Politechnika Białostocka									
Kierunek studiów	**Informatyka**							**Poziom i forma studiów**	**pierwszego stopnia inżynierskie niestacjonarne**
Specjalność / Ścieżka dyplomowania	**---**							**Profil kształcenia**	ogólnoakademicki
Nazwa przedmiotu	**Bezpieczeństwo sieci komputerowych**							**Kod przedmiotu**	**INZ1BSK**
								Rodzaj przedmiotu	obowiązkowy
Forma zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	**Semestr**	6
	20				20			**Punkty ECTS**	**4**
Przedmioty wprowadzające	Sieci komputerowe (INZ1SKO), Sztuczna inteligencja (INZ1SIN),								
Cele przedmiotu	Zapoznanie z metodami zabezpieczania systemów i sieci komputerowych oraz ich testowania pod kątem bezpieczeństwa. Zapoznanie z metodami kryptograficznymi umożliwiającymi zapewnienie poufności i wiarygodności danych cyfrowych.								
Treści programowe	Wykład: 1. Podstawowe pojęcia kryptografii. Kryptografia symetryczna/asymetryczna. 2. Protokół Diffiego-Hellmana. Przykłady szyfrów symetrycznych/asymetrycznych. 3. Usługi sieciowe podnoszące poziom bezpieczeństwa (SSH, SFTP, HTTPS, VPN, etc.). 4. Popularne ataki na systemy i sieci komputerowe (MITM, DoS/DDoS, etc.). 5. Systemy IDS/IPS. 6. Reakcja na incydenty naruszenia systemów ochrony. 7. Anonimizacja połączeń sieciowych. 8. Utwardzanie systemów operacyjnych i sieci komputerowych. 9. Przeprowadzanie testów penetracyjnych. Pracownia specjalistyczna: 1. Implementacja podstawowych modułów kryptograficznych 2. Generatory liczb pseudolosowych. Szyfry strumieniowe. 3. Kryptosystemy symetryczne i asymetryczne. 4. Konfiguracja bezpiecznych usług sieciowych. 5. Testy penetracyjne.								
Metody dydaktyczne	wykład konwersatoryjny, wykład informacyjny, symulacja, metoda projektów, programowanie z użyciem komputera, dyskusja związana z wykładem,								
Forma zaliczenia	Wykład - zaliczenie pisemne. Pracownia specjalistyczna - realizacja zadań praktycznych.								

Symbol efektu uczenia się	**Zakładane efekty uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**
EU1	zna podstawowe algorytmy kryptograficzne oraz potrafi z nich korzystać	K_W05 K_W08 K_U02
EU2	zna podstawowe ataki na sieci komputerowe oraz metody zapobiegania im	K_W08
EU3	zna zasady przeprowadzania testów penetracyjnych oraz potrafi przeprowadzić podstawowe testy	K_W08 K_U08
EU4	zna wybrane usługi podnoszące poziom bezpieczeństwa systemów i sieci komputerowych oraz potrafi je konfigurować	K_W08 K_U08

Symbol efektu uczenia się	**Sposób weryfikacji efektu uczenia się**	**Forma zajęć na której zachodzi weryfikacja**
EU1	zaliczenie pisemne, realizacja zadań praktycznych	W, Ps
EU2	zaliczenie pisemne	W
EU3	zaliczenie pisemne, realizacja zadań praktycznych	W, Ps
EU4	zaliczenie pisemne, realizacja zadań praktycznych	W, Ps

Bilans nakładu pracy studenta (w godzinach)	**Liczba godz.**
Wyliczenie	
1 - Udział w wykładach - 10x2	20
2 - Udział w pracowni specjalistycznej - 10x2	20
3 - Przygotowanie do pracowni specjalistycznej -	3
4 - Opracowanie sprawozdań z pracowni i wykonanie zadań domowych (prac domowych) -	40
5 - Udział w konsultacjach -	2
6 - Przygotowanie do zaliczenia wykładu -	15
RAZEM:	**100**

Wskaźniki ilościowe	**GODZINY**	**ECTS**
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela	42 (5)+(1)+(2)	1.7
Nakład pracy studenta związany z zajęciami o charakterze praktycznym	63 (2)+(4)+(3)	2.5

Literatura podstawowa

1. J.P. Aumasson, Nowoczesna kryptografia: praktyczne wprowadzenie do szyfrowania, PWN, 2018.
2. M. Karbowski, Podstawy kryptografii, Helion, 2014.
3. W. Stallings , L. Brown, Bezpieczeństwo systemów informatycznych. Zasady i praktyka, Helion, 2019.
4. J. Muniz, A. Lakhani, Kali Linux. Testy penetracyjne, Helion, 2014.
5. D. Kennedy, J. O'Gorman, D. Kearns, M. Aharoni, Metasploit. Przewodnik po testach penetracyjnych, Helion, 2013.
6. C. Binnie, Linux Server: bezpieczeństwo i ochrona sieci, Helion, 2017.
7. J. Hutchens, Skanowanie sieci z Kali Linux : receptury : bezpieczeństwo sieci w Twoich rękach!, Helion, 2015.

Literatura uzupełniająca	1. D.E. Robling-Denning, Kryptografia i ochrona danych, WNT, 1993. 2. S. Suehring, Zapory sieciowe w systemie Linux: kompendium wiedzy o nftables, Helion, 2015. 3. K. Mitnick, Sztuka podstępu: łamałem ludzi, nie hasła, Helion, 2016. 4. Netfilter, https://www.netfilter.org 5. Apache project, https://www.apache.org 6. OpenSSH, https://openssh.org 7. OpenVPN, https://openvpn.net 8. Snort, https://www.snort.org 9. Suricata, https://suricata-ids.org	
Jednostka realizująca	Katedra Systemów Informacyjnych i Sieci Komputerowych	**Data opracowania programu**
Program opracował(a)	dr inż. Andrzej Chmielewski	2019.06.05