SYLABUS PRZEDMIOTU

Podstawy bezpieczeństwa komputerowego

I. Informacje ogólne

Nazwa przedmiotu	*Podstawy bezpieczeństwa komputerowego*
Kod przedmiotu	PBK
Rodzaj przedmiotu	specjalistyczny
Kierunek studiów	Informatyka
Poziom kształcenia	Uzupełniający
Profil kształcenia	Ogólnoakademicki
Rok studiów	I
Rodzaje zajęć i liczba godzin	
Wykład	30
Ćwiczenia	0
Laboratoria	30
Praktyki	0
Liczba punktów ECTS	6

Imię, nazwisko, tytuł/stopień naukowy, adres e-mail wykładowcy (wykładowców)/ prowadzących zajęcia

- dr Tomasz Kowalski

Język wykładowy	polski
Przedmiot prowadzony zdalnie (e-learning)	tak, częściowo

II. Informacje szczegółowe

1. Cele przedmiotu

Przedmiot stawia następujące cele:

-. wykształcenie świadomości wyzwań związanych z zapewnieniem bezpieczeństwa,

- wykształcenie intuicji dążenia do zrównoważonego rozwoju w zakresie bezpieczeństwa,

- przekazanie ogólnej wiedzy o możliwie najszerszym zakresie potencjalnych problemów bezpieczeństwa w całości systemu informatycznego, a w szczególności o sposobach ich identyfikacji oraz mechanizmach zapobiegania ich wystąpieniu.

- umożliwienie zdobycia doświadczenia w wykrywaniu i eksploatacji rzeczywistych podatności w analogach rzeczywistych systemów (bez obawy o konsekwencje prawne lub majątkowe podejmowanych działań ofensywnych).

2. Wymagania wstępne w zakresie wiedzy, umiejętności oraz kompetencji społecznych

Wiedza i umiejętności w zakresie programowania i znajomości systemów operacyjnych na poziomie inżyniera informatyki.

3. Efekty uczenia się (EU) dla zajęć i odniesienie do efektów uczenia się (EK) dla kierunku studiów

Symbol EU dla przedmiotu	Symbol EK dla kierunku studiów	Po zakończeniu modułu i potwierdzeniu osiągnięcia EU student/ka:
PBK_01	KINF2_W02	Rozumie rolę zabezpieczeń fizycznych.
PBK_02	KINF2_W02 KINF2_W03	Zna popularne produkty lub rozwiązania służące do zwiększenia bezpieczeństwa fizycznego.
PBK_03	KINF2_W02 KINF2_W03	Zna popularne wektory ataku na infrastrukturę lokalną.
PBK_04	KINF2_W02 KINF2_W03	Zna popularne wektory ataku na infrastrukturę zdalną.
PBK_05	KINF2_W07	Zna popularne produkty lub rozwiązania służące do wykrywania podatności i zapobiegania ich powstawaniu.

PBK_06	KINF2_U04 KINF2_U05	Potrafi zastosować popularne produkty lub rozwiązania służące do wykrywania podatności.
PBK_07	KINF2_U05 KINF2_K03	Potrafi wykorzystać wykrytą podatność dla dalszej penetracji, destabilizacji systemu, przejęcia kontroli nad systemem lub pozyskania danych.
PBK_08	KINF2_U04 KINF2_U05	Potrafi prowadzić przegląd kodu w celu wyeliminowania faktycznych i potencjalnych podatności.
PBK_09	KINF2_U11 KINF2_U12 KINF2_K01	Potrafi pozyskiwać wiedzę na temat aktualnych zagrożeń i mechanizmów zapobiegania im.
PBK_10	KINF2_W07	Rozumie potrzebę ustawicznego podnoszenia wiedzy i umiejętności z zakresu bezpieczeństwa komputerowego.
PBK_11	KINF2_W06 KINF2_K03 KINF2_K06	Rozumie kulturowe i socjologiczne uwarunkowania bezpieczeństwa komputerowego.

