KARTA MODUŁU

I. OGÓLNE INFORMACJE O MODULE							
COLLEGIUM WITELONA UCZELNIA PAŃSTWOWA WYDZIAŁ NAUK TECHNICZNYCH I EKONOMICZNYCH							
Kierunek studiów:		**INŻYNIERIA PRODUKCJI I LOGISTYKI**					
Poziom studiów:		studia drugiego stopnia					
Profil studiów:		praktyczny					
Forma studiów:		stacjonarne/niestacjonarne					
Nazwa modułu:		**Cyberbezpieczeństwo**					
Rodzaj modułu:		Obowiązkowy					
Język wykładowy:		Język polski*					
Rok studiów:	2	**Formy prowadzenia zajęć wraz z liczbą godzin dydaktycznych:**					
Semestr:	3	Wykład	Ćwiczenia	Laboratorium	Warsztat	Projekt	Seminarium
Liczba punktów ECTS ogółem:	1	-	-	-	15/8	-	-
Forma zaliczenia:		Zaliczenie na ocenę					
Wymagania wstępne:		Wiedza i umiejętności z matematyki na poziomie podstawowym, umiejętność obsługi komputera.					

II. CELE KSZTAŁCENIA
Cele kształcenia:
Cel 1: Zbudowanie u studentów podstawowej świadomości w dziedzinie bezpieczeństwa systemów informatycznych **Cel 2:** Zapewnienie umiejętności przeprowadzenia prostej analizy zagrożeń w dziedzinie cyberbezpieczeństwa

III. EFEKTY UCZENIA SIĘ WRAZ Z ODNIESIENIEM DO EFEKTÓW KIERUNKOWYCH ORAZ METODY WERYFIKACJI EFEKTÓW			
Efekt	Student, który zaliczył moduł w zakresie:	Odniesienie do efektów kierunkowych	Metody weryfikacji
wiedzy:			
W01	Student posiada wiedzę z zakresu podstawowych pojęć dotyczących bezpieczeństwa systemów informatycznych.	K2IPL_W05	Test wyboru
W02	Student rozumie relację pomiędzy działaniami własnymi i zespołu a poziomem ryzyk.		Test wyboru
umiejętności:			
U01	Student umie wskazać określone zagrożenie w dziedzinie cyberbezpieczeństwa.	K2IPL_U05	Referat w trakcie zajęć
U02	Student umie wskazać najważniejsze metody minimalizacji ryzyk stosowane w branży IT.	K2IPL_U05	Referat w trakcie zajęć
U03	Potrafi podejmować decyzje menedżerskie uwzględniając problematykę cyberbezpieczeństwa.	K2IPL_U09	Referat w trakcie zajęć
kompetencji społecznych:			
K01	Jest odpowiedzialny za powierzoną mu rolę zawodową z uwzględnieniem przestrzegania zasad etyki oraz kultury współpracy.	K2IPL_K04	Referat w trakcie zajęć

IV. TREŚCI PROGRAMOWE
Treści programowe (tematyka zajęć, zaprezentowana z podziałam na poszczególne formy zajęć z określeniem liczby godzin potrzebnych na ich realizację)
Warsztaty:

Kod	Tematyka zajęć	Liczba godzin 15/8
war1	Wprowadzenie do współczesnych sieci i Internetu	5/3
war2	Pojęcie bezpieczeństwa jako procesu i jego najważniejsze funkcje.	2/1
war3	Typowe zagrożenia dla bezpieczeństwa systemów informatycznych oraz metody zabezpieczeń.	4/2
war4	Dobre praktyki w zakresie bezpieczeństwa.	4/2

V. METODY KSZTAŁCENIA, NARZĘDZIA DYDAKTYCZNE

1. **Metody kształcenia:** Warsztaty problemowe w laboratorium komputerowym z wygłoszeniem referatu przez studentów.
2. **Narzędzia (środki) dydaktyczne:** oprogramowanie specjalistyczne w laboratorium komputerowym, tablica multimedialna

VI. FORMA I KRYTERIA ZALICZENIA MODUŁU

Forma zaliczenia modułu.
Kolokwium w formie testu
Zadania praktyczne w formie ćwiczeń praktycznych do wykonania własnego przez studentów.

