnie zidentyfikować i zastosować metody analizy danych.	W_06	Realizacja projektu, prezentacje projektowe, raport, aktywność na zajęciach zintegrowanych
W02	Zna i rozumie główne tendencje rozwojowe cyberbezpieczeństwa, w szczególności dotyczące analizy danych.	W_01 W_06	Realizacja projektu, prezentacje projektowe, raport, aktywność na zajęciach zintegrowanych
W03	Zna i rozumie różne modele informatyczne służące do analizy danych, w szczególności dotyczące cyberbezpieczeństwa.	W_03 W_04 W_06	Realizacja projektu, prezentacje projektowe, raport, aktywność na zajęciach zintegrowanych
W04	Zna i rozumie metody i narzędzia informatyczne służące do weryfikacji hipotez dotyczących analizy danych.	W_03 W_04 W_06	Realizacja projektu, prezentacje projektowe, raport, aktywność na zajęciach zintegrowanych
UMIEJĘTNOŚCI			
U01	Potrafi, na podstawie analizy istniejących uwarunkowań, formułować i testować hipotezy dotyczące analizowanych danych, przy wykorzystaniu właściwych narzędzi informatycznych.	U_02 U_04 U_05 U_06	Realizacja projektu, prezentacje projektowe, raport, aktywność na zajęciach zintegrowanych
U02	Potrafi używać, formułować i parametryzować modele informatyczne służące do analizy danych.	U_04 U_06	Realizacja projektu, prezentacje projektowe, raport, aktywność na zajęciach zintegrowanych
U03	Potrafi dobrać i skutecznie wykorzystać metody i narzędzia służące do weryfikacji postawionych hipotez.	U_04 U_05 U_06	Realizacja projektu, prezentacje projektowe, raport, aktywność na zajęciach zintegrowanych
U04	Potrafi planować i przeprowadzać eksperymenty i badania, w tym symulacje komputerowe, w celu weryfikacji postawionych hipotez.	U_03 U_06 U_09	Realizacja projektu, prezentacje projektowe, raport, aktywność na zajęciach zintegrowanych
U05	Potrafi poprawnie identyfikować, selekcjonować i wybierać dane z różnych źródeł, także dane w języku angielskim.	U_01 U_12	Realizacja projektu, prezentacje projektowe, raport, aktywność na zajęciach zintegrowanych
U06	Potrafi realizować zadanie projektowe w zespole, podejmować różne role w zespole.	U_13	Realizacja projektu, prezentacje projektowe
KOMPETENCJE SPOŁECZNE			
K01	Jest gotów do zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemów związanych z projektem.	K_01	Realizacja projektu, prezentacje projektowe, raport, aktywność na zajęciach zintegrowanych

Symbol efektu uczenia się dla przedmiotu	Opis efektów uczenia się	Symbole efektów uczenia się dla programu studiów	Sposób weryfikacji
	Student		
K02	Jest gotów do formułowania i przekazywania społeczeństwu, poprzez wybrane sieci społecznościowe – informacji i opinii dotyczących zagrożeń związanych z cyberbezpieczeństwa i opracowanych sposobów ich im przeciwdziałania.	K_02	Realizacja projektu, prezentacje projektowe, raport, aktywność na zajęciach zintegrowanych
K03	Jest gotów do ponoszenia odpowiedzialności za pracę całej grupy.	K_03	Raport – publikacja wyników w sieci społecznościowej

BEZPIECZEŃSTWO INTERNETU RZECZY (PBL2)

rodzaj zajęć/liczba godzin	wykład	0
	ćwiczenia	0
	laboratorium	0
	projekt	60
	zajęcia zintegrowane (warsztaty)	120
liczba punktów ECTS	12	
status przedmiotu	obowiązkowy	

Treści kształcenia

ZAJĘCIA ZINTEGROWANE - WARSZTATY

Zajęcia zintegrowane mają charakter zajęć praktycznych, prowadzonych w wymiarze 2 razy po 4 godz. w każdym tygodniu, z bogatą częścią wprowadzającą w dane zagadnienie. „Minimisja" określa przykładową aktywność, jaką studenci mogą zrealizować podczas zajęć lub/i w ramach pracy samodzielnej w danym tygodniu.

W1: Wprowadzenie do zagadnień bezpieczeństwa sieci IoT, modelowanie zagrożeń.
Specyfika systemów IoT i kwestie bezpieczeństwa, przykłady incydentów. Standardy, frameworki, protokoły, stan prawny, kierunki rozwoju. Pojęcia constrained-node, constrained-networks. Identyfikacja zagrożeń. Łączność w sieciach IoT – przewodowa i bezprzewodowa. Tablica przeznaczeń częstotliwości. Źródła informacji o urządzeniach IoT (np. FCC ID, inżynieria odwrotna). Technika Software Defined Radio – charakterystyka i rola w systemach IoT.
Minimisja: Na przykładzie specyfikacji wybranych urządzeń elektronicznych z najbliższego otoczenia – samodzielna próba identyfikacji sposobu i parametrów komunikacji (np. częstotliwość, moc, standard telekomunikacyjny).

W2: Protokoły sieciowe w IoT.
Podstawy najpopularniejszych protokołów sieciowych wykorzystywanych w sieciach IoT np. HTTP, MQTT, CoAP. Narzędzia do generowania żądań i analizy komunikacji (np. Postman, MQTT Explorer, Mosquitto, Wireshark). Biblioteki wspomagające implementację klienta/serwera np. w Pythonie. Podgląd komunikacji na poziomie pakietów TCP/IP – program Wireshark.
Minimisja: Klient/serwer w Pythonie – uruchomienie i modyfikacja przykładów. Analiza przechwyconych żądań i odpowiedzi za pomocą Wireshark dla protokołów sieci IoT.
Minimisja: Wykorzystując dostępne online odbiorniki SDR, odebrać i spróbować zidentyfikować wybrane sygnały radiowe.

W3: Podstawy komunikacji radiowej.
Fale elektromagnetyczne – właściwości propagacyjne, modele propagacji. Obliczanie bilansu łącza. Sygnał radiowy – definicja, miary jakości, cechy charakterystyczne. Podstawowe schematy modulacji analogowych i cyfrowych. Podstawowe problemy związane z przesyłaniem informacji za pomocą sygnału radiowego (np. stosunek sygnał-szum, zniekształcenia, synchronizacja, publiczność przekazu). Reprezentacja sygnału radiowego w domenie cyfrowej – sygnał kwadraturowy (IQ). Wizualizacja sygnału w dziedzinie czasu, częstotliwości, czasu-częstotliwości. Parametry widmowe sygnałów różnych standardów, identyfikacja sygnałów.
Minimisja: Zainstalować i uruchomić odbiornik SDR na własnym komputerze. Przy jego pomocy odebrać i spróbować zidentyfikować wybrane sygnały dostępne lokalnie w eterze.
Minimisja: Analiza literaturowa obecnego stanu techniki w zakresie bezpieczeństwa systemów bezprzewodowych powszechnego użytku.

W4: Podstawowe narzędzia do testów penetracyjnych w sieciach radiowych IoT
Architektura Zero-IF w systemach SDR. Przykłady dostępnych komercyjnie urządzeń odbiorczych i nadawczo-odbiorczych SDR – przegląd, wady, zalety ze szczególnym uwzględnieniem cech szczególnie ważnych dla badania bezpieczeństwa sieci IoT. Analizator widma. Oprogramowanie

do odbioru i analizy sygnałów radiowych, np. Universal Radio Hacker, GNU Radio Companion, Gqrx, SDR#, SDR Console, Audacity.
Minimisja: Odbiór sygnałów z wybranego otwartego standardu za pomocą mobilnej platformy SDR. Dyskusja nad potencjalnymi zagrożeniami wynikającymi z otwartości przekazu.

