Załącznik nr 9
do Zarządzenia Rektora PŚk Nr 35/19
w brzmieniu ustalonym Zarządzeniem Nr 12/22

KARTA PRZEDMIOTU

Kod przedmiotu	studia stacjonarne:	E-ID2C-16-s2, E-ID2C-16-s3
	studia niestacjonarne:	E-2IZ2C-1020-s3
Nazwa przedmiotu	**Uczenie maszynowe w bezpieczeństwie**	
Nazwa przedmiotu w języku angielskim	**Machine Learning in Cybersecurity**	
Obowiązuje od roku akademickiego	**2022/23**	

USYTUOWANIE PRZEDMIOTU W SYSTEMIE STUDIÓW

Kierunek studiów	**Informatyka**
Poziom kształcenia	**II stopień**
Profil studiów	**Ogólnoakademicki**
Forma i tryb prowadzenia studiów	**Studia stacjonarne i niestacjonarne**
Zakres	**Cyberbezpieczeństwo**
Jednostka prowadząca przedmiot	**Katedra Urządzeń Elektrycznych i Automatyki**
Koordynator przedmiotu	**Dr inż. Michał Łaskawski**
Zatwierdził	**Dziekan Wydziału Elektrotechniki, Automatyki i Informatyki dr hab. inż. Roman Deniziak, prof. PŚk**

OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

Przynależność do grupy/bloku przedmiotów		**Przedmiot specjalnościowy**
Status przedmiotu		**Wybieralny**
Język prowadzenia zajęć		**Polski**
Usytuowanie w planie studiów - semestr	studia stacjonarne	**Semestr II lub Semestr III**
	studia niestacjonarne	**Semestr II lub Semestr III**
Wymagania wstępne		**Wprowadzenie do cyberbezpieczeństwa**
Egzamin (TAK/NIE)		**NIE**
Liczba punktów ECTS		**3**

Forma prowadzenia zajęć		**wykład**	**ćwiczenia**	**laborato-rium**	**projekt**	**inne**
Liczba godzin w semestrze	studia stacjonarne:	**30**			**30**	
	studia niestacjonarne:	**18**			**18**	

EFEKTY UCZENIA SIĘ

Kategoria	Symbol efektu	Efekty uczenia się	Odniesienie do efektów kierunkowych
Wiedza	W01	Student zna i rozumie zagadnienia związane z weryfikacją zabezpieczeń systemów informatycznych i wykorzystaniem w tym celu algorytmów uczenia maszynowego.	INF2_W05, INF2_W07
	W02	Student zna i rozumie zagrożenia dotyczące systemów informatycznych oraz algorytmy uczenia maszynowego pozwalające je wykrywać.	INF2_W04 INF2_W05, INF2_W07
	W03	Student zna i rozumie zasady, metody uczenia maszynowego pozwalające tworzyć oprogramowanie spełniające wymogi bezpieczeństwa.	INF2_W04, INF2_W05, INF2_W07
Umiejętności	U01	Student potrafi, przy użyciu metod uczenia maszynowego, przeprowadzić czynności audytowe pozwalające ocenić stan zabezpieczenia systemu informatycznego i wskazać ewentualne braki.	INF2_U01, INF2_U05, INF2_U07, INF2_U09, INF2_U11
	U02	Student potrafi, przy użyciu metod uczenia maszynowego, monitorować, wykrywać, usuwać i zapobiegać zagrożeniom.	INF2_U07, INF2_U09
Kompetencje społeczne	K01	Student rozumie potrzebę ciągłego podnoszenia kompetencji w zakresie cyberbezpieczeństwa.	INF2_K03, INF2_K04

