Karta opisu zajęć - Sylabus

Państwowa Wyższa Szkoła Techniczno-Ekonomiczna im. ks. Bronisława Markiewicza w Jarosławiu

I. INFORMACJE PODSTAWOWE

Nazwa zajęć: **Polityki i standardy cyberbezpieczeństwa**	Cykl kształcenia rozpoczynający się w roku akademickim 2023/2024
Nazwa kierunku studiów, poziom i profil kształcenia: Bezpieczeństwo wewnętrzne II stopień, profil praktyczny	
Język wykładowy: polski	Rodzaj zajęć: zajęcia specjalistyczne
Rok studiów: II	Semestr: 3
Liczba punktów ECTS przypisana zajęciom: 2	Koordynator zajęć Imię, nazwisko, tytuł/stopień naukowy, adres e-mail:
Jednostka organizacyjna: Instytut Ekonomii i Zarządzania	

FORMA PROWADZENIA ZAJĘĆ I LICZBA GODZIN

Ogólna liczba godzin zajęć dydaktycznych na studiach stacjonarnych i niestacjonarnych z podziałem na formy:

Studia stacjonarne		**Studia niestacjonarne**	
Wykład:	15	Wykład:	
Ćwiczenia:	15	Ćwiczenia:	
Laboratorium:		Laboratorium:	
Lektorat:		Lektorat:	
Projekt:		Projekt:	
Zajęcia praktyczne:		Zajęcia praktyczne:	
Seminarium:		Seminarium:	
Zajęcia terenowe:		Zajęcia terenowe:	
Praktyki:		Praktyki:	
Inna forma (jaka):		Inna forma (jaka):	
RAZEM:	30	**RAZEM:**	

II. INFORMACJE SZCZEGÓŁOWE

Wymagania wstępne i dodatkowe: brak

Cel (cele) kształcenia dla zajęć: pogłębienie wiedzy i umiejętności w zakresie europejskiego i krajowego systemu cyberbezpieczeństwa, identyfikacji współczesnych zagrożeń systemów teleinformatycznych oraz stosowania odpowiednich zabezpieczeń

EFEKTY UCZENIA SIĘ OKREŚLONE DLA ZAJĘĆ I ICH ODNIESIENIE DO EFEKTÓW UCZENIA SIĘ OKREŚLONYCH DLA KIERUNKU STUDIÓW

Efekty uczenia się określone dla zajęć w kategorii wiedza, umiejętności oraz kompetencje społeczne oraz metody weryfikacji efektów uczenia się

UWAGA:

Dzielimy efekty uczenia się określone dla zajęć na kategorie wiedzy, umiejętności i kompetencji społecznych. Określone dla zajęć efekty uczenia się nie muszą obejmować wszystkich trzech kategorii i zależą od formy zajęć.

Symbol efektów uczenia się określonego dla zajęć*	Treść efektu uczenia się. Po zakończeniu zajęć i potwierdzeniu osiągnięcia efektów uczenia się, student w kategorii:	Odniesienie do efektów uczenia się określonych dla kierunku studiów (symbol efektów uczenia się)

Wiedzy - zna i rozumie		
PiSC_W01	europejski i krajowy system cyberbezpieczeństwa, organizację krajowego systemu cyberbezpieczeństwa, zagrożenia cyberbezpieczeństwa i zarządzanie bezpieczeństwem w sieci	K_W02
Umiejętności - potrafi		
PiSC_U01	identyfikować współczesne zagrożenia systemów teleinformatycznych oraz stosować odpowiednie zabezpieczenia	K_U02
Kompetencji społecznych - jest gotów do		
PiSC_K01	krytycznej analizy posiadanej wiedzy, hierarchizowania celów i metod działania na bazie posiadanych i pozyskanych informacji.	K_K01

UWAGA!

Zaleca się, aby w zależności od liczby godzin zajęć, liczba efektów uczenia się zawierała się w przedziale: 3-7, ale są to wartości umowne.

TREŚCI PROGRAMOWE I ICH ODNIESIENIE DO EFEKTÓW UCZENIA SIĘ OKREŚLONYCH DLA ZAJĘĆ

Treści programowe (uszczegółowione, zaprezentowane z podziałem na poszczególne formy zajęć, tj. wykład, ćwiczenia, laboratoria, projekty, seminaria i inne):

Symbol treści programowych	Opis treści programowych	Forma zajęć	Metody dydaktyczne prowadzenia zajęć umożliwiające osiągniecie założonych efektów uczenia się *	Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć #
		wykład		
TP-01	Cyberbezpieczeństwo państwa. Europejski i krajowy system cyberbezpieczeństwa (Podstawy ustrojowe europejskiego cyberbezpieczeństwa. Dyrektywa NIS. Organizacja krajowego systemu cyberbezpieczeństwa. Doktryna i strategia cyberbezpieczeństwa RP na tle innych krajów). Zagrożenia. (Identyfikacja zagrożeń. Nieobliczalne oprogramowanie. Ewolucja zagrożeń. Ataki ukierunkowane. Podatność Internetu Rzeczy (IoT). Oprogramowanie ransomware).	x	wykład podający z prezentacją multimedialną	kolokwium pisemne (egzamin)
TP-02	Bezpieczeństwo systemów operacyjnych (Zagrożenia dla systemów operacyjnych i sposoby ochrony - Ataki na systemy WINDOWS i metody przeciwdziałania. Ataki na systemy UNIX). Bezpieczeństwo sieci (Sieć informatyczna. Mechanizmy bezpieczeństwa usług sieciowych. Detekcja. Podatności w zabezpieczeniach sieci. Zarządzanie	x	wykład podający z prezentacją multimedialną	kolokwium pisemne (egzamin)

	bezpieczeństwem sieci). Zagrożenia dla aplikacji webowych i środki przeciw. Działania (Ataki na serwery aplikacji. Ataki na aplikacje webowe).			
		ćwiczenia		
TP-03	Prywatność i poufność w środowisku chmurowym. Współczesne zagrożenia systemów teleinformatycznych, wirusy polimorficzne, inżynieria wsteczna. Zapory sieciowe nowej generacji, zaawansowane mechanizmy wykrywania zagrożeń.	x	studium przypadku z użyciem narzędzi informatycznych, pogadanka	kolokwium pisemne – rozwiązanie wskazanego problemu
TP-04	Socjotechnika, ochrona danych i inwigilacja. Ujawnianie informacji. Transakcje elektroniczne. Kryteria wyboru zabezpieczeń. (Zasady ogólne. Polityka dotycząca haseł. Wytyczne dotyczące różnych platform technologicznych. Przetwarzanie transakcyjne. Technologie biometryczne).	x	studium przypadku z użyciem narzędzi informatycznych, pogadanka	kolokwium pisemne – rozwiązanie wskazanego problemu

Metody weryfikacji osiągnięcia efektów uczenia się określonych dla zajęć, powinny być zróżnicowane w zależności od kategorii, tj. inne dla kategorii wiedza i inne dla kategorii umiejętności i kompetencje społeczne.

Dla wykładu:

* np. wykład podający, wykład problemowy, ćwiczenia oparte na wykorzystaniu różnych źródeł wiedzy

np. egzamin ustny, test, prezentacja, projekt

Zaleca się podanie przykładowych zadań (pytań) służących weryfikacji osiągniecia efektów uczenia się określonych dla zajęć.

ZALECANA LITERATURA (w tym pozycje w języku obcym)

Literatura podstawowa:

1. Krawiec J., Cyberbezpieczeństwo. Podejście systemowe, Politechnika Warszawska. Warszawa 2019. Ibuk Libra
2. Górka M, Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku, Difin, Warszawa 2014.
3. McNab Chris, Ocena bezpieczeństwa sieci, Wydaw. APN Promise. Warszawa 2017.
4.

Literatura uzupełniająca:

1. Banasiński C., Cyberbezpieczeństwo. Zarys wykładu, Wydaw. Wolters Kluwer, Warszawa 2018.
2. Hoffman T., Wybrane aspekty cyberbezpieczeństwa w Polsce, Wydaw. Fnc, Warszawa 2018.
3. Kluczewski J., Bezpieczeństwo sieci komputerowych. Praktyczne przykłady i ćwiczenia w symulatorze Cisco Packet Tracer, Wydaw. itstart, Warszawa 2019.

III. INFORMACJE DODATKOWE

BILANS PUNKTÓW ECTS

OBCIĄŻENIE PRACĄ STUDENTA (godziny)

<table>
<tr><th>Forma aktywności</th><th colspan="3">Liczba godzin *</th></tr>
<tr><td>Godziny zajęć (według harmonogramu)
z nauczycielem akademickim lub inna osobą prowadzącą zajęcia</td><td colspan="3">30</td></tr>
<tr><td>Praca własna studenta</td><td colspan="3">20</td></tr>
<tr><td>SUMA GODZIN:</td><td colspan="3">50</td></tr>
<tr><td colspan="4">OBCIĄŻENIE PRACĄ STUDENTA (punkty ECTS)</td></tr>
<tr><td colspan="2"></td><td colspan="2">Liczba punktów ECTS</td></tr>
<tr><td rowspan="2">SUMARYCZNA LICZBA PUNKTÓW ECTS PRZYPISANYCH DO ZAJĘĆ</td><td>Praca studenta wymagająca bezpośredniego kontaktu z nauczycielem akademickim lub inną osobą prowadzącą zajęcia</td><td rowspan="2">Ogółem: 2</td><td>1,2</td></tr>
<tr><td>Praca własna studenta</td><td>0,8</td></tr>
<tr><td colspan="4">* godziny lekcyjne, czyli 1 godz. oznacza 45 min;</td></tr>
<tr><td colspan="4">OPIS PRACY WŁASNJE STUDENTA:</td></tr>
<tr><td colspan="4">Praca własna studenta musi być precyzyjnie opisana, uwzględniając charakter praktyczny zajęć. Należy podać symbol efektu uczenia się, którego praca własna dotyczy oraz metody weryfikacji efektów uczenia się stosowane w ramach pracy własnej.
Przykładowe formy aktywności: (1) przygotowanie do zajęć, (2) opracowanie wyników, (3) czytanie wskazanej literatury, (4) napisanie raportu z zajęć, (5) przygotowanie do egzaminu, opracowanie projektu.</td></tr>
<tr><td colspan="4">▪ przygotowanie do kolokwium pisemnego (egzaminu) z wykładów (K_W02, K_K01) – 10 godz.
▪ przygotowanie do kolokwium pisemnego z ćwiczeń (K_U02, K_K01) – 10 godz.</td></tr>
<tr><td colspan="4">KRYTERIA OCENIANIA</td></tr>
<tr><td colspan="4">Ocena kształtująca:
wykład – dyskusja
ćwiczenia – dyskusja</td></tr>
<tr><td colspan="4">Ocena podsumowująca:
wykład - kolokwium pisemne (egzamin)
ćwiczenia – kolokwium pisemne – rozwiązanie wskazanego problemu</td></tr>
<tr><td colspan="4">INFORMACJA O PRZEWIDYWANEJ MOŻLIWOŚCI WYKORZYSTANIA E-LEARNINGU
Zajęcia z wykładów przygotowywane są w formie e-learningu</td></tr>
</table>