W5: Testy bezpieczeństwa w sieciach IoT.
Badanie bezpieczeństwa systemu IoT w różnych warstwach: rekonesans sieciowy (odkrywanie hostów, identyfikacja systemów operacyjnych oraz wersji narzędzi, mapowanie topologii), badanie protokołów w łączach bezprzewodowych i przewodowych, atakowanie usług/protokołów, przegląd konfiguracji hostów, testowanie aplikacji mobilnych / webowych / chmurowych, warstwa sprzętowa, rekonesans pasywny / OSINT.
Rekonesans pasywny w sieci bezprzewodowej na przykładzie nasłuchu transmisji radiowych przy użyciu odbiorników SDR oraz ogólnodostępnego oprogramowania. Źródła wiedzy o sygnałach radiowych. Ulot elektromagnetyczny, urządzenia klasy TEMPEST.
Minimisja: Wykorzystanie narzędzi do automatycznego skanowania sieci i podatności urządzeń IoT.
Minimisja: Przechwytywanie i analiza emisji ujawniającej – ulot elektromagnetyczny.

W6: Rekonesans systemu radiowego.
Zagrożenia wynikające z możliwości przechwycenia transmisji, zarejestrowania sygnału, jego analizy/dekodowania i retransmisji. Inżynieria odwrotna protokołów radiowych na przykładzie urządzeń klasy Sub-1GHz. Typowe elementy ramki radiowej (np. preambuła, payload, suma kontrolna). Systemy o stałym i zmiennym kluczu.
Minimisja: Dekodowanie sygnałów z urządzeń powszechnego użytku, np. stacje pogodowe, wodomierze, piloty zdalnego sterowania.

W7: Ingerowanie w działanie systemów radiokomunikacyjnych – nadawanie sygnałów.
Aspekty prawne. Przegląd urządzeń i podzespołów pozwalających wytwarzać sygnały radiowe: dedykowane dla określonych schematów modulacji oraz generatory przebiegów arbitralnych (określanych na podstawie próbek IQ). Odtwarzanie zarejestrowanego sygnału – atak typu replay. Modyfikacja zarejestrowanego sygnału. Ataki typu brute-force, jamming, spoofing, tampering.
Minimisja: Zaimplementować nadajnik podszywający się pod oryginalny czujnik stacji pogodowej (atak typu spoofing).
Minimisja: Przeprowadzić atak typu brute-force oraz jamming na wskazanym systemie IoT.

W8: Sieci WiFi / Bluetooth
Organizacja łączności, charakterystyka komunikacji w warstwie radiowej, techniki zabezpieczeń. Znane podatności, narzędzia i techniki ataku.
Minimisja: Przeprowadzenie ataków typu deauthentication, jamming sieci WiFi.
Minimisja: Podsłuchiwanie klawiatury / myszki bezprzewodowej.

W9: Systemy ZigBee i BLE
Organizacja łączności, charakterystyka komunikacji w warstwie radiowej, techniki zabezpieczeń. Znane podatności, narzędzia i techniki ataku.
Minimisja: Podsłuch oraz atak typu replay względem wybranego urządzenia konsumenckiego pracującego w standardzie ZigBee.
Minimisja: Analiza komunikacji BLE. Odczyt deskryptorów, autentykacja, MAC spoofing.

W10: Systemy łączności dalekiego zasięgu (np. LoRa, GPS, DCF77, publiczne emisje rozsiewcze)
Organizacja łączności, charakterystyka komunikacji w warstwie radiowej, techniki zabezpieczeń. Właściwości i propagacja fal elektromagnetycznych w różnych zakresach częstotliwości i na dużych dystansach. Modele propagacyjne. Znane podatności, narzędzia i techniki ataku.
Minimisja: przeprowadzić wybrany atak na sieć LoRa np. bitflip, replay, ack spoofing).
Minimisja: przeprowadzić atak GPS spoofing.

W11: Systemy łączności bliskiego zasięgu (np. RFID, NFC)
Organizacja łączności, charakterystyka komunikacji w warstwie radiowej, techniki zabezpieczeń. Systemy RFID aktywne i pasywne. Tagi RFID i ich zabezpieczenia. Znane podatności, narzędzia i techniki ataku.

Minimisja: Klonowanie tagów. Modyfikowanie zawartości tagów. Podsłuchiwanie transmisji pomiędzy czytnikiem a tagiem.

W12: Inżynieria odwrotna urządzeń IoT – część 1. Komunikacja i diagnostyka za pomocą interfejsów szeregowych.
Inżynieria odwrotna urządzenia IoT: inspekcja zewnętrzna, pozyskiwanie wszelkich informacji o urządzeniu z różnych źródeł, inspekcja wewnętrzna, identyfikacja roli kluczowych komponentów. FCC ID. Wyszukiwanie oraz czytanie not katalogowych komponentów elektronicznych. Komunikacja szeregowa UART – odczyt informacji diagnostycznych. Standardy RS-232 / RS-485 i sieci przemysłowe. Protokół Modbus – podgląd transmisji, sterowanie urządzeniami.
Minimisja: Inżynieria odwrotna wskazanego urządzenia IoT.
Minimisja: Komunikacja w sieci przemysłowej Modbus – nasłuch i ingerencja.

W13: Inżynieria odwrotna urządzeń IoT – część 2. Komunikacja pomiędzy podzespołami urządzenia IoT (np. SPI, I2C, 1-Wire).
Komunikacja pomiędzy komponentami składowymi urządzeń IoT – protokoły szeregowe SPI, I2C, 1-Wire itp. Podglądanie komunikacji z układami peryferyjnymi – wykorzystanie oscyloskopu, analizatora stanów logicznych itp. Pozyskiwanie listy zajętych adresów na magistrali I2C. Inżynieria odwrotna protokołu komunikacji w przypadku, gdy nota katalogowa układu nie jest dostępna. Wysyłanie własnych komend do sprzętu.
Minimisja: odczyt, modyfikacja i zapis szeregowej pamięci EEPROM przechowującej nastawy lub firmware urządzenia.
Minimisja: podgląd komunikacji szeregowej pomiędzy mikrokontrolerem a czujnikiem.

W14: Bezpieczeństwo IoT – aspekty prawne, moralne i praktyczne. Audyt bezpieczeństwa.
Regulacje prawne (w tym planowane regulacje EU) dotyczące bezpieczeństwa urządzeń i systemów IoT. Kwestia ochrony prywatności użytkowników urządzeń IoT, anonimizacja danych, ochrona danych przed podsłuchaniem, szyfrowanie. Nieoczywiste drogi do utraty/zabrania komuś elementów prywatności, np. profilowanie zachowań ludzi na podstawie pomiarów zużycia energii elektrycznej, wody itp., ulot elektromagnetyczny, kamery i analiza obrazu za pomocą sztucznej inteligencji. Wykorzystywanie publicznie dostępnych danych do nieoczywistych zastosowań, np. https://dictatoralert.org/. Dalsze kierunki rozwoju dla inżynierów bezpieczeństwa IoT, rynek pracy.
Minimisja: przygotowanie i poprowadzenie prelekcji lub dyskusji na wybrany temat dotyczący bezpieczeństwa IoT.

W15 – Rezerwa, prezentacje końcowe projektów semestralnych.
Seminarium podsumowujące zrealizowane projekty semestralne. Każdy z zespołów prezentuje przygotowane rozwiązanie techniczne oraz uzyskane wyniki z zakresu bezpieczeństwa i stabilności działania sieci. Omawiane są logi wykrytych i przeprowadzonych prób naruszeń integralności systemów. Dyskusja nad potencjalnymi podatnościami poszczególnych rozwiązań.

PROJEKT

Projekt realizowany jest w kilkuosobowych zespołach. Zajęcia związane z realizacją projektu odbywają w wymiarze 2 godz. w każdym tygodniu wspólnie dla całej grupy oraz 2 godz. w każdym tygodniu w formie konsultacji poszczególnych zespołów z opiekunami.

Projekt składa się z dwóch odrębnie ocenianych części.