4. Treści programowe zapewniające uzyskanie efektów uczenia się (EU) z odniesieniem do odpowiednich efektów uczenia się (EU) dla przedmiotu

Lp.	Symbol EU dla przedmiotu	Godzin Wykład	Godzin ĆW/ LAB/ SEM	Godzin pracy własnej	Opis treści kształcenia modułu zajęć/przedmiotu
Suma		30	30	90	
1.	PBK_01, PBK_03, PBK_04	2			Przedstawienie układu treści kursu. Wprowadzenie podstawowej terminologii. Charakteryzacja "bezpieczeństwa" jako szerokiego wachlarza zagadnień technicznych i nietechnicznych.
2.	PBK_09, PBK_10		2	6	Linux i pisanie skryptów w powłoce systemu Linux. Doświadczalne zidentyfikowanie poziomu wiedzy i umiejętności uczestników w tym zakresie. Samodzielne uzupełnienie lub rozszerzenie wiedzy i umiejętności w oparciu o wskazane materiały. Określenie konfiguracji eksperymentów na podstawie deklaracji uczestników co do ich wiedzy, umiejętności i doświadczenia w zakresie konkretnych języków programowania, bibliotek, narzędzi, itd.,
3.	PBK_03, PBK_04, PBK_05, PBK_09	2		2	Identyfikacja i zapobieganie podatnościom. Najbardziej rozpoznawalne grupy problemów. Symptomy podatności i standardowe rozwiązania.
4.	PBK_06, PBK_07, PBK_08		2	4	Przeprowadzenie eksperymentów: Wykrycie i wykorzystanie podatności. Praca w izolowanym i kontrolowanym środowisku, w którym podatności zostały celowo umieszczone. Samodzielne uzupełnienie lub rozszerzenie wiedzy i umiejętności w zakresie narzędzi lub technologii występujących w omawianym środowisku.
5.	PBK_05	2		2	Przegląd narzędzi do wykrywania podatności. Omówienie popularnych rozwiązań dla danego zastosowania.
6.	PBK_06, PBK_07, PBK_08		2	4	Przeprowadzenie eksperymentów związanych z wykrywaniem podatności.

7.	PBK_01, PBK_02, PBK_03	2		2	Systemy kontroli dostępu w zabezpieczaniu infrastruktury: Wyzwania. Przegląd produktów i rozwiązań.
8.	PBK_06, PBK_07, PBK_08		2	4	Przeprowadzenie eksperymentów związanych z systemami kontroli dostępu w zabezpieczaniu infrastruktury.
9.	PBK_01, PBK_02, PBK_05	2		2	Systemy monitoringu infrastruktury: Wyzwania. Przegląd produktów i rozwiązań.
10.	PBK_06, PBK_07, PBK_08		2	4	Przeprowadzenie eksperymentów związanych z monitoringiem infrastruktury.
11.	PBK_01, PBK_02, PBK_05, PBK_09	2		2	Systemy wykrywania wtargnięć i ich raportowanie: Przegląd rozwiązań.
12.	PBK_06, PBK_07, PBK_08		2	4	Przeprowadzenie eksperymentów związanych z wykrywaniem wtargnięć.
13.	PBK_01, PBK_05, PBK_09	2		2	Zabezpieczenia maszyn lokalnych. Ustanowienie warstwowości zabezpieczeń. Specyfika czynności administracyjnych.
14.	PBK_06, PBK_07, PBK_08		2	4	Przeprowadzenie eksperymentów związanych z zabezpieczeniem maszyn lokalnych.
16.	PBK_04, PBK_05, PBK_09	2		2	Ochrona dostępu zdalnego. Implementacja lokalnych środków zapobiegawczych. Utwardzanie.
17.	PBK_06, PBK_07, PBK_08		2	4	Przeprowadzenie eksperymentów związanych z ochroną dostępu zdalnego.
19.	PBK_01, PBK_04, PBK_09	2		2	Budowa sieci i protokoły sieciowe. Wykorzystanie niezgodnie z przeznaczeniem.
20.	PBK_06, PBK_07, PBK_08		2	4	Przeprowadzenie eksperymentów związanych z ochroną protokołów sieciowych.
22.	PBK_01, PBK_04, PBK_05, PBK_09	2		2	Konfiguracja serwerów. Dobre praktyki czynności administracyjnych.
23.	PBK_06, PBK_07, PBK_08		2	4	Przeprowadzenie eksperymentów związanych z konfiguracją serwerów.
25.	PBK_01, PBK_03, PBK_04, PBK_09	2		2	Urządzenia sieciowe i media transmisyjne. Perspektywa bezpieczeństwa.
26.	PBK_06, PBK_07, PBK_08		2	4	Przeprowadzenie eksperymentów związanych z urządzeniami sieciowymi i mediami transmisyjnymi.
28.	PBK_01, PBK_03, PBK_04, PBK_05, PBK_09	2		2	Ochrona sieci prywatnej. *Perimeter security.*
29.	PBK_06, PBK_07, PBK_08		2	4	Przeprowadzenie eksperymentów związanych z ochroną sieci prywatnej.

