AKADEMIA WSB				
Kierunek studiów: Bezpieczeństwo Narodowe				
Przedmiot: Metody ataków cyberterrorystycznych				
Profil kształcenia: praktyczny				
Poziom kształcenia: studia II stopnia				
Liczba godzin w semestrze	1		2	
	I	II	III	**IV**
Studia stacjonarne (w/ćw/lab/pr/e)				**22ćw**
Studia niestacjonarne (w/ćw/lab/pr/e)				
JĘZYK PROWADZENIA PRZEDMIOTU	Polski			
WYKŁADOWCA	dr inż. Krystian Mączka			
FORMA ZAJĘĆ	Ćwiczenia			
CELE PRZEDMIOTU	Celem przedmiotu jest zapoznanie studentów z zagrożeniami bezpieczeństwa danych cyfrowych oraz zdobycie umiejętności identyfikacji zagrożeń oraz doboru metod obrony			

Odniesienie do efektów uczenia się		**Opis efektów uczenia się**	**Sposób weryfikacji efektu uczenia się**
Efekt kierunkowy	**PRK**		
WIEDZA			
BN2_W07	P7U_W	Student posiada wiedzę o zagrożeniach w sieci Internet i zagrożeniach systemów komputerowych, które mogą zagrażać systemom w rzeczywistych środowiskach produkcyjnych oraz infrastrukturze krytycznej;	Kolokwium / zadanie praktyczne;
UMIEJĘTNOŚCI			
BN2_U02	P67U_U	Student potrafi analizować poziom bezpieczeństwa systemów informatycznych oraz w razie potrzeby decydować o potrzebie zwiększenie ich bezpieczeństwa;	Kolokwium / zadanie praktyczne;
KOMPETENCJE SPOŁECZNE			
BN2_K03	P7U_K	Ma świadomość istnienia zagrożeń w sieci Internet, podejmuje decyzje w zakresie doboru metod zabezpieczeń;	Kolokwium / zadanie praktyczne;

Nakład pracy studenta (w godzinach dydaktycznych 1h dyd.=45 minut)**

Stacjonarne	**Niestacjonarne**
udział w wykładach =	udział w wykładach =
udział w ćwiczeniach = 22	udział w ćwiczeniach =
przygotowanie do ćwiczeń = 12	przygotowanie do ćwiczeń =
przygotowanie do wykładu =	przygotowanie do wykładu =
przygotowanie do egzaminu = 12	przygotowanie do egzaminu =
realizacja zadań projektowych =	realizacja zadań projektowych =
e-learning =	e-learning =
zaliczenie/egzamin =	zaliczenie/egzamin =
inne (określ jakie) = konsultacje = 4	inne (określ jakie) =
RAZEM:50	**RAZEM:**
Liczba punktów ECTS:2	**Liczba punktów ECTS:**
w tym w ramach zajęć praktycznych:2	**w tym w ramach zajęć praktycznych:**