Kryteria oceny formującej*:**
1.Wykazanie się wiedzą teoretyczną w trakcie rozwiązywania testu na platformie Cisco NetAcad
2. Umiejętność samodzielnej analizy wybranego problemu i przedstawienie wniosków w formie referatu.

Kryteria oceny podsumowującej***
1. Test z wykładu:
50-59% - ocena dostateczna,
60-69% - ocena dostateczna plus,
70-79% - ocena dobra,
80-89% - ocena dobra plus,
powyżej 90% - ocena bardzo dobra.

2. Referat
1 pkt. - ocena dostateczna,
2 pkt. - ocena dostateczna plus,
3 pkt. - ocena dobra,
4 pkt. - ocena dobra plus,
5 pkt. - ocena bardzo dobra

Na ocenę 3,0: student zna podstawowe pojęcia.
Na ocenę 3,5: student zna podstawowe pojęcia i rozumie ich rolę.
Na ocenę 4,0: student zna podstawowe pojęcia i rozumie ich rolę. Potrafi samodzielnie wskazać potencjalne zagrożenia.
Na ocenę 4.5: student zna podstawowe pojęcia i rozumie ich rolę. Potrafi samodzielnie wskazać potencjalne zagrożenia i potrafi zaproponować typowe rozwiązania minimalizujące ryzyko.
Na ocenę 5: student zna podstawowe pojęcia i rozumie ich rolę. Potrafi samodzielnie wskazać potencjalne zagrożenia.
Na ocenę 4.5: student zna podstawowe pojęcia i rozumie ich rolę. Potrafi samodzielnie wskazać potencjalne zagrożenia i potrafi zaproponować typowe rozwiązania minimalizujące ryzyko oraz samodzielnie przeprowadzić analizę ryzyka

Ocena podsumowująca*:**
Ocena z modułu: średnia ocen z prac pisemnych i aktywności na zajęciach.

VII. BILANS PUNKTÓW ECTS - NAKŁAD PRACY STUDENTA

Kategoria	**Obciążenie studenta S/N**
Liczba godzin realizowanych przy bezpośrednim udziale nauczyciela (godziny kontaktowe)	**15/8**
Udział w wykładach	-
Udział w innych formach zajęć (warsztat)	15/8
Inne: udział w egzaminie	-
Samodzielna praca studenta (godziny niekontaktowe	**15/22**
Przygotowanie do wykładu	-
Przygotowanie do innych form zajęć (warsztat**)	5/10
Przygotowanie do egzaminu	-
Przygotowanie do zaliczenia innych zajęć (warsztat**)	5/7
Inne (np. gromadzenie materiałów do projektu, kwerenda internetowa, opracowanie prezentacji multimedialnej itp.)	5

Łączna liczba godzin	**30**
Punkty ECTS za moduł	**1**

VIII. ZALECANA LITERATURA

Literatura podstawowa:

1. Kurs Introduction to Cybersecurity naplatformie Cisco NetAcad

Literatura uzupełniająca:

1. Wskazane przez prowadzącego aktualne artykuły w mediach poświęconych problematyce cyberbezpieczeństwa.

*należy odpowiednio wypełnić

**należy wpisać formę/formy przypisane do modułu określone w programie studiów (wykład, semiczenia, seminarium, konwersatorium, lektorat, laboratorium, warsztat, projekt, zajęcia praktyczne, zajęcia terenowe, zajęcia wychowania fizycznego, praktyka zawodowa, inne)

*** proszę wpisać odpowiednie kryteria oceny formującej i podsumowującej