Część 1 – projekt i implementacja sieci IoT
Zadaniem każdego z kilkuosobowych zespołów studenckich jest zaprojektowanie i zaimplementowanie uproszczonego modelu niskobudżetowej, możliwie bezpiecznej sieci IoT, realizującej zadania z zakresu akwizycji danych lub / i sterowania, zgodne z zarysem założeń funkcjonalnych określonym przez prowadzącego zajęcia. Istotą zadania jest zaprojektowanie własnego sposobu komunikacji bezprzewodowej wykorzystującego scalone transceiwery Sub-1GHz lub / i urządzenia SDR (wykluczone jest stosowanie fabrycznych rozwiązań oferujących wbudowane szyfrowanie, np. WiFi, BLE, LTE itp.). Zadanie obejmuje wybór schematu modulacji, projekt ramki radiowej, wybór lub projekt protokołu warstwy aplikacji, decyzje o tym, czy system jest jedno – czy dwukierunkowy

(z potwierdzeniami), wybór algorytmu szyfrowania (lub jego braku) itp. oraz implementację modelu sieci z wykorzystaniem dostępnych komponentów (np. minikomputer jednoukładowy Raspberry Pi plus dołączony interfejs bezprzewodowy, czujnik lub / i element wykonawczy). Elementem zadania jest także wyposażenie sieci w mechanizmy pozwalające zorientować się, że ktoś próbuje naruszać jej integralność (monitorowanie ruchu).
Zadanie kończy się przygotowaniem dokumentacji technicznej systemu, obejmującej m.in. specyfikację opracowanego protokołu radiowego, szczegóły implementacji, podjęte działania i zastosowane rozwiązania mające na celu podniesienie poziomu bezpieczeństwa sieci.

Część 2 – przegląd bezpieczeństwa sieci IoT
Działający model sieci dany zespół studentów przekazuje w ręce innego zespołu, w celu zweryfikowania jej bezpieczeństwa. Względem swojej sieci zespół występuje w roli Zespołu Broniącego, natomiast względem obcej sieci zespół pełni rolę Testera.
Zadaniem Testera jest przeprowadzenie przeglądu bezpieczeństwa sieci podążając za zaleceniami (np. zgodnie z wybranym frameworkiem bezpieczeństwa) przedstawionymi przez prowadzącego zajęcia. Zespół Broniący udostępnia Testerom kod źródłowy stworzonego oprogramowania (np. poprzez repozytorium), ale nie hasła czy innego rodzaju klucze autoryzujące.
Przegląd bezpieczeństwa polega zarówno na analizie kodu źródłowego jak również przeprowadzeniu prób spenetrowania sieci oraz złamania jej zabezpieczeń, w tym tych dotyczących komunikacji radiowej. Przeprowadzane próby są odnotowywane w sprawozdaniu, z uwzględnieniem typu, dokładnej daty i godziny prowadzonych działań, oraz szczegółów technicznych pozwalających na odtworzenie ataku w późniejszym terminie np. przez prowadzącego zajęcia lub Zespół Broniący w ramach zabezpieczania swojego rozwiązania. Tester przedstawia sprawozdanie z przeprowadzonych badań, wskazując na wykryte podatności analizowanego systemu.
Zadaniem Zespołu Broniącego na tym etapie jest przede wszystkim wychwycenie prób spenetrowania oraz złamania zabezpieczeń własnej sieci. Do tego celu wykorzystane powinny zostać wbudowane w sieć rozwiązania monitorujące podejrzane zachowania (np. zaimplementowane w części 1 monitorowanie ruchu). Zespół Broniący przedstawia sprawozdanie, w którym zamieszcza wiarygodne zestawienie wykrytych prób naruszenia integralności swojej sieci

Efekty uczenia się dla przedmiotu

Symbol efektu uczenia się dla przedmiotu	Opis efektów uczenia się	Symbole efektów uczenia się dla programu studiów	Sposób weryfikacji
	Student		
WIEDZA			
W01	Zna i rozumie główne kierunki rozwoju urządzeń oraz sposobów łączności w sieciach urządzeń Internetu Rzeczy.	W_01	Warsztat W1, W2, egzamin
W02	Zna i rozumie procedury bezpieczeństwa stosowane w popularnych standardach komunikacyjnych wykorzystywanych w systemach IoT.	W_02	Warsztaty W8-W11, egzamin
W03	Ma wiedzę dotyczącą metodyki prowadzenia rekonesansu w sieciach pakietowych oraz w systemach radiowych, pozwalającą na wykrywanie i analizowanie podatności systemów IoT.	W_03	Warsztat W5, W6, projekt cz. 2, egzamin
W04	Ma wiedzę dotyczącą metodyki prowadzenia prac z zakresu inżynierii wstecznej urządzeń IoT w zakresie pozyskiwania informacji o wykorzystywanych sposobach łączności pomiędzy komponentami urządzenia oraz pomiędzy urządzeniami.	W_03	Warsztaty W12, W13, egzamin
W05	zna specjalistyczne narzędzia informatyczne niezbędne do analizy ruchu w sieciach IoT przewodowych i bezprzewodowych	W_04	Warsztat W2, W4, egzamin
W06	W pogłębionym stopniu zna i rozumie zasady wymiany informacji pomiędzy urządzeniami komunikującymi się bezprzewodowo (sposób formowania sygnału radiowego, modulacji, budowy ramki itp.) dla różnych standardów telekomunikacyjnych w kontekście wyszukiwania potencjalnych luk w obszarze cyberbezpieczeństwa.	W_06	Warsztaty W3, W6-W11, egzamin
W07	W pogłębionym stopniu zna i rozumie możliwości wpływania na nadawany sygnał i działanie nadajnika radiowego i jego podstawowych podzespołów oraz wybranych techniki dostępu i modulacji, a także aspekty prawne dot. transmisji radiowej.	W_07	Warsztaty W3, W7, egzamin
W08	Zna przykłady incydentów bezpieczeństwa dotyczących systemów IoT dotyczących rozwiązań sprzętowych oraz łączności bezprzewodowej, rozumie przyczyny ich zaistnienia oraz zna metody wykrywania i zapobiegania.	W_08	Warsztat W1, egzamin
UMIEJĘTNOŚCI			
U01	Potrafi pozyskiwać informacje o działaniu urządzeń IoT na podstawie ogólnodostępnych źródeł oraz analizie układu „z natury”, dokonywać ich krytycznej oceny źródeł, wyciągać wnioski i wyczerpująco je uzasadniać.	U_01	Warsztat W1, W12

Symbol efektu uczenia się dla przedmiotu	Opis efektów uczenia się	Symbole efektów uczenia się dla programu studiów	Sposób weryfikacji
	Student		
U02	Potrafi przeprowadzić krytyczną analizę sposobu funkcjonowania istniejących standardów komunikacji w sieciach IoT z zakresu bezpieczeństwa systemów teleinformatycznych i oceniać te rozwiązania.	U_02	Warsztaty W8-W11
U03	Potrafi planować i przeprowadzać eksperymenty polegające na wygenerowaniu zasymulowanych sygnałów radiowych w celu ich wstrzyknięcia do sieci bezprzewodowej oraz potrafi interpretować uzyskane wyniki.	U_03	Warsztat W7
U04	Potrafi wykorzystać specjalistyczne oprogramowanie do analizy sygnałów radiowych w celu analizy protokołów bezprzewodowych pod kątem cyberbezpieczeństwa i analizy ich wyników.	U_04	Warsztat W4, W6
U05	Potrafi formułować i testować hipotezy odnośnie bezpieczeństwa danego systemu oraz skuteczności zabezpieczeń.	U_05	Projekt
U06	Potrafi identyfikować potencjalne wektory ataku oraz formułować wymagania dotyczące poziomu bezpieczeństwa w projektowanym lub analizowanym systemie.	U_06	Projekt
U07	Potrafi zaprojektować – zgodnie z zadaną specyfikacją – bezpieczną sieć urządzeń IoT komunikujących się ze sobą bezprzewodowo za pomocą autorskiego protokołu, a także zweryfikować poprawność projektu.	U_07	Projekt
U08	Potrafi dostrzegać aspekty dotyczące ochrony prywatności użytkowników w trakcie projektowania nowych sieci urządzeń IoT lub analizy istniejących sieci.	U_08	warsztat W14
U09	Potrafi dokonać wyboru oraz zastosować właściwe metody, techniki i narzędzia do przeprowadzenia badań bezpieczeństwa sieci urządzeń IoT.	U_09	Projekt
U10	Potrafi pracować indywidualnie oraz współdziałać z innymi osobami w ramach prac zespołowych; potrafi kierować pracą zespołu.	U_13	Projekt
U11	Potrafi określić kierunki dalszego uczenia się, zaplanować i zrealizować proces samokształcenia, a także ukierunkowywać innych w tym zakresie.	U_14	Warsztat W14
KOMPETENCJE SPOŁECZNE			
K01	Jest gotów do krytycznej oceny posiadanej wiedzy i odbieranych treści oraz do uznawania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu; jest gotów do stałego aktualizowania i wzbogacania posiadanej wiedzy.	K_01	Projekt

BEZPIECZNE SYSTEMY CYFROWE

rodzaj zajęć/liczba godzin	wykład	30
	ćwiczenia	0
	laboratorium	30
	projekt	15
	zajęcia zintegrowane (warsztaty)	0
liczba punktów ECTS	5	
status przedmiotu	obowiązkowy	

Treści kształcenia

WYKŁAD

Mikroelektroniczne systemy cyfrowe – przegląd. System zintegrowany (*System-on-Chip*): przykłady architektur, w tym układy wielordzeniowe i wieloprocesorowe. Układy rekonfigurowalne. Bloki IP. Komunikacja: magistrale, sieć zintegrowana (*Network-on-Chip*). Układy wejścia/wyjścia.
Modelowanie i synteza bloków IP. Języki opisu sprzętu (Verilog, VHDL) i synteza logiczna. Języki opisu systemu (SystemC, SystemVerilog) i synteza behawioralna: harmonogramowanie i wybór mikroarchitektury systemu. Modelowanie systemów na poziomie transakcji (TLM). Ograniczenia i możliwości syntezy behawioralnej, logicznej i syntezy topografii.
Problemy projektowania dużych systemów jednoukładowych SoC. Dystrybucja sygnałów zegarowych. Szacowanie poboru mocy dynamicznej i zarządzanie poborem mocy (bramkowanie zegara i adaptacyjne sterowanie częstotliwością taktowania itp.). Techniki minimalizacji poboru mocy statycznej, adaptacyjne sterowanie napięciem zasilania i polaryzacją podłoża itp.
Weryfikacja i testowanie. Metody weryfikacji formalnej i funkcjonalnej na różnych poziomach abstrakcji, weryfikacja wykorzystująca systemy asercji (PSL, SystemVerilog), metodyka UVM. Jakość weryfikacji a bezpieczeństwo systemu. Zarys problemów testowania i projektowania systemów łatwo testowalnych.
Bezpieczeństwo systemów VLSI. Układy funkcji fizycznie nieklonowalnych PUF i generatorów liczb prawdziwie losowych TRNG. Zabezpieczanie bloków IP. Projektowanie i weryfikacja systemów wykorzystujących zabezpieczone bloki IP. Kompromisy projektowe wynikające z konfliktów pomiędzy wymaganiami dotyczącymi funkcjonalności, bezpieczeństwa, weryfikowalności i testowalności. Zabezpieczenia układów scalonych przed atakami typu *hardware trojan, side-channel, via JTAG, microprobing* itp. Integralność procesu projektowania układu scalonego.

LABORATORIUM

Zajęcia laboratoryjne będą polegać na wykonywaniu zadań indywidualnie przydzielanych każdemu studentowi, które ilustrują główne zagadnienia poruszane na wykładzie: modelowanie systemów z wykorzystaniem języka opisu sprzętu, synteza behawioralna, synteza logiczna, weryfikacja formalna i funkcjonalna.

PROJEKT

W ramach zajęć projektowych wykonywane są zadania wyrabiające umiejętności implementacji systemów, na podstawie wiedzy uzyskanej na wykładach. W ramach pracy zespołowej studenci wykonują projekt prostego systemu cyfrowego. Tematy projektów będą nawiązywać do przykładowych praktycznych zastosowań.

Efekty uczenia się dla przedmiotu

Symbol efektu uczenia się dla przedmiotu	Opis efektów uczenia się	Symbole efektów uczenia się dla programu studiów	Sposób weryfikacji
	Student		
WIEDZA			
W01	Zna metody projektowania bloków cyfrowych IP i systemów jednoukładowych wykorzystujące narzędzia syntezy behawioralnej, syntezy logicznej i syntezy topografii.	W_03 W_08	Egzamin, laboratorium, projekt
W02	Zna techniki weryfikacji cyfrowych bloków IP i systemów jednoukładowych wykorzystujące metody formalne oraz metodykę UVM.	W_03 W_08 W_12	Egzamin, laboratorium, projekt
W03	Zna metody zabezpieczania bloków IP i systemów jednoukładowych przed atakami.	W_03 W_07 W_08 W_12	Egzamin, laboratorium, projekt
UMIEJĘTNOŚCI			
U01	Potrafi formułować i analizować specyfikacje projektu oraz przeprowadzić weryfikację zrealizowanego projektu.	U_01 U_03 U_04	Laboratorium, projekt
U02	Potrafi zaprojektować specjalizowany cyfrowy układ scalonych z wykorzystaniem narzędzi do syntezy behawioralnej, syntezy logicznej i syntezy topografii.	U_03 U_04 U_07	Laboratorium, projekt
U03	Potrafi wykorzystać technikę układów funkcji fizycznie nieklonowalnych PUF.	U_07 U_09	Laboratorium, projekt
U04	Potrafi zrealizować sprzętowy generator liczb prawdziwie losowych.	U_07 U_09	Laboratorium, projekt
U05	Potrafi samodzielnie rozwiązywać problemy projektowe oraz pracować w zespole.	U_13	Laboratorium, projekt
KOMPETENCJE SPOŁECZNE			
K01	Umie współpracować w grupie.	K_03	Projekt zespołowy

BEZPIECZEŃSTWO SIECI 5G I 6G

rodzaj zajęć/liczba godzin	wykład	30
	ćwiczenia	0
	laboratorium	0
	projekt	15
	zajęcia zintegrowane (warsztaty)	0
liczba punktów ECTS	4	
status przedmiotu	obowiązkowy	