30.	PBK_04, PBK_05, PBK_09	2		2	Ochrona transferu przez sieć publiczną. Metody i narzędzia.
31.	PBK_06, PBK_07, PBK_08		2	4	Przeprowadzenie eksperymentów związanych z ochroną transferu przez sieć publiczną.
32.	PBK_11	2		2	Kulturowe spojrzenie na bezpieczeństwo. Ludzie, organizacje, styl życia i pracy.
33.	PBK_06, PBK_07, PBK_08		2	4	Przeprowadzenie eksperymentów związanych z kulturowym spojrzeniem na bezpieczeństwo.
34.	PBK_10			6	Przygotowanie do egzaminów końcowych.
35.	PBK_10	2	2		Podsumowanie kursu.

5. Zalecana literatura

1) Ken Douglas, "Cyber Security for Beginners: Understanding Cybersecurity and Ways to Protect Yourself", 2019.
2) Scott Augenbaum, "The Secret to Cybersecurity: A Simple Plan to Protect Your Family and Business from Cybercrime", Forefront Books, 2019
3) Peter Kim, "The Hacker Playbook 3: Practical Guide To Penetration Testing", 2018
4) Erdal Ozkaya, "Cybersecurity: The Beginner's Guide: A comprehensive guide to getting started in cybersecurity", Packt, 2018
5) Yuri Diogenes, "Cybersecurity – Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics", Packt, 2018
6) Yuri Diogenes, "Cybersecurity – Attack and Defense Strategies: Counter modern threats and employ state-of-the-art tools and techniques to protect your organization against cybercriminals", Packt, 2019
7) Marcus Carey, "Tribe of Hackers: Cyber Advice from the Best Hackers in the World". 2019
8) Marcus Carey, "Tribe of Hackers Red Team: Tribal Knowledge from the Best in Offensive Cybersecurity", Wiley, 2019.
9) Marcus Carey, "Tribe of Hackers Blue Team: Tribal Knowledge from the Best in Defensive Cybersecurity", Wiley, 2020.

