KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Wojna cybernetyczna

Przedmiot

Kierunek studiów
Informatyka

Rok/semestr
1/2

Studia w zakresie (specjalność)
Cyberbezpieczeństwo

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
angielski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład
15

Laboratoria

Inne (np. online)

Ćwiczenia

Projekty/seminaria

Liczba punktów ECTS

1

Wykładowcy

Odpowiedzialny za przedmiot/wykładowca:
mgr inż. Michał Weissenberg
email: michal.weissenberg@put.poznan.pl
tel: 51 665 3946

Wydział Informatyki i Telekomunikacji
Polanka 3, 60-965 Poznań

Odpowiedzialny za przedmiot/wykładowca:
dr hab. inż. Sławomir Hanczewski

email: slawomir.hanczewski@put.poznan.pl

tel:61 665 3946

Faculty of Computing and Telecommunications
Polanka 3, 60-965 Poznań

Wymagania wstępne

Student rozpoczynający ten kurs powinien posiadać podstawową wiedzę z zakresu cyberbezpieczeństwa, sieci teleinformatycznych oraz posiadać podstawowe umiejętności programowania. Powinien także posiadać umiejętność pozyskiwania informacji ze wskazanych źródeł.

Student powinien wykazywać takie cechy jak uczciwość, odpowiedzialność, wytrwałość, ciekawość poznawczą, kreatywność, kulturę osobistą oraz szacunek dla drugiego człowieka.

Cel przedmiotu

1. Zapewnienie studentom teoretycznych podstaw dotyczących pojęcia wojny cybernetycznej.

2. Zapoznanie studentów z teoretycznymi podstawami koncepcji cyberwojowników oraz przykładami rodzajów broni i najnowszymi trendami w zakresie wojny cybernetycznej.

3. Przedstawienie teoretycznych podstaw ataków na sieć komputerową i jej obrony.

4. Wskazanie studentom społecznych, etycznych, prawnych i politycznych aspekty wojny cybernetycznej.

Przedmiotowe efekty uczenia się

Wiedza

Student posiada uporządkowaną i podbudowaną teoretycznie wiedzę ogólną dotyczącą kluczowych zagadnień z zakresu informatyki, w tym analizy systemów operacyjnych. [K2st_W2]

Student ma zaawansowaną wiedzę szczegółową dotyczącą wybranych zagadnień informatycznych i ich zastosowań w analizie ryzyka wojny cybernetycznej. [K2st_W3]

Student zna trendy rozwojowe i najważniejsze przełomowe osiągnięcia w informatyce, w szczególności w zakresie analizy ryzyka wojny cybernetycznej. [K2st_W4]

Student zna podstawowe programy i aplikacje służące do zbierania danych i ich analizy w procesie analizy ryzyka wojny cybernetycznej. [K2st_W6]

Umiejętności

Student potrafi ocenić przydatność i możliwość wykorzystania informacji uzyskanych w analizie literatury i dostępnych w Internecie w obszarze wojny cybernetycznej. [K2st_U1]

Student potrafi ocenić przydatność i możliwość wykorzystania nowych osiągnięć (metod i narzędzi) oraz nowych produktów informatycznych z zakresu cyberbezpieczeństwa. [K2st_U6]

Student potrafi ocenić przydatność oraz możliwość wykorzystania i rozwijania podstawowych narzędzi wykorzystywanych w obszarze analizy zagrożeń związanych z wojną cybernetyczną. [K2st_U8]

Student zna podstawowe pojęcia związane z wojną cybernetyczną i potrafi wykorzystać je do opisu procesu analizy zagrożeń związanych z wojną cybernetyczną. [K2_U12]

Student potrafi definiować etapy dalszego zdobywania wiedzy z zakresu wojny cybernetycznej, a także pozyskiwać informacje na ten temat oraz realizować proces samokształcenia, w tym innych osób w tym zakresie. [K2_U16]

Kompetencje społeczne

Student rozumie, że wiedza i umiejętności szybko się dezaktualizują w zakresie IT, cyberbezpieczeństwa i wojny cybernetycznej. [K2st_K1]

Student rozumie znaczenie wykorzystania najnowszej wiedzy z zakresu informatyki, cyberbezpieczeństwa i kryminalistyki cyfrowej w rozwiązywaniu problemów badawczych i praktycznych. [K2st_K2]

Student rozumie znaczenie działań popularyzujących najnowsze osiągnięcia w dziedzinie wojny cybernetycznej. [K2st_K3]

Student ma świadomość konieczności rozwijania dorobku zawodowego oraz przestrzegania zasad etyki zawodowej. [K2st_K4]

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:
Wykład: wiedza jest weryfikowana poprzez test pisemny i/lub ustny. Ocena zaliczeniowa wynosi 51% punktów, a podczas egzaminu nie wolno używać żadnych materiałów pomocniczych.

Treści programowe

1. Wstęp – pojęcia, definicje, historia i akty związane z wojną cybernetyczną.

2. Cyber Threatscape - metodologia ataków, narzędzia, techniki z opisanymi typami ataków i typami obrony.

3. Pole bitwy w cyberprzestrzeni.

4. Cyberdoktryna, wpływ na system prawny i etyka w różnych krajach.

5. Cyberwojownicy.

6. Rodzaje broni w cyberwojnie - broń logiczna, broń fizyczna, broń psychologiczna.

7. Bezpieczeństwo sieci komputerowych.

Metody dydaktyczne

1. Wykład: prezentacja multimedialna ilustrowana przykładami.

Literatura

Podstawowa

J. Andress and S. Winterfeld, "Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners", 2nd Edition, Syngress, 2013

J. Carr, "Inside Cyber Warfare. Mapping the Cyber Underworld", 2nd Edition, O'Reilly Media,

C. Whyte, B. Mazanec, "Understanding Cyber Warfare. Politics, Policy and Strategy", Routledge 2018

Uzupełniająca

H. H. Dinniss, "Cyber Warfare and the Laws of War", Cambridge University Press, 2014

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	25	1,0
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	15	0,5
Praca własna studenta (studia literaturowe, przygotowanie do egzaminu)[1]	10	0,5

[1] niepotrzebne skreślić lub dopisać inne czynności