Treści kształcenia

WYKŁAD

1. Wprowadzenie.
Wprowadzenie do przedmiotu. Omówienie zasad zaliczania przedmiotu i zakresu projektu. Omówienie zagadnień bezpieczeństwa sieciowego i klas typowych ataków sieciowych. Rekomendacje dotyczące bezpieczeństwa sieci (m.in. ITU-T, NGMN).
2. Omówienie sieci 2G, 3G i 4G oraz ich mechanizmów bezpieczeństwa.
Zwięzłe wprowadzenie do sieci 2G, 3G, 4G omówienie i rola usług oferowanych przez omawiane sieci, omówienie ewolucji mechanizmów bezpieczeństwa w ww. sieciach.
3. Architektura sieci 5G .
Omówienie architektury sieci 5G (wersje Non-Stand-Alone i Stand-Alone) oraz podsystemu radiowego NR. Łącze radiowe w systemach 5G. Protokoły w łączu radiowym. Wykorzystanie techniki network slicing do tworzenia wirtualnych sieci usługowych (programowanie płaszczyzny sterowania).
4. Architektura bezpieczeństwa sieci 5G.
Zwięzłe wprowadzenie do omawianych rozwiązań sieciowych, omówienie i rola usług oferowanych przez omawiane systemy. Podkreślenie roli bezpieczeństwa omawianych systemów.
5. Bezpieczeństwo łącza radiowego.
Omówienie aspektów bezpieczeństwa łącza radiowego oraz podsystemu radiowego NR. Uwierzytelnianie. Szyfrowanie i kontrola integralności. Numery tymczasowe stacji ruchomych. Generacja i dystrybucja kluczy kryptograficznych. Odporność łącza radiowego na zakłócenia i zagłuszanie.
6. Bezpieczeństwo wirtualizacji.
Sieci 5G i 6G budowane są/będą z wykorzystaniem technik wirtualizacyjnych w rozproszonym środowisku chmurowym. W ramach wykładu zostaną omówione aspekty bezpieczeństwo rozwiązań ETSI NFV (MANO) i Kubernetes w przypadku sieci 5G i 6G.
7. Usługi i architektura sieci 6G.
W ramach wykładu przedstawione zostaną wymagania, usługi i szkic architektury sieci 6G (architektura docelowa spodziewana jest w roku 2030).
8. Mechanizmy bezpieczeństwa sieci 6G .
W ramach wykładu przedstawione zostaną mechanizmy bezpieczeństwa (uwierzytelniania, szyfrowania, integralności danych) oraz wiarygodności wymiany danych w środowisku wielooperatorskim (np. Gaia-X) wymagania, usługi i szkic architektury bezpieczeństwa sieci 6G (architektura docelowa spodziewana jest w roku 2030).

PROJEKT

W ramach projektu 2-3 osobowe zespoły będą odpowiedzialne za rozwiązanie wybranego problemu z zakresu tematyki wykładów. Projekt zakończy się raportem oraz prezentacją wyników prac. Każda grupa projektowa dostanie inny temat projektu.

Efekty uczenia się dla przedmiotu

Symbol efektu uczenia się dla przedmiotu	Opis efektów uczenia się	Symbole efektów uczenia się dla programu studiów	Sposób weryfikacji
	Student		
WIEDZA			
W01	Zna i rozumie główne tendencje rozwojowe sieci komunikacji ruchomej.	W_01	Kolokwium, egzamin
W02	Ma wiedzę dotyczącą zagrożeń bezpieczeństwa sieci 5G i 6G.	W_02	Kolokwium, egzamin
W03	Ma wiedzę dotyczącą architektury bezpieczeństwa sieci 5G i 6G.	W_08	Kolokwium, egzamin
W04	Ma wiedzę dotyczącą bezpieczeństwa techniki network slicing i wirtualizacji.	W_08 W_09	Kolokwium, egzamin
W05	Ma wiedzę z zakresu przetwarzania danych osobowych w sieciach 5G i 6G.	W_10 W_11	Kolokwium, egzamin
UMIEJĘTNOŚCI			
U01	Potrafi planować i przeprowadzać symulacje komputerowe dotyczące bezpieczeństwa sieci komunikacji ruchomej.	U_03	Symulacje/ implementacje mechanizmów bezpieczeństwa zrealizowane w ramach projektu
U02	Potrafi skonfigurować i zoptymalizować podstawowe mechanizmy bezpieczeństwa w sieciach 5G.	U_07 U_08	Symulacje/ implementacje mechanizmów bezpieczeństwa zrealizowane w ramach projektu
KOMPETENCJE SPOŁECZNE			
K01	Ma świadomość konieczności komunikowania się z podmiotami ekosystemu 5G w calu zapewnienia jego pełnego bezpieczeństwa.	K_03	Projekt, egzamin
K02	Jest świadomy konieczności ciągłej aktualizacji wiedzy o sieciach komunikacji ruchomej w związku z pojawianiem się ich nowych generacji.	K_01	Projekt, egzamin

POZATECHNICZNE ASPEKTY CYBERBEZPIECZEŃSTWA

przedmiot prowadzony w języku angielskim:
NON-TECHNICAL DIMENSIONS OF CYBERSECURITY

rodzaj zajęć/liczba godzin	wykład	30
	ćwiczenia	0
	laboratorium	0
	projekt	30
	zajęcia zintegrowane (warsztaty)	0
liczba punktów ECTS	4	
status przedmiotu	obowiązkowy	

Treści kształcenia

WYKŁAD

1. Wprowadzenie do pozatechnicznych aspektów cyberbezpieczeństwa.
Rola jednostki w systemie cyberbezpieczeństwa. Człowiek jako element struktury bezpieczeństwa: poziom prywatny, korporacyjny, instytucjonalny, państwowy i międzynarodowy. Prezentacja podstawowych pojęć i podejść z zakresu kryminologii, kryminalistyki, wiktymologii, socjologii i psychologii i ich konfrontacja z technicznymi aspektami cyberbezpieczeństwa.
2. Czynnik ludzki w cyberbezpieczeństwie.
Socjologia i psychologia atakujących i ofiar. Cyberprzestępcy jako jednostki patologiczne. Motywacja cyberprzestępców. Człowiek jako narzędzie i wektor ataku. Aspekty wiktymologiczne: analiza podatności na stanie się ofiarą przestępstwa a strategie zapobiegawcze i ochronne.
3. Inżynieria społeczna a cyberbezpieczeństwo.
Manipulacja psychologiczna ludźmi w celu wykonania określonych działań lub ujawnienia poufnych informacji. Techniki manipulacji. Podatność na szantaż i manipulację. Cyber insiders – świadome i nieświadome narażanie organizacji na ryzyko.
4. Taktyka ataków wykorzystujących elementy społeczne.
Taktyki społeczne wykorzystujące podstęp, manipulację, zastraszanie itp. wW celu wykorzystania czynnika ludzkiego w pozyskiwaniu informacji i realizacji ataków. Phishing, vishing, baiting, pretexting, przekupstwo.
5. Źródła informacji wywiadowczych i metody ich pozyskiwania.
Wywiad i kontrwywiad – poziom taktyczny, operacyjny i strategiczny. Klasyfikacja typów informacji wywiadowczych. Źródła informacji wywiadowczych. HumInt, SigInt, TechInt, MasInt, GarbInt. Wprowadzenie do OSInt/SocMint.
6. Biały wywiad i otwarte źródła informacji.
Wartość OSInt. Źródła Osint. Problemy z wykorzystaniem OSInt. Analiza powiązań, relacji i tożsamości. Analiza przestrzenna i czasowa. Filtrowanie Osint. Agregacja i analiza live. Biały wywiad w wojskowości, organach ścigania, zastosowaniach cywilnych, biznesowych, prywatnych i przestępczych.
7. Bezpieczeństwo operacyjne.
Projektowanie i wdrażanie strategii bezpieczeństwa operacyjnego (OpSec) na poziomie indywidualnym i organizacyjnym, korporacyjnym i instytucjonalnym. Zarządzanie informacjami wrażliwymi i prywatnymi.
8. Aspekty biznesowe cyberbezpieczeństwa.
Skutki ekonomiczne ataków. Analiza ryzyka. Zarządzanie ryzykiem. Wykrywanie i przeciwdziałanie nieuczciwej konkurencji. Zastosowanie metod wywiadowczych i kontrwywiadowczych (business intelligence).
9. Wojna informacyjna i konflikt hybrydowy.
Charakterystyka konfliktu asymetrycznego, wojny hybrydowej i wojny informacyjnej. Rola i znaczenie technik dezinformacyjnych, typowania i lokowania agentury wpływu, tworzenie i sterowanie bańkami informacyjnymi w sieciach społecznościowych. Propagacja teorii spiskowych. Analiza przypadków.
10. Infodemia: dezinformacja, misinformacja i malinformacja.

Przedstawienie aparatu pojęciowego. Zarządzanie infodemią. Zagrożenia dla zdrowia publicznego, infrastruktury krytycznej, bezpieczeństwa systemów władzy, stabilności wyborów. Problem dezinformacji, a ochrona dobrego imienia osób, firm i instytucji.