V. Informacje dodatkowe

1. Metody i formy prowadzenia zajęć umożliwiające osiągnięcie założonych EU (proszę wskazać z proponowanych metod właściwe dla opisywanych zajęć lub/i zaproponować inne)

Realizacja	Metody i formy prowadzenia zajęć
✔	Wykład z prezentacją multimedialną wybranych zagadnień
	Wykład konwersatoryjny
	Wykład problemowy
	Dyskusja

	Praca z tekstem
✔	Metoda analizy przypadków
✔	Uczenie problemowe (Problem-based learning)
	Gra dydaktyczna/symulacyjna
✔	Rozwiązywanie zadań (np.: obliczeniowych, artystycznych, praktycznych)
	Metoda ćwiczeniowa
✔	Metoda laboratoryjna
	Metoda badawcza (dociekania naukowego)
✔	Metoda warsztatowa
	Metoda projektu
✔	Pokaz i obserwacja
	Demonstracje dźwiękowe i/lub video
✔	Metody aktywizujące (np.: „burza mózgów”, technika analizy SWOT, technika drzewka decyzyjnego, metoda „kuli śniegowej”, konstruowanie „map myśli”)
	Praca w grupach
✔	Wykład zdalny w czasie rzeczywistym
	Wykład zdalny asynchroniczny uzupełniony spotkaniem w czasie rzeczywistym
	Wykład zdalny asynchroniczny z aktywnością studenta uzupełniony spotkaniem w czasie rzeczywistym
	Ćwiczenia/laboratoria/konwersatoria zdalne w czasie rzeczywistym
	Ćwiczenia zdalne asynchroniczne z pracą indywidualną studenta uzupełnione spotkaniem w czasie rzeczywistym
	Ćwiczenia zdalne asynchroniczne z pracą grupową studentów uzupełnione spotkaniem w czasie rzeczywistym
	Laboratorium cyfrowe zdalne uzupełnione spotkaniem w czasie rzeczywistym
	Konwersatorium asynchroniczne zdalne uzupełnione spotkaniem w czasie rzeczywistym
	Seminarium zdalne w czasie rzeczywistym
	Seminarium asynchroniczne zdalne ze spotkaniem w czasie rzeczywistym
	Inne (jakie?) -

2. Sposoby oceniania stopnia osiągnięcia EU (proszę wskazać z proponowanych sposobów właściwe dla danego EU lub/i zaproponować inne

Sposoby oceniania	Symbole EU dla modułu zajęć/przedmiotu									
	PBK_01, PBK_02, PBK_03, PBK_04, PBK_05, PBK_09, PBK_11	PBK_05, PBK_06, PBK_07, PBK_08, PBK_09								
Egzamin pisemny	✔	✔								
Egzamin ustny										
Egzamin z „otwartą książką”										
Kolokwium pisemne										
Kolokwium ustne										

Test	✔	✔								
Projekt										
Esej										
Raport										
Prezentacja multimedialna										
Egzamin praktyczny (obserwacja wykonawstwa)		✔								
Portfolio										
Zadania cząstkowe na wykładzie	✔									
...										

3. Nakład pracy studenta i punkty ECTS

Forma aktywności		Średnia liczba godzin na zrealizowanie aktywności
Godziny zajęć (wg planu studiów) z nauczycielem		60
Praca własna studenta*	Przygotowanie do zajęć	6
	Czytanie wskazanej literatury	30
	Przygotowanie pracy pisemnej, raportu, prezentacji, itp.	0
	Przygotowanie projektu	0
	Przygotowanie pracy semestralnej	0
	Przygotowanie do egzaminu/zaliczenia	6
	Praca z materiałem do samokształcenia (np. Jupyter Notebook)	54
	Praca z laboratorium cyfrowym (np. Code Runner)	0
	Inne (jakie?)	
SUMA GODZIN		150
LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU		6

* proszę wskazać z proponowanych przykładów pracy własnej studenta właściwe dla opisywanego modułu lub/i zaproponować inne

4. Kryteria oceniania wg skali stosowanej w UAM

Ocena	Kryterium
bardzo dobry (bdb; 5,0)	od 83% punktów
dobry plus (+db; 4,5)	od 75% punktów
dobry (db; 4,0)	od 67% punktów
dostateczny plus (+dst; 3,5)	od 59% punktów
dostateczny (dst; 3,0)	od 50% punktów
niedostateczny (ndst; 2,0)	poniżej 50% punktów