

KARTA KURSU

Nazwa	Wykład monograficzny 2
Nazwa w j. ang.	Monograph lecture 2

Koordynator	prof. dr hab. Inż. Mikołaj Karpiński	Zespół dydaktyczny
		prof. dr hab. Inż. Mikołaj Karpiński
Punktacja ECTS*	2	

Opis kursu (cele kształcenia)

Celem kursu jest wprowadzenie studenta we współczesne problemy zabezpieczania:

- a) technologii informatycznych (IT), ze szczególnym uwzględnieniem zagadnień kryptoanalizy;
- b) bezprzewodowych sieci sensorowych (WSN) przed istniejącymi zagrożeniami;
- c) Web aplikacji.

Student poznaje matematyczne podstawy kryptoanalizy, techniki i metody kryptoanalityczne, rodzaje ataków na bezpieczeństwo IT, WSN i Web aplikacje oraz obronę przed nimi.

Warunki wstępne

Wiedza	Wiedza z zakresu analizy numerycznej, tworzenia aplikacji mobilnych, kontroli jakości systemów informatycznych.
Umiejętności	-
Kursy	-

Efekty uczenia się

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Wiedza	W01: zna teoretyczne podstawy bezpieczeństwa technologii informatycznych (IT) i główne obszary związane z bezpieczeństwem IT.	K_W02, K_W10
	W02: zna poziom bezpieczeństwa systemów kryptograficznych i matematyczne podstawy kryptoanalizy.	K_W05, K_W10
	W03: ma wiedzę w zakresie technik i metod kryptoanalitycznych.	K_W02, K_W03, K_W10
	W04: ma wiedzę w zakresie ataków na bezprzewodowe sieci sensorowe (WSN) i Web aplikacje oraz zabezpieczania WSN i Web aplikacji przed nimi.	K_W08
	W05: ma wiedzę w zakresie bezpieczeństwa przed trojanami sprzętowymi.	K_W03, K_W08, K_W10
Umiejętności	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych

	U01: student potrafi swobodnie operować pojęciami nabytymi w trakcie trwania kursu.	K_U03
	U02: student swobodnie potrafi ułożyć zdobyte informacje w ciąg przyczynowo-skutkowy.	K_U09
	U03: student na podstawie nabytych informacji potrafi wskazać mechanizmy istniejące w omawianej na kursie dziedzinie wiedzy.	K_U10
	U04: potrafi korzystać z źródeł dotyczących omawianej tematyki.	K_U11

Kompetencje społeczne	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
	K01: student potrafi w zrozumiały sposób przekazywać nabytą na kursie wiedzę.	K_K01
	K02: student w trakcie dyskusji uczy argumentacji i obrony własnego stanowiska.	K_K05
	K03: student potrafi samodzielnie uzupełniać nabytą w trakcie kursu wiedzę, korzystając zarówno z literatury, jak i źródeł internetowych.	K_K06

Studia stacjonarne

Organizacja											
Forma zajęć	Wykład (W)	Ćwiczenia w grupach									
		A		K		L		S		P	E
Liczba godzin	30										

Studia niestacjonarne

Organizacja											
Forma zajęć	Wykład (W)	Ćwiczenia w grupach									
		A		K		L		S		P	E
Liczba godzin	20										

Opis metod prowadzenia zajęć

studia stacjonarne (dopuszcza się realizację zajęć z wykorzystaniem metod i technik kształcenia na odległość)

Wykład prowadzony w sposób klasyczny, wspomagany metodami audiowizualnymi (w tym filmami dokumentalnymi) i multimedialnymi.

studia niestacjonarne (dopuszcza się realizację zajęć z wykorzystaniem metod i technik kształcenia na odległość)

Wykład prowadzony w sposób klasyczny, wspomagany metodami audiowizualnymi (np. filmami dokumentalnymi) i multimedialnymi.

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				X	
W04							X	X				X	
W05								X				X	
U01							X	X				X	
U02							X	X				X	
U03							X	X				X	
U04							X					X	
K01							X	X				X	
K02							X	X					
K03							X						

Kryteria oceny

Egzamin: dopuszcza się przeprowadzenie egzaminu z zastosowaniem metod i technik kształcenia na odległość.

Uwagi

Treści merytoryczne (wykaz tematów)