11. Przestępstwa przyszłości.

Znaczenie interdyscyplinarnego i intersektorowego planowania strategii bezpieczeństwa w związku z pojawianiem się, rosnącą dostępnością i malejącymi kosztami nowoczesnych technologii informacyjnych

12. Sztuczna inteligencja i uczenie maszynowe, a cyberbezpieczeństwo.

Technologie AI i ML jako miecz obosieczny. Wywieranie wpływu na opinie, nastroje społeczne i decyzje. Deep fake, realistyczna impersonacja audio i video – wyzwania dla prewencji kryminalnej.

LECTURES

1. Introduction to non-technical dimensions of cyber security.

The role of an individual in cybersecurity system. A person as an element of security structure at the private, corporate, institutional, state and international levels. Presentation of basic concepts and methodologies of the fields of criminology, forensics, victimology, sociology and psychology and their confrontation with technical aspects of cyber security.

2. Human considerations in cybersecurity.

Sociology and psychology of attackers and their victims. Cyber criminals as pathological individuals. Motivation of cyber criminals. Man as a tool and vector of attack. Victimological aspects: analysis of vulnerability to becoming a victim of crime. Prevention and protection strategies.

3. Social engineering and cybersecurity.

Psychological manipulation of people to perform certain actions or disclose confidential information. Techniques of manipulation. Vulnerability to blackmail and manipulation. Cyber insiders – knowingly or unknowingly putting organizations at risk.

4. Tactics for the attacks that use social elements.

Social tactics that use deception, manipulation, intimidation, etc. To leverage the human element in acquiring information and executing attacks. Phishing, vishing, baiting, pretexting, bribery.

5. Sources of intelligence information and methods of Intel acquisition.

Intelligence and counterintelligence – tactical, operational and strategic levels. Classification and types of intelligence information. Sources of intelligence information. HumInt, SigInt, TechInt, MasInt, GarbInt. Introduction to OSInt/SocMint.

6. Open Source Intelligence and Social Media Intelligence

The value of OSInt. Osint sources. Problems associated with using OSInt. Link analysis. Analysis of relationships. Identity analysis. Spatial analysis. Temporal analysis. Osint filtering. Live aggregation and analysis. Open Source Intelligence in military, law enforcement, civilian, business, private and criminal applications.

7. Operational Security.

Design and implementation of operational security (OpSec) strategies at individual and organizational, corporate and institutional levels. Management of sensitive and private information.

8. Business dimensions of cybersecurity.

Economic impact of cyberattacks. Risk analysis. Risk management. Detection and prevention of unfair competition. Application of intelligence and counterintelligence methods (business intelligence).

9. Information warfare and hybrid conflict.

Characteristics of asymmetric conflict, hybrid warfare and information war. The role and importance of disinformation techniques, selection, grooming and placement of agents of influence, creation and control of information bubbles in social networks. Propagation of conspiracy theories. Case study analysis.

10. Infodemics: disinformation, misinformation and malinformation.

Presentation of the conceptual framework. Managing infodemics. Threats to public health, critical infrastructure, security of government systems, stability of elections. Problem of disinformation and the protection of public image of persons, companies and institutions.

11. Future Crimes.

The importance of interdisciplinary and intersectoral planning of security strategies in connection with the emergence, gincreasing availability and decreasing costs of modern information technologies.

12. Artificial Intelligence, Machine Learning, and Cybersecurity.

AI and ML technologies as a double-edged sword. Influencing opinions, public sentiment and decisions. Deep fakes, realistic audio and video impersonation – challenges for crime prevention.

PROJEKT

W ramach Projektu studenci pracować będą w podgrupach (zespołach 3-4 – osobowych) nad konkretnymi problemami (strategie cyberbezpieczeństwa w organizacji, human-centric cybersecurity, bezpieczeństwo operacyjne, strategie kontr-dezinformacyjne itp.). Część projektowa zarówno w formie pracy własnej, jak i stacjonarnie (warsztaty, symulacje). Podsumowaniem części projektowej będzie Raport przygotowany przez podgrupę (zespół). Przewidywane jest okazjonalny gościnny udział (wideokonferencje) ekspertów zagranicznych – praktyków (organy ścigania, służby specjalne). Istotnym elementem Projektu, wzmacniającym wiedzę, umiejętności i kompetencje będą indywidualne i grupowe konsultacje projektowe pozwalające na prowadzenie dyskusji i konfrontację własnych przekonań i poglądów z odmiennymi perspektywami i punktami widzenia.

PROJECT

Within the Project part, the students will work in subgroups (teams of 3-4 students) focused on specific problems (cyber security strategies in the organization, human-centric cybersecurity, operational security, counter-disinformation strategies, etc.). Project part both in the form of own work and on-site (workshops, simulations). The conclusion of the project part will be a Report prepared by the subgroup (team). Occasional guest participation (videoconferences) of foreign experts – practitioners (law enforcement agencies, intelligence services) is planned. An important element of the Project, strengthening knowledge, skills and competencies will be the individual and group project consultations allowing for discussion and confrontation of own beliefs and opinions with different perspectives and points of view.

Efekty uczenia się dla przedmiotu

Symbol efektu uczenia się dla przedmiotu	Opis efektów uczenia się	Symbole efektów uczenia się dla programu studiów	Sposób weryfikacji
	Student		
WIEDZA			
W01	Posiada – w pogłębionym stopniu – informacje o pozatechnicznych aspektach cyberbezpieczeństwa.	W_01 W_09 W_10 W_11	Raport z projektu; końcowy esej (praca pisemna); dyskusje podczas konsultacji projektowych
W02	Posiada informacje na temat inżynierii społecznej, technik manipulacji i metod wywierania wpływu.	W_10 W_11	Raport z projektu; końcowy esej (praca pisemna); dyskusje podczas konsultacji projektowych
W03	Ma świadomość problemów związanych z uwarunkowaniami psychologicznymi i socjologicznymi w kontekście planowania strategii cyberbezpieczeństwa.	W_10 W_11	Raport z projektu; końcowy esej (praca pisemna); dyskusje podczas konsultacji projektowych
UMIEJĘTNOŚCI			
U01	Umie ocenić możliwości i ograniczenia związane z wykorzystaniem metod wywiadowczych i kontrwywiadowczych.	U_01 U_02	Raport z projektu; końcowy esej (praca pisemna); dyskusje podczas konsultacji projektowych
U02	Potrafi zaplanować strategie zarządzania bezpieczeństwem operacyjnym na poziomie prywatnym, korporacyjnym i instytucjonalnym.	U_08 U_10 U_11 U_13	Raport z projektu; końcowy esej (praca pisemna); dyskusje podczas konsultacji projektowych; ocena podziału pracy, nakładu pracy i indywidualnego zaangażowania w ramach zadań grupowych (projekt)

Symbol efektu uczenia się dla przedmiotu	Opis efektów uczenia się	Symbole efektów uczenia się dla programu studiów	Sposób weryfikacji
	Student		
U03	Posiada podstawowe umiejętności wykrywania przejawów dezinformacji i misinformacji, oraz umie projektować strategie zapobiegawcze i kontrnarracje.	U_08 U_10 U_11 U_13	Raport z projektu; końcowy esej (praca pisemna); dyskusje podczas konsultacji projektowych; ocena podziału pracy, nakładu pracy i indywidualnego zaangażowania w ramach zadań grupowych (projekt)
U04	Ma świadomość znaczenia krytycznej analizy informacji i potrafi ją przeprowadzić.	U_01 U_02	Raport z projektu; końcowy esej (praca pisemna); dyskusje podczas konsultacji projektowych
U05	Potrafi posługiwać się językiem angielskim na poziomie przynajmniej B2+, aktywnie uczestnicząc w zajęciach prowadzonych w języku angielskim, opracowując zadania pisemne w tym języku i zapoznając się z obcojęzyczną literaturą i materiałami dostarczanymi przez prowadzącego.	U_12	Stała weryfikacja kompetencji językowych podczas zajęć (wykładowy język angielski, dyskusje w języku angielskim), ocena raportu z projektu i końcowego eseju (pracy pisemnej) opracowanych w języku angielskim
KOMPETENCJE SPOŁECZNE			
K01	Potrafi skutecznie współpracować z ekspertami zewnętrznymi i odbiorcami końcowymi rozwiązań, również spoza swojej macierzystej dyscypliny.	K_01 K_02	Raport z projektu; końcowy esej (praca pisemna); ocena podziału pracy, nakładu pracy i indywidualnego zaangażowania w ramach zadań grupowych (projekt)

