KARTA MODUŁU

I. OGÓLNE INFORMACJE O MODULE									
COLLEGIUM WITELONA UCZELNIA PAŃSTOWA 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:		**MODUŁ KSZTAŁCENIA KIERUNKOWEGO**							
Język wykładowy:		Język polski*							
Rok studiów:	**2**	**Formy prowadzenia zajęć wraz z liczbą godzin dydaktycznych:**							
Semestr:	**3**	Warsztat							
Liczba punktów ECTS ogółem:	**2**	30/16							
Forma zaliczenia:		Zaliczenie z oceną							
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		
Efekt uczenia się	Student, który zaliczył moduł w zakresie:	Odniesienie do efektów kierunkowych
wiedzy:		
W01	posiada wiedzę z zakresu podstawowych pojęć dotyczących bezpieczeństwa poszczególnych elementów złożonych systemów informatycznych wykorzystywanych w zadaniach produkcyjnych.	K2IPL_W05
umiejętności:		
U01	potrafi stosować standardowe metody zabezpieczeń i dobre praktyki w celu optymalizacji poziomu bezpieczeństwa systemów informatycznych, oraz potrafi określić specyficzne zagrożenia dla procesów realizowanych w nowoczesnych środowiskach	K2IPL_U05
U02	potrafi identyfikować podatności systemów oraz stosować narzędzia i procedury (np. systemy IDS/IPS, szyfrowanie, polityki haseł) mające na celu minimalizację prawdopodobieństwa i skutków wystąpienia cyberzagrożeń.	K2IPL_U09
kompetencji społecznych:		
K01	jest świadomy prawnej i etycznej odpowiedzialności związanej z dostępem do zasobów sieciowych i informacji oraz rozumie konieczność współpracy z użytkownikami w celu budowania kultury bezpieczeństwa i propagowania dobrych praktyk w organizacji.	K2IPL_K04

IV. TREŚCI PROGRAMOWE		
Treści programowe (tematyka zajęć, zaprezentowana z podziałam na poszczególne formy zajęć z określeniem liczby godzin potrzebnych na ich realizację)		
Warsztat:		
Kod	Tematyka zajęć	Liczba godzin 30/16
war1	Przedstawienie treści karty modułu. Wprowadzenie do współczesnych sieci i Internetu.	2/2
war2	Charakterystyka pojęć związanych z cyberbezpieczeństwem.	4/2
war3	Ochrona systemu komputerowego.	4/2
war4	Hasła i logowanie. Ataki na hasła.	4/2

war5	Ataki socjotechniczne – phishing.	4/2
war6	Bezpieczeństwo elementów sieci komputerowych.	4/2
war7	Szyfrowanie. Szyfrowanie symetryczne, asymetryczne, hybyrdowe.	4/2
war8	Wykorzystanie szyfrowania w IT.	4/2

V. METODY KSZTAŁCENIA, NARZĘDZIA DYDAKTYCZNE

1. **Metody kształcenia:** metoda problemowa, metoda ćwiczeniowa, metoda projektu, dyskusja.
2. **Narzędzia (środki) dydaktyczne:** prezentacja multimedialna, tablica multimedialna

VI. FORMA I KRYTERIA ZALICZENIA MODUŁU

1. **Formy zaliczenia:**
   Warsztat: zaliczenie z oceną.

2. **Sposób weryfikacji i oceniania efektów uczenia się:**
   Warsztat:
   - przygotowanie: projektu, referatu – kryteria oceny: 51% - 60% - ocena dostateczna; 61% - 70% - ocena dostateczna plus; 71% - 80% - ocena dobra; 81% - 90% - ocena dobra plus; 91% - 100% - ocena bardzo dobra,
   - obserwacja i ocena postaw studenta.

3. **Podstawowe kryteria** oceny lub wymagania egzaminacyjne określane są indywidualnie, jednak powinny zachować adekwatność wobec zaplanowanych efektów uczenia się.

VII. BILANS PUNKTÓW ECTS - NAKŁAD PRACY STUDENTA

Kategoria	Obciążenie studenta
Liczba godzin realizowanych przy bezpośrednim udziale nauczyciela (godziny kontaktowe)	**30/16**
Udział w wykładach	-
Udział w warsztacie	30/16
Samodzielna praca studenta (godziny niekontaktowe)	**20/34**
Przygotowanie do wykładu	-
Przygotowanie do warsztatu	10/20
Przygotowanie do egzaminu	-
Przygotowanie do zaliczenia warsztatu	10/14
Łączna liczba godzin	**50**
Punkty ECTS za moduł	**2**

VIII. ZALECANA LITERATURA

Literatura podstawowa:

1. Krawiec, J. (2019). *Cyberbezpieczeństwo: podejście systemowe*. Oficyna Wyd. Politechniki Warszawskiej.
2. Kurs Introduction to Cybersecurity na platformie Cisco NetAcad.

Literatura uzupełniająca:

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

Na kierunkach studiów, na których obowiązują standardy kształcenia oraz odrębne przepisy określone przez właściwego ministra, karty modułów powinny także uwzględniać powyższe uregulowania

*należy odpowiednio wypełnić

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