1. Podstawy bezpieczeństwa technologii informatycznych (IT): Wstęp. Ewolucja systemów bezpieczeństwa. Główne obszary związane z bezpieczeństwem IT. Ocena kryptograficznych sposobów zabezpieczania IT (metody łamania szyfrów: ze znanym szyfrogramem, ze znanym tekstem jawnym, z wybranym tekstem jawnym, z adaptacyjne wybranym tekstem jawnym, z wybranym szyfrogramem, z wybranym kluczem).
2. Poziomy bezpieczeństwa systemów kryptograficznych. Matematyczne podstawy kryptoanalizy. Techniki i metody kryptoanalityczne.
3. Kryptoanaliza różnicowa algorytmu DES: pojęcia podstawowe, kryptoanaliza różnicowa jednego cyklu algorytmu DES, algorytm DES zredukowany do 4 cykli.
4. Kryptoanaliza liniowa algorytmu DES.
5. Kryptoanaliza algorytmu RSA (przyśpieszenie działania programowych realizacji RSA, bezpieczeństwo zapewniane przez algorytm RSA, atak na algorytm RSA za pomocą wybranych szyfrogramów, atak na algorytm RSA przy wspólnym module, atak na algorytm RSA z małym wykładnikiem szyfrującym, atak na algorytm RSA z małym wykładnikiem deszyfrującym, wnioski z nauki, atak na protokół stosujący szyfrowanie i podpisywanie algorytmem RSA, standardy).
6. Ataki bocznym kanałem.
7. Ataki na bezprzewodowe sieci sensorowe (WSN).
8. Atak odmowy snu a bezpieczeństwo WSN.
9. Atak wielu tożsamości a bezpieczeństwo WSN.
10. Atak przyciągania ruchu na węzle a bezpieczeństwo WSN.
11. Atak mylenia protokołu routingu a bezpieczeństwo WSN.
12. Bezpieczeństwo a trojan sprzętowy.
13. Web bezpieczeństwo.

Wykaz literatury podstawowej

1. Bezpieczeństwo nowoczesnych aplikacji internetowych : przewodnik po zabezpieczeniach / Andrew Hoffman ; przekład: Joanna Zatorska. Gliwice : Helion, 2021.
2. Dotson C.; [tł. P. Fabijańczyk na zlecenie Witkom Witold Sikorski]. Bezpieczeństwo w chmurze : przewodnik po projektowaniu i wdrażaniu zabezpieczeń. Warszawa: Warszawa : Wydawnictwo Naukowe PWN. 2020.
3. Karpiński M. Bezpieczeństwo informacji, Wydawnictwo Pomiar Automatyka Kontrola, Warszawa,

- 2012.
4. LeBlanc J., Messerschmidt T.; [tł. M. Włodarz]: Bezpieczeństwo tożsamości i danych w projektach Web. Warszawa: Wydawnictwo APN Promise, 2016.
5. Messier R.; [tł. A. Watrak]: Kali Linux : testy bezpieczeństwa, testy penetracyjne i etyczne hakowanie, Wydawnictwo Helion, Gliwice, 2019.
6. Wojciechowska-Filipek S., Ciekanowski Z.: Bezpieczeństwo funkcjonowania w cyberprzestrzeni jednostki, organizacji, państwa. Warszawa: Wydawnictwo CeDeWu, 2016.

Wykaz literatury uzupełniającej

1. Hope B., Hope P., Ben Walther B.: Web Security Testing Cookbook: Systematic Techniques to Find Problems Fast, "O'Reilly Media, Inc.", 2009.
2. Kryptografia i bezpieczeństwo sieci komputerowych : matematyka szyfrów i techniki kryptologii / William Stallings ; [tł. Andrzej Grażyński]. Gliwice : Helion, 2012.
3. Long J., Gardner B., Brown J.: Google Hacking for Penetration Testers, Volume 2, Elsevier, 2011.
4. Sieci bezprzewodowe : praktyczny przewodnik / Adam Engst, Glenn Fleishman ; [tł. Adam Jarczyk]. Gliwice : Wydawnictwo Helion, 2005.
5. OWASP Testing Guide v4 (<http://www.slideshare.net/matteomeucci/matteo-meucci-owasp-testing-guide>). The OWASP Testing Guide includes a "best practice" penetration testing framework which users can.
6. Thiel D., Clark C., Dwivedi H.: Mobile Application Security, McGraw-Hill, 2010.
7. Zdziarski J.: Hacking and Securing iOS Applications: Stealing Data, Hijacking Software, and How to Prevent It, "O'Reilly Media, Inc.", 2012.
8. 125 sposobów na bezpieczeństwo sieci / Andrew Lockhart ; [tł.: Leszek Sagalara]. Wyd. 2. Gliwice : Helion, 2007.

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

liczba godzin w kontakcie z prowadzącymi	Wykład	30
	Konwersatorium (ćwiczenia, laboratorium itd.)	
	Pozostałe godziny kontaktu studenta z prowadzącym	5
liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	5
	Opracowanie zadań domowych (problemowych) po zapoznaniu się z niezbędną literaturą przedmiotu	5
	Przygotowanie projektu (praca indywidualna lub w grupie)	5
	Przygotowanie do egzaminu/zaliczenia	
Ogółem bilans czasu pracy		50
Liczba punktów ECTS w zależności od przyjętego przelicznika		2

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

liczba godzin w kontakcie z prowadzącymi	Wykład	20
	Konwersatorium (ćwiczenia, laboratorium itd.)	
	Pozostałe godziny kontaktu studenta z prowadzącym	5
liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	10
	Opracowanie zadań domowych (problemowych) po zapoznaniu się z niezbędną literaturą przedmiotu	10
	Przygotowanie projektu (praca indywidualna lub w grupie)	5
	Przygotowanie do egzaminu/zaliczenia	
Ogółem bilans czasu pracy		50
Liczba punktów ECTS w zależności od przyjętego przelicznika		2