KARTA MODUŁU

I. OGÓLNE INFORMACJE O MODULE						
COLLEGIUM WITELONA UCZELNIA PAŃSTWOWA WYDZIAŁ NAUK TECHNICZNYCH I EKONOMICZNYCH						
Kierunek studiów:		**INFORMATYKA**				
Poziom studiów:		studia pierwszego stopnia				
Profil studiów:		praktyczny				
Forma studiów:		stacjonarne/niestacjonarne				
Nazwa modułu:		**Bezpieczeństwo systemów informatycznych**				
Rodzaj modułu:		Moduł kształcenia kierunkowego				
Język wykładowy:		Język polski*				
Rok studiów:	**3**	**Formy prowadzenia zajęć wraz z liczbą godzin dydaktycznych:**				
Semestr:	**6**	Wykład**	Projekt**			
Liczba punktów ECTS ogółem:	**4**	30/12	30/12			
Forma zaliczenia:		Egzamin				
Wymagania wstępne:		Wiedza z zakresu sieci komputerowych, znajomość standardów, protokołów i usług sieciowych, podstaw algebry				

II. CELE KSZTAŁCENIA
Cele kształcenia:
Cel 1: Przekazanie wiedzy z zakresu bezpieczeństwa systemów informatycznych, współczesnych zagrożeń i mechanizmów zabezpieczających. **Cel 2:** Nabycie umiejętności praktycznego wykorzystania i konfiguracji mechanizmów bezpieczeństwa. **Cel 3:** Nabycie umiejętności samodzielnego pozyskiwania, selekcji i syntezy informacji z zakresu bezpieczeństwa informatycznego oraz przygotowania i przedstawienia ich w postaci prezentacji multimedialnej.

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 szeroką wiedzę z zakresu bezpieczeństwa systemów informatycznych, współczesnych zagrożeń i mechanizmów zabezpieczających	K1I_W06
W02	Zna architekturę i zasady działania urządzeń zabezpieczających sieci teleinformatyczne (np. zapory sieciowe, systemy IDS/IPS), metody ich bezpiecznej konfiguracji (m.in. filtrowanie ruchu, listy ACL) oraz techniki diagnostyki i monitorowania sieci w celu wykrywania zagrożeń.	K1I_W08
W03	Zna zasady bezpiecznej konfiguracji aplikacji sieciowych i systemów bazodanowych (w tym metody ochrony przed atakami typu SQL Injection), mechanizmy kryptograficzne stosowane do zabezpieczania transmisji danych (SSL/TLS, VPN) oraz standardy sterowania dostępem do zasobów sieciowych (AAA, RADIUS).	K1I_W09
W04	Zna prawne i normalizacyjne uwarunkowania ochrony informacji (RODO, ustawa o podpisie elektronicznym, normy rodziny ISO 27000), zasady etyki zawodowej w działaniach audytorskich oraz procedury zapewnienia bezpieczeństwa i higieny pracy w środowisku przetwarzania danych (polityki bezpieczeństwa).	K1I_W13
W05	Zna regulacje prawne dotyczące ochrony własności intelektualnej i prawa autorskiego w odniesieniu do oprogramowania i baz danych, a także rozumie prawne aspekty stosowania mechanizmów bezpieczeństwa (ustawa o podpisie elektronicznym, ochrona danych osobowych) oraz zasady odpowiedzialności karnej za cyberprzestępczość.	K1I_W14
umiejętności:		
U01	Umie praktycznie wykorzystać oraz wykonać konfigurację mechanizmów bezpieczeństwa.	K1I_U01

U02	Potrafi samodzielnie pozyskać i wykorzystać informacje z zakresu bezpieczeństwa informatycznego oraz przygotować ich w postaci prezentacji multimedialnej.	K1I_U11
kompetencji społecznych:		
K01	Jest gotów do odpowiedzialnego współdziałania w zespole projektowym (np. audytorskim), ściśle stosując się do przyjętych procedur i polityk bezpieczeństwa, oraz ponoszenia odpowiedzialności za skutki własnych decyzji konfiguracyjnych wpływających na szczelność systemu.	K1I_K03

