KARTA KURSU

Nazwa	Analiza zagrożeń komputerowych
Nazwa w j. ang.	Analysis of computer threats

Koordynator	mgr inż. Karolina Baron	Zespół dydaktyczny
		mgr inż. Karolina Baron
Punktacja ECTS*	st. niestacjonarne: 2	

Opis kursu (cele kształcenia)

Celem kursu jest zapoznanie studentów z typowymi zagrożeniami dla bezpieczeństwa w cyberprzestrzeni oraz zrozumienie działania i metod używanych przez hackerów. Ponadto poznanie technik i narzędzi ochrony wraz ze zdobyciem podstawowych umiejętności projektowania i opracowania oraz wdrożenia polityki bezpieczeństwa systemów informatycznych, sieci i aplikacji.

Warunki wstępne

Wiedza	Podstawowe informacje o systemach operacyjnych i sieciach komputerowych.
Umiejętności	Podstawy programowania w dowolnym języku.
Kursy	Wstępne kursy nie są wymagane.

Efekty uczenia się

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Wiedza	W01: zna rodzaje i metody rozpoznawania zagrożeń dla systemów operacyjnych, sieci komputerowych i aplikacji; W02: zna zasady bezpieczeństwa dotyczące wdrożenia i eksploatacji systemów informatycznych oraz mechanizmy ochrony; W03: zna mankamenty i najbardziej narażone elementy na utratę bezpieczeństwa oraz ciągłości działania; W04: zna i rozumie wpływ cyberbezpieczeństwa na świat fizyczny, a przede wszystkim ciągłość pracy infrastruktury krytycznej na wypadek kryzysu;	K_W03 K_W04 K_W07 K_W08 K_W10 K_W12

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Umiejętności	U01: potrafi używać metod i technik zmierzających do podnoszenia bezpieczeństwa systemów, sieci i aplikacji oraz ich pracy; U02: potrafi ocenić architekturę oprogramowania z perspektywy bezpieczeństwa; U03: potrafi identyfikować źródło ryzyka oraz zagrożenia i oszacować jego rozmiary; U04: potrafi podjąć kroki zapobiegawcze przed wystąpieniem zagrożenia oraz w trakcie sytuacji kryzysowej;	K_U02 K_U03 K_U05 K_U06 K_U09 K_U011 K_U013

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Kompetencje społeczne	K01: rozumie potrzebę uczenia ustawicznego i zapoznawania z nowymi trendami oraz zagrożeniami w cyberprzestrzeni; K02: respektuje różnicę w podejściu do zjawisk i zagrożeń w cyberprzestrzeni, wynikające z odmiennych uwarunkowań, dostrzega potrzebę dyskusji naukowych i branżowych; K03: rozumie konieczność aktywności i współdziałania z innymi jednostkami i podmiotami na rzecz utrzymania cyberbezpieczeństwa oraz potrafi ponosić odpowiedzialność za swoją rolę w pracy grupowej oraz cały zespół;	K_K01 K_K02 K_K06 K_K07

Studia niestacjonarne

Organizacja											
Forma zajęć	Wykład (W)	Ćwiczenia w grupach									
		A	K	L	S	P	E				
Liczba godzin				15							

Opis metod prowadzenia zajęć

Konwersatorium, zajęcia laboratoryjne z pracą ćwiczeniową, dyskusja problemowa, analiza problemów typu case study.

Formy sprawdzania efektów uczenia się

	E – learning	Gry dydaktyczne	Ćwiczenia w szkole	Zajęcia terenowe	Praca laboratoryjna	Projekt indywidualny	Projekt grupowy	Udział w dyskusji	Referat	Praca pisemna (esej)	Egzamin ustny	Egzamin pisemny	Inne
W01					X				X				
W02					X				X				
W03					X				X				
W04					X				X				
W05					X				X				
U01					X								
U02					X								
U03					X								
U04					X								
K01					X			X					
K02					X			X					
K03					X			X					

Kryteria oceny	Zaliczenie na podstawie liczby punktów zdobytych łącznie z: prezentacji indywidualnej lub grupowej, testów oraz obecności na zajęciach.

Uwagi	Zajęcia prowadzone w formie zdalnej.

Treści merytoryczne (wykaz tematów)

Dyskusja problemowa dotycząca:
- bezpieczeństwa systemów operacyjnych;
- bezpieczeństwa infrastruktury sieciowej;
- bezpieczeństwa aplikacji;
- zarządzania bezpieczeństwem (polityka i narzędzia);

Szczegółowe omówienie wybranych zagadnień:
- atak na sesję SSL;
- przechwytywanie informacji w sieciach LAN;
- ukrywanie plików i katalogów i podatność Path Traversal;
- przepełnienia stertowe (Heap Overflow);
- ataki ciągiem formatującym (Format String);
- protokół ICMP i wykorzystanie niewidzialnego przesyłania informacji za pośrednictwem sieci;
- skanowanie sieci i Netfilter;
- ataki zdalne;
- spim;
- atak z serwera stron www;
- atak Cross-site scripting (XSS);
- wstrzyknięcie kodu (SQL injection);
- technika cross site tracing (XST);

Wykaz literatury podstawowej

- William Stallings, Lawrie Brown, *Computer Security: Principles and Practice*, Pearson Education, 2018
- William Stallings, *Cryptography and Network Security: Principles and Practice*, Pearson Education, 2017
- Mark Stamp, *Information Security: Principles and Practice*, Wiley, 2011

- David Salomon, *Elements of Computer Security*, Springer-Verlag, 2010
- Michał Szychowiak, *Bezpieczeństwo systemów informatycznych. Zaawansowane ćwiczenia w systemach Windows i Linux*, WPP, 2017
- Quinn Kiser, *Computer Networking and Cybersecurity. A Guide to Understanding Communications Systems, Internet Connections, and Network Security Along with Protection from Hacking and Cyber Security Threats*, 2023

Wykaz literatury uzupełniającej

- Doug Barth, Evan Gilman, *Zero Trust Networks: Building Secure Systems in Untrusted Networks,* O'Reilly Media, 2017
- Lee Brotherston, *Defensive Security Handbook: Best Practices for Securing Infrastructure*, O'Reilly Media, 2017
- Neil Smyth, *Security+ Essentials*, Payload Media, 2012 (http://techotopia.com/index.php?title=Security%2B_Essentials)
- Tim Rains, *Cybersecurity Threats, Malware Trends, and Strategies. Second Edition. Discover risk mitigation strategies for modern threats to your organization,* Published by Packt Publishing Ltd., 2023
- Alyssa Miller, *Cybersecurity Career Guide*, Manning Publications Co., 2022

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) **studia niestacjonarne**

Ilość godzin w kontakcie z prowadzącymi	Wykład	-
	Konwersatorium (ćwiczenia, laboratorium itd.)	15
	Pozostałe godziny kontaktu studenta z prowadzącym	-
Ilość godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	8
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	10
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	-
	Przygotowanie do egzaminu/zaliczenia	7
Ogółem bilans czasu pracy		40
Ilość punktów ECTS w zależności od przyjętego przelicznika		2