WARUNKI WSTĘPNE	Podstawowa wiedza z zakresu technologii informatycznych

TREŚCI PRZEDMIOTU (z podziałem na zajęcia w formie bezpośredniej i e-learning)	Treści realizowane w formie bezpośredniej: • Podział i definicje wybranych kategorii zagrożeń • Audyt systemu informatycznego • Zagrożenie systemów informatycznych. Podział i definicje • Ataki DoS i DDoS • Ataki ukierunkowane na uzyskanie dostępu (hacking) • Kradzieże danych i wycieki • Podsłuch sieci teleinformatycznej • Podsłuch komputerowy – aplikacje szpiegujące • Ataki typu ransomware / cryptolocker • Sieć TOR i zagrożenia z nią związane • Anonimizacja ruchu w sieci • Zastosowania kryptografii • Projektowanie bezpieczeństwa poprzez kontrolę dostępu do zasobów • Identyfikacja zasobów informatycznych podlegających ochronie • Analiza i identyfikacja zagrożeń wymierzonych w dany typ zasobów Treści realizowane w formie e-learning
LITERATURA OBOWIĄZKOWA	• Magdalena Molendowska, Rafał Miernik, Bezpieczeństwo w cyberprzestrzeni Wybrane zagadnienia, Wydawnictwo: Adam Marszałek, 2020 • Jakub Kowalewski, Marian Kowalewski, Zagrożenia informacji w cyberprzestrzeni, cyberterroryzm, Oficyna Wydawnicza Politechniki Warszawskiej, 2017
LITERATURA UZUPEŁNIAJĄCA	• Andrzej Podraza Paweł Potakowski Krzysztof Wiak, Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna, Difin ISBN: 978-83-7641-902-2 2013 • Julie Mehan, CyberWar, CyberTerror, CyberCrime and CyberActivism: An i-depth guide to the role of standards in the cybersecurity environment, IT Governance Publishing, 2014
PUBLIKACJE NAUKOWE OSÓB PROWADZĄCYCH ZAJĘCIA ZWIĄZANE Z TEMATYKĄ MODUŁU	• Buchwald P., Rostański M., Mączka K.: Network steganography method for user's identity confirmation in web applications. In: Theoretical and Applied Informatics, vol. 26 – No.3, 4/2014, pp. 179-190 • Gontarz T., Mączka K.: Techniczne i prawne aspekty bycia zapomnianym w sieci Internet („right to be forgotten"), w: Pregiel R., Buchwald P. (ed.): Internet w społeczeństwie informacyjnym. Nowoczesne systemy informatyczne i ich bezpieczenstwo, Wyższa Szkoła Biznesu w Dąbrowie Górniczej, Dąbrowa Górnicza 2014, ISBN: 978-83-62897-90-2, s. 111-122 • Buchwald P., Mączka K., Rostański M.: Pozyskiwanie informacji o użytkownikach portali społecznościowych, w: Kosiński J. (red.): Przestępczość teleinformatyczna 2014, Wydawnictwo Wyższej Szkoły Policji w Szczytnie, Szczytno 2015, ISBN: 978-83-934456-5-3, s. 141-158 • Grzywak A., Mączka K. (red.): Internet w społeczeństwie informacyjnym. Nowoczesne systemy informatyczne i ich bezpieczeństwo, Wyższa Szkoła Biznesu w Dąbrowie Górniczej, Dąbrowa Górnicza 2015, ISBN: ISBN 978-83-64927-41-6 • Mączka K., Peterek P.: Ochrona informacji w prawie karnym na tle elektronicznych zabezpieczeń przed nieuprawnionym do niej dostępem, w: Grzywak A., Mączka K. (red.): Internet w społeczeństwie informacyjnym. Nowoczesne systemy informatyczne i ich bezpieczeństwo, Wyższa Szkoła Biznesu w Dąbrowie Górniczej, Dąbrowa Górnicza 2015, ISBN: ISBN 978-83-64927-41-6, s. 137-146 • Buchwald P., Mączka K., Rostański M.: Metody pozyskiwania informacji o geolokalizacji użytkowników sieci Internet, w: Kosiński J. (red.): Przestępczość teleinformatyczna 2015, Wydawnictwo Wyższej Szkoły Policji w Szczytnie, Szczytno 2015, ISBN: 978-83-7462-506-7, s. 179-192 • Rostański M., Borczyk W., Buchwald P., Duda J., Mączka K., Świtała P.: Bezpieczeństwo technologii mobilnych, w: Projektowanie, zastosowania i rozwój aplikacji mobilnych, Wyższa Szkoła Biznesu w Dąbrowie Górniczej, Dąbrowa Górnicza 2015 • Mączka K., 2018, Zaawansowane techniki informatyki śledczej, Pomiędzy kryminalistyką i procesem karnym. Z zagadnień analizy śledczej Konieczny J. (red.) Wydawnictwo Uniwersytetu Opolskiego, 978–83–7395–780–0, Opole • Mączka K., 2019, Management of Digital Data Security in the Context of Users' Awareness of Computer Attacks, Proceedings of the 34th International Business Information Management Association Conference (IBIMA), 13-14 November 2019 IBIMA Publishing, 978-0-9998551-3-3, Madrid, Spain

METODY NAUCZANIA	W formie bezpośredniej: Wykład multimedialny, dyskusja, burza mózgów W formie e-learning: nie dotyczy
POMOCE NAUKOWE	Rzutnik multimedialny, tablica
PROJEKT	Cel projektu: Temat projektu: Forma projektu:
FORMA I WARUNKI ZALICZENIA	W formie bezpośredniej: Kolokwium

** W-wykład, ćw- ćwiczenia, lab- laboratorium, pro- projekt, e- e-learning*