IV. TREŚCI PROGRAMOWE

Treści programowe (tematyka zajęć, zaprezentowana z podziałam na poszczególne formy zajęć z określeniem liczby godzin potrzebnych na ich realizację)

Wykład:

Kod	Tematyka zajęć	Liczba godzin S/N
W1	Zapoznanie z treścią karty modułu. Wprowadzenie, podstawowe pojęcia bezpieczeństwa	2/1
W2	Zagrożenia i podatności systemów informatycznych	2/1
W3	Standaryzacja bezpieczeństwa	2/1
W4	Kryptografia symetryczna	4/1
W5	Kryptografia asymetryczna, funkcje skrótu	2/1
W6	Dystrybucja kluczy	2/1
W7	Podpis cyfrowy, infrastruktura klucza publicznego	2/1
W8	Sterowanie dostępem	2/1
W9	Bezpieczne usługi sieciowe	4/1
W10	Filtrowanie i kontrola ruchu sieciowego	4/1
W11	Niezawodność systemów informatycznych	2/1
W12	Projektowanie i wdrażanie polityki bezpieczeństwa	2/1

Projekt:**

Kod	Tematyka zajęć	Liczba godzin S/N
P1	Zapoznanie z treścią karty modułu. Wprowadzenie, zasady przygotowywania i przedstawiania prezentacji, omówienie i wybór tematów	4/1
P2	Prezentacje studenckie na wybrane tematy z zakresu bezpieczeństwa systemów informatycznych, dyskusje w grupie seminaryjnej dotyczące każdej prezentacji	26/11

V. METODY KSZTAŁCENIA, NARZĘDZIA DYDAKTYCZNE

1. Metody kształcenia:
- Ćwiczenia laboratoryjne,
- Demonstracja,
- Dyskusja.

2. Narzędzia (środki) dydaktyczne:
- Tablica multimedialna
- Komputer

VI. FORMA I KRYTERIA ZALICZENIA MODUŁU

1. Forma zaliczenia modułu:
- Wykład: egzamin
- Projekt: zaliczenie z oceną

2. Sposób weryfikacji i oceniania efektów uczenia się:
- Wykład: egzamin pisemny lub ustny
- Projekt: prezentacje projektów
- Obserwowanie postaw studentów

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

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 (S/N)**
Liczba godzin realizowanych przy bezpośrednim udziale nauczyciela (godziny kontaktowe)	**60/24**
Udział w wykładach	30/12
Udział w projekcie	30/12
Samodzielna praca studenta (godziny niekontaktowe)	**40/76**
Przygotowanie do wykładu	10/20
Przygotowanie do projektu	20/30
Przygotowanie do egzaminu	6/11
Przygotowanie do zaliczenia projektu	4/15
Łączna liczba godzin	**100**
Punkty ECTS za moduł	**4**

VIII. ZALECANA LITERATURA

Literatura podstawowa:

1. Cole, E., Krutz, R., & Conley, J. (2005). *Bezpieczeństwo sieci: Biblia*. Helion.
2. Dostálek, L. (2006). *Bezpieczeństwo protokołu TCP/IP: Kompletny przewodnik*. Wydawnictwo Naukowe PWN.
3. Stallings, W. (2012). *Kryptografia i bezpieczeństwo sieci komputerowych: Matematyka szyfrów i techniki kryptologii*. Helion.

Literatura uzupełniająca:

1. Anderson, R. (2005). *Inżynieria zabezpieczeń*. Wydawnictwa Naukowo-Techniczne.
2. Fry, C., & Nystrom, M. (2010). *Monitoring i bezpieczeństwo sieci.* Helion.

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)