Symbol efektu uczenia się dla przedmiotu	Opis efektów uczenia się	Symbole efektów uczenia się dla programu studiów	Sposób weryfikacji
	Student		
K02	Umie w klarowny sposób prezentować i popularyzować rozwiązania i strategie cyberbezpieczeństwa odbiorcom nietechnicznym.	K_03	Raport z projektu; końcowy esej (praca pisemna); ocena podziału pracy, nakładu pracy i indywidualnego zaangażowania w ramach zadań grupowych (projekt)
K03	Potrafi planować rozwój swoich kompetencji zawodowych, oraz przewidywać i rozwijać nowe trendy z zakresu cyberbezpieczeństwa, biorąc pod uwagę ich aspekty społeczne.	K_03 K_04	Raport z projektu; końcowy esej (praca pisemna); ocena podziału pracy, nakładu pracy i indywidualnego zaangażowania w ramach zadań grupowych (projekt)

METODOLOGICZNE I ETYCZNE PROBLEMY BADAŃ TECHNONAUKOWYCH

Przedmiot prowadzony w języku angielskim
METHODOLOGICAL AND ETHICAL ISSUES OF TECHNOSCIENTIFIC RESEARCH

rodzaj zajęć/liczba godzin	wykład	20
	ćwiczenia	10
	laboratorium	0
	projekt	0
	zajęcia zintegrowane (warsztaty)	0
liczba punktów ECTS	2	
status przedmiotu	obowiązkowy	

Treści kształcenia

WYKŁAD

1. Podstawowe pojęcia związane z metodologią badań naukowych (2 h):
   – nauka i dyscypliny naukowe,
   – informacja i wiedza naukowa.
2. Modelowanie matematyczne i pomiar (3 h):
   – zasady modelowania matematycznego,
   – identyfikacja modeli matematycznych,
   – matematyczny metamodel pomiaru.
3. Metoda naukowa i proces badawczy (3 h):
   – pojęcia podstawowe,
   – naiwna interpretacja metody naukowej i krytyka tej interpretacji,
   – kontekst odkrycia i kontekst uzasadnienia,
   – niepewność wiedzy naukowej.
4. Elementy metaetyki i etyki ogólnej (2 h):
   – podstawowe pojęcia etyki i metaetyki,
   – etyka a inne obszary aktywności intelektualnej.
5. Etyczne aspekty eksperymentowania (2 h):
   – formułowanie problemu badawczego,
   – planowanie i przeprowadzanie eksperymentów,
   – zbieranie i obróbka danych eksperymentalnych.
6. Etyczne aspekty procesów informacyjnych w badaniach naukowych (2 h):
   – prowadzenie dyskusji technonaukowej,
   – ochrona własności intelektualnej,
   – recenzowanie prac naukowych,
   – wnioskowanie o środki na badania.
7. Etyczne aspekty użytkowania nowych technik (2 h):
   – zarys problematyki etycznej związanej z technikami,
   – problemy etyczne związane z cyberbezpieczeństwem, sztuczną inteligencją i robotyką.
8. Sprawdziany (4 h):

– Sprawdzian #1 i Sprawdzian #1 dotyczące pierwszej połowy wykładu,
–Sprawdzian #2 i Sprawdzian #2 dotyczące drugiej połowy wykładu.

ĆWICZENIA

- Sztuka dyskursu metanaukowego (2h),
- Nowoczesne ujęcia metodologii badań technonaukowych (2h),
- Metodologiczne problemy związane z uzasadnieniem naukowym (2h),
- Dylematy etyczne związane z obróbką danych i publikowaniem wyników badań (2h),
- Dylematy etyczne związane z nowymi technikami (2h).

LECTURES

1. Basic concepts of research methodology (2 h):
   – science and sciences,
   – scientific information and scientific knowledge.
2. Mathematical modelling and measurement (3 h):
   – principles of mathematical modelling,
   – identification of mathematical models,
   – mathematical meta-model of measurement.
3. Scientific method and research process (3 h):
   – basic concepts and approaches,
   – naïve understanding of scientific method and its critics,
   – context of discovery and context of justification,
   – uncertainty of scientific knowledge.
4. Elements of meta-ethics and general ethics (2 h):
   – basic concepts of ethics and meta-ethics,
   – relation of ethics to other forms of intellectual activity.
5. Ethical aspects of key research operations (2 h):
   – formulation of a research problem,
   – design and execution of experiments,
   – acquisition and processing of experimental data.
6. Ethical aspects of research-related information processes (2 h):
   – technoscientific discussion,
   – protection of intellectual property,
   – reviewing process,
   – research grant application.
7. Ethical aspects of new technologies (2 h):
   – basic approaches of ethical problems related to new technologies,
   – ethical issues related to cybersecurity, AI and robotics.
8. Tests (4 h):
   – Class Test #1 and Class Test #1' cover the first half of the contents of lectures.
   – Class Test #2 and Class Test #2' cover the second half of the contents of lectures.

TUTORIALS

- Art and science of meta-scientific discourse (2h),
- Modern approaches to research methodology (2h),
- Methodological issues related to scientific justification (2h),
- Ethical dilemmas related to data processing and publication (2h),
- Ethical dilemmas related to new technologies (2h).

Efekty uczenia się dla przedmiotu

Symbol efektu uczenia się dla przedmiotu	Opis efektów uczenia się	Symbole efektów uczenia się dla programu studiów	Sposób weryfikacji
	Student		
WIEDZA			
W01	Ma podstawową wiedzę dotyczącą: – podstawowych pojęć metodologii badań, – modelowania matematycznego i pomiaru, – metody naukowej i procesu badawczego.	W_03 W_05	Sprawdzian #1, Sprawdzian #1
W02	Ma podstawową wiedzę dotyczącą: – podstawowych pojęć etyki i metaetyki, – etycznych aspektów pracy inżyniera, – etycznych aspektów procesów informacyjnych związanych z działalnością badawczo-rozwojową, – etycznych aspektów ochrony własności intelektualnej, – etycznych aspektów wykorzystywania technik informacyjnych w działalności badawczo-rozwojowej.	W_10 W_11 W_12	Sprawdzian #2, Sprawdzian #2
UMIEJĘTNOŚCI			
U01	Potrafi: – identyfikować i krytycznie analizować problemy metodologiczne i etyczne związane z działalnością badawczo-rozwojową, – podchodzić metodycznie do dylematów etycznych związanych z działalnością badawczo-rozwojową, – omawiać problemy etyczne związane z działalnością badawczo-rozwojową i bronić własnej postawy etycznej.	U_01 U_08 U_11 U_12	Weryfikacja podczas animacji dyskusji i udziału w dyskusjach animowanych przez innych studentów
U02	Potrafi porozumiewać się w języku angielskim, w szczególności na temat metodologicznych i etycznych problemów badań technonaukowych.	U_12	Weryfikacja na sprawdzianach a także podczas animacji dyskusji i udziału w dyskusjach animowanych przez innych studentów
KOMPETENCJE SPOŁECZNE			

Symbol efektu uczenia się dla przedmiotu	Opis efektów uczenia się	Symbole efektów uczenia się dla programu studiów	Sposób weryfikacji
	Student		
K01	Jest: – bardziej wrażliwy na wartości moralne związane z działalnością badawczo-rozwojową, – lepiej przygotowany do podejmowania odpowiedzialności za działalność badawczo-rozwojową, – lepiej przygotowany do rozwiązywania dylematów etycznych pojawiających się w praktyce badawczo-rozwojowej, – bieglejszy w kształtowaniu indywidualnej postawy etycznej w odniesieniu do działalności badawczo-rozwojowej, – bardziej skłonny do systematycznej refleksji nad etycznymi aspektami życia codziennego.	K_01 K_03 K_04	Weryfikacja podczas animacji dyskusji i udziału w dyskusjach animowanych przez innych studentów

SEMINARIUM DYPLOMOWE

rodzaj zajęć/liczba godzin	wykład	0
	ćwiczenia	30
	laboratorium	0
	projekt	0
	zajęcia zintegrowane (warsztaty)	0
liczba punktów ECTS	2	
status przedmiotu	obowiązkowy	

Treści kształcenia

Tematyka zajęć prowadzonych w formie seminaryjnej obejmuje szerokie spektrum zagadnień dotyczących cyberbezpieczeństwa, związanych z tematyką prac dyplomowych aktualnie realizowanych przez studentów.

Oprócz przedstawienia prezentacji związanej z tematyką pracy dyplomowej student musi:
- poprowadzić dyskusję na temat prezentacji przedstawionej przez innego studenta,
- przygotować tekst mający charakter komunikatu naukowego dotyczący zagadnienia będącego przedmiotem pracy dyplomowej.

Efekty uczenia się dla przedmiotu

Symbol efektu uczenia się dla przedmiotu	Opis efektów uczenia się	Symbole efektów uczenia się dla programu studiów	Sposób weryfikacji
	Student		
WIEDZA			
-	-	-	-
UMIEJĘTNOŚCI			
U01	Potrafi przygotować i przedstawić prezentację ustną dotyczącą zagadnień z zakresu cyberbezpieczeństwa.	U_10	Prezentacja
U02	Potrafi przygotować tekst o charakterze naukowym dotyczący zagadnień z zakresu cyberbezpieczeństwa.	U_11	Komunikat naukowy
U03	Potrafi komunikować się na tematy zawodowe; potrafi prowadzić dyskusję.	U_11	Udział w dyskusji, prowadzenie dyskusji
KOMPETENCJE SPOŁECZNE			
K01	Jest gotów do krytycznej oceny odbieranych treści.	K_01	Udział w dyskusji, prowadzenie dyskusji
K02	Jest gotów do stałego aktualizowania i wzbogacania posiadanej wiedzy.	K_01	Udział w dyskusji
K03	Jest gotów do formułowania i przekazywania informacji związanych z cyberbezpieczeństwem; podejmuje starania, aby przekazać takie informacje w sposób zrozumiały.	K_02	Prezentacja, udział w dyskusji

CYKL RZEDMIOTÓW ZWIĄZANYCH Z PROWADZENIEM BADAŃ I PRZYGOTOWANIEM PRACY DYPLOMOWEJ

- **PRACOWNIA PROBLEMOWA,**
- **PRACOWNIA DYPLOMOWA,**
- **PRZYGOTOWANIE PRACY DYPLOMOWEJ,**
- **REDAKCJA I EDYCJA PRACY DYPLOMOWEJ.**

rodzaj zajęć/liczba godzin	zajęcia prowadzone indywidualnie, nieuwidocznione w planie studiów	0
liczba punktów ECTS	PRACOWNIA PROBLEMOWA	2
	PRACOWNIA DYPLOMOWA	6
	PRZYGOTOWANIE PRACY DYPLOMOWEJ	20
	REDAKCJA I EDYCJA PRACY DYPLOMOWEJ	0
status przedmiotu	obowiązkowy	

Treści kształcenia.

Zajęcia realizowane indywidualnie pod opieką promotora pracy dyplomowej obejmują wybrane aspekty spośród szerokiego spektrum zagadnień dotyczących cyberbezpieczeństwa, związane z tematyką pracy dyplomowej realizowanej przez studenta.

Zajęcia – oprócz pracy realizowanej przez studenta poza Uczelnią – obejmują:
- konsultacje z promotorem pracy dyplomowej i innymi nauczycielami akademickimi,
- badania prowadzone na Uczelni z wykorzystaniem specjalistycznej aparatury lub oprogramowania, realizowane pod nadzorem promotora lub innej osoby upoważnionej do prowadzenia tego typu zajęć.

Efekty uczenia się dla przedmiotu

Symbol efektu uczenia się dla przedmiotu	Opis efektów uczenia się	Symbole efektów uczenia się dla programu studiów	Sposób weryfikacji
	Student		
WIEDZA			
W01	W pogłębionym stopniu zna i rozumie wybrane fakty, teorie i metody, stanowiące zaawansowaną wiedzę z zakresu wybranych aspektów cyberbezpieczeństwa związanych z tematyką pracy dyplomowej.	W_08	Sprawozdania z pracowni, praca dyplomowa
UMIEJĘTNOŚCI			
U01	Potrafi pozyskiwać informacje z właściwie dobranych źródeł, dokonywać ich krytycznej oceny, analizy, syntezy i twórczej interpretacji, wyciągać wnioski i wyczerpująco je uzasadniać.	U_01	Konsultacje z promotorem, sprawozdania z pracowni, praca dyplomowa
U02	Potrafi planować i przeprowadzać eksperymenty/badania dotyczące bezpieczeństwa systemów teleinformatycznych oraz interpretować uzyskane wyniki.	U_03	Konsultacje z promotorem, sprawozdania z pracowni, praca dyplomowa
U03	Potrafi formułować i testować hipotezy związane z prostymi problemami badawczymi dotyczącymi m.in. zapewnienia bezpieczeństwa systemów teleinformatycznych.	U_05	Sprawozdania z pracowni, praca dyplomowa

Symbol efektu uczenia się dla przedmiotu	Opis efektów uczenia się	Symbole efektów uczenia się dla programu studiów	Sposób weryfikacji
	Student		
U04	Potrafi sformułować specyfikację złożonego zadania dotyczącego cyberbezpieczeństwa.	U_06	Konsultacje z promotorem, sprawozdania z pracowni, praca dyplomowa
U05	Potrafi zaprojektować – zgodnie z zadaną specyfikacją, używając właściwie dobranych metod i narzędzi – rozwiązanie zawierające elementy innowacyjności, związane z zapewnieniem bezpieczeństwa systemów teleinformatycznych, a także zweryfikować jego poprawność.	U_06	Praca dyplomowa, obrona pracy dyplomowej podczas egzaminu dyplomowego
U06	Potrafi – w pracy badawczej oraz przy rozwiązywaniu zadania dotyczącego zapewnienia bezpieczeństwa systemów teleinformatycznych – zastosować właściwie wybrane metody (analityczne, symulacyjne lub eksperymentalne), techniki i narzędzia oraz, jeśli zachodzi taka potrzeba, odpowiednio przystosować istniejące lub opracować nowe metody i narzędzia.	U_09	Konsultacje z promotorem, sprawozdania z pracowni, praca dyplomowa, obrona pracy dyplomowej podczas egzaminu dyplomowego
U07	Potrafi przygotować opracowanie i przedstawić prezentację ustną, dotyczącą zagadnień z zakresu cyberbezpieczeństwa.	U_13	Sprawozdania z pracowni, praca dyplomowa, obrona pracy dyplomowej podczas egzaminu dyplomowego
U08	Potrafi zaplanować i zrealizować proces samokształcenia.	U_14	Praca dyplomowa
KOMPETENCJE SPOŁECZNE			
K01	Jest gotów do krytycznej oceny posiadanej wiedzy i odbieranych treści oraz do uznawania znaczenia wiedzy w rozwiązywaniu problemów oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu; jest gotów do stałego aktualizowania i wzbogacania posiadanej wiedzy.	K_01	Konsultacje z promotorem i innymi nauczycielami akademickimi, praca dyplomowa, obrona pracy dyplomowej podczas egzaminu dyplomowego