TREŚCI PROGRAMOWE

Forma zajęć	Treści programowe
wykład	1. **Uczenie maszynowe a bezpieczeństwo systemów komputerowych** (obszar zagrożeń związanych z technologiami informatycznymi, przykłady zastosowania uczenia maszynowego do celów zabezpieczenia systemów informatycznych). 2. **Zagadnienia klasyfikacji i klastrowania** (algorytmy trenowania, algorytmy klasyfikacyjne i klastrowania, przykłady praktyczne). 3. **Wykrywanie anomalii pracy systemów komputerowych i nieoczekiwanych zdarzeń** (wykrywanie włamań przy pomocy algorytmów heurystycznych i bazujących na danych, problemy uczenia maszynowego w wykrywaniu anomalii). 4. **Analiza złośliwego oprogramowania** (definicja i klasyfikacja oprogramowania typu malware, ekstrakcja informacji z danych binarnych i wykorzystanie ich w celu utworzenia opisywalnych zbiorów danych, wybór istotnych cech w kontekście uczenia maszynowego). 5. **Analiza ruchu sieciowego przy użyciu uczenia maszynowego** (kontrola dostępu i autoryzacja, wykrywanie naruszeń protokołów bezpieczeństwa, detekcja anomalii w sieci, zabezpieczanie danych, ataki pasywne i aktywne, botnets, budowa predykcyjnego modelu klasyfikującego ataki sieciowe). 6. **Ochrona serwisów internetowych** (rodzaje nadużyć, w tym problemy związane z autoryzacją, przejęciem i tworzeniem konta, klasyfikowanie nadużyć oraz wykorzystanie nadzorowanego uczenia maszynowego w kontekście problemów związanych z nadużyciami ochrony serwisów internetowych,). 7. **Kontradyktoryjne uczenie maszynowe** (znaczenie kontradyktoryjnych algorytmów uczenia maszynowego, luki w zabezpieczeniach algorytmów uczenia maszynowego, techniki ataku: „model poisoning", „evasion attack").
projekt	W ramach projektu, studenci realizować będą zadania z zakresu analizy anomalii pracy systemów komputerowych, analizy oprogramowania typu malware i analizy ruchu sieciowego pod kątem bezpieczeństwa systemu komputerowego. Prace będą wykonywane w zespołach liczących nie więcej niż pięć osób.

METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ

Symbol efektu	Metody sprawdzania efektów uczenia się					
	Egzamin ustny	Egzamin pisemny	Kolokwium	Projekt	Sprawozdanie	Inne
W01			x			
W02			x			
W03			x			
U01				x		
U02				x		
K01			x			

FORMA I WARUNKI ZALICZENIA

Forma zajęć	Forma zaliczenia	Warunki zaliczenia
wykład	zaliczenie z oceną	Uzyskanie co najmniej 50% punktów z kolokwium
projekt	zaliczenie z oceną	Uzyskanie co najmniej 50% punktów za realizację projektu

NAKŁAD PRACY STUDENTA

Bilans punktów ECTS													
Lp.	Rodzaj aktywności	Obciążenie studenta										Jednostka
		studia stacjonarne					studia niestacjonarne					
1.	Udział w zajęciach zgodnie z planem studiów	W	C	L	P	S	W	C	L	P	S	h
		30			**30**		**18**			**18**		
2.	Inne (konsultacje, egzamin)	**2**			**2**		**2**			**2**		h
3.	**Razem przy bezpośrednim udziale nauczyciela akademickiego**	**64**					**40**					h
4.	**Liczba punktów ECTS, którą student uzyskuje przy bezpośrednim udziale nauczyciela akademickiego**	**2,56**					**1,6**					ECTS
5.	**Liczba godzin samodzielnej pracy studenta**	**11**					**35**					h
6.	**Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy**	**0,44**					**1,4**					ECTS
7.	**Nakład pracy związany z zajęciami o charakterze praktycznym**	**30**					**18**					h
8.	**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym**	**1,20**					**0,72**					ECTS
9.	**Sumaryczne obciążenie pracą studenta**	**75**					**75**					h
10.	**Punkty ECTS za moduł** *1 punkt ECTS=25 godzin obciążenia studenta*	**3**										ECTS

LITERATURA

1. Clarence Chio, David Freeman: "Machine learning and security: Protecting with Data and Algorithms 1st Edition", O'Reilly Media, 2018.
2. Anthony D. Joseph, Blaine Nelson, Benjamin P. Rubinstein: "Adversarial Machine Learning 1st Edition", Cambridge University Press, 2019.
3. Leslie F. Sikos: "AI in Cybersecurity (Intelligent Systems Reference Library, 151)", Springer, 2019.
4. Sumeet Dua, Xian Du: "Data Mining and Machine Learning in Cybersecurity", Auerbach Publications, 2011.
5. Joshua Saxe, Hillary Sanders: "Malware Data Science, Attack Detection and Attribution", No Starch Press, 2018.