

KARTA KURSU

Nazwa	Wojny informacyjne
Nazwa w j. ang.	Information Wars

Koordynator	prof. dr hab. inż. Anna Korchenko	Zespół dydaktyczny
Punktacja ECTS*	Studia stacjonarne: 2 Studia niestacjonarne: 2	prof. dr hab. inż. Anna Korchenko

Opis kursu (cele kształcenia)

Kurs „Wojny informacyjne” ma na celu zapoznanie studentów z podstawowymi pojęciami, strategiami i narzędziami stosowanymi we współczesnych wojnach informacyjnych. Studenci zdobędą wiedzę na temat klasyfikacji wojen informacyjnych, mechanizmów dezinformacji, specyfiki wojen hybrydowych, zastosowania broni informacyjnej oraz ataków socjotechnicznych. Ważnym elementem kursu jest również zapoznanie z modelami grafowymi oraz dużymi modelami językowymi w analizie i modelowaniu procesów informacyjno-psychologicznych. Celem kursu jest rozwinięcie umiejętności analizy, oceny oraz przeciwdziałania operacjom informacyjnym w środowisku cyfrowym i społecznym.

Warunki wstępne

Wiedza	Znajomość analizy matematycznej, algebry, stosowania myślenia oraz podejść algorytmicznych. Rozumienie podstaw bezpieczeństwa systemów informacyjnych, procesów dezinformacyjnych, zasad funkcjonowania mass mediów i sieci społecznościowych w kontekście bezpieczeństwa informacji.
Umiejętności	Umiejętność analizowania przepływów informacyjnych oraz identyfikacji zagrożeń w przestrzeni informacyjnej. Zdolność stosowania metod ochrony informacji i analizy socjotechnicznej, a także samodzielnego korzystania z odpowiedniej literatury z zakresu bezpieczeństwa informacji.
Kursy	Biały wywiad

Efekty uczenia się

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Wiedza	<p>Po zakończeniu kursu student:</p> <p>W01: Student zna mechanizmy dezinformacji oraz potrafi rozróżniać jej główne rodzaje i zastosowania w ramach współczesnych wojen hybrydowych.</p> <p>W02: Student posiada wiedzę o atakach socjotechnicznych – rozumie wektory tych ataków, ich wpływ na bezpieczeństwo informacyjne oraz powiązania z wojnami informacyjnymi.</p> <p>W03: Student zna podstawowe metody budowy i analizy modeli sieciowych (grafowych i semantycznych) oraz ich zastosowanie do badania i modelowania procesów informacyjno-psychologicznych.</p>	K_W01 K_W07 K_W09

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Umiejętności	<p>Po zakończeniu kursu student:</p> <p>U01: potrafi identyfikować i analizować operacje informacyjne z wykorzystaniem modelu OODA oraz rozpoznawać schematy działań przeciwnika w cyberprzestrzeni.</p> <p>U02: modelować kampanie phishingowe, analizować stosowane w nich pułapki poznawcze i rozpoznawać fałszywe strony internetowe jako elementy wojny informacyjnej.</p> <p>U03: stosować wybrane narzędzia sztucznej inteligencji i dużych modeli językowych w analizie i modelowaniu procesów informacyjno-psychologicznych.</p>	K_U06 K_U09 K_U10

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Kompetencje społeczne	<p>Po zakończeniu kursu student:</p> <p>K01: krytycznej oceny poziomu swojej wiedzy oraz ciągłego dokształcania się i konsultacji z innymi ekspertami z branży IT w szczególności związanej z cyberbezpieczeństwem, a także planowania własnego rozwoju zawodowego.</p>	K_K02

Studia stacjonarne

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

Studia niestacjonarne

Organizacja											
Forma zajęć	Wykład (W)	Ćwiczenia w grupach									
		A		K		L		S		P	E
Liczba godzin	10	10									

Opis metod prowadzenia zajęć

1. Wykłady: Podczas wykładów prowadzący przedstawiają materiał teoretyczny, wyjaśniają kluczowe koncepcje i metody oraz prezentują przykłady, ilustracje, slajdy i filmy. Wykłady mogą być prowadzone w auli lub online, a nagrania z nich mogą być udostępniane do późniejszego obejrzenia.
2. Ćwiczenia laboratoryjne: Ćwiczenia laboratoryjne pozwalają studentom przeprowadzać praktyczne eksperymenty z rzeczywistymi danymi, które pomagają studentom utrwalić wiedzę teoretyczną.
3. Dyskusje i zadania grupowe: Dyskusje i zadania grupowe promują wymianę wiedzy między studentami i zachęcają do wspólnego uczenia się. Metody te mogą obejmować forum dyskusyjne, grupowe projekty oraz wspólne rozwiązywanie zadań.

4. Samodzielne uczenie się: Dodatkowo, studentom mogą być udostępniane materiały do samodzielnego uczenia się, takie jak podręczniki, artykuły i kursy online. To pozwala studentom na pogłębienie swojej wiedzy i badanie tematów, które ich szczególnie interesują.

5. Testy i ocena: W trakcie kursu studenci mogą przechodzić testy i prace kontrolne w celu oceny swojego poziomu wiedzy i osiągnięć. Oceny te mogą obejmować zarówno egzaminy pisemne, jak i ocenę wyników ćwiczeń laboratoryjnych.

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		X			X					
W02	X		X		X			X					
W03	X		X		X			X					
U01	X		X		X			X					
U02	X		X		X			X					
U03	X		X		X			X					
K01	X		X		X			X					

Kryteria oceny	<p>Ocena końcowa jest zależna od ocen cząstkowych, systematyczności realizowanych zadań oraz oceny uzyskanej za realizację projektu zespołowego (indywidualnego). W szczególności ocenę dobrą i bardzo dobrą z ćwiczeń może uzyskać student, który: na podstawie zdobytej wiedzy potrafi samodzielnie wykorzystywać metody kryptograficzne do pracy w systemach zdecentralizowanych oraz stosować nowoczesne podejścia i zasady systemów blockchain.</p> <p>Audytorium Student jest oceniany za:</p> <ul style="list-style-type: none"> - Aktywność na zajęciach - ocenie podlega zaangażowanie w przebieg zajęć, w tym rozwiązywanie zadań przy tablicy oraz umiejętność poprawnego przytaczania definicji i metod adekwatnych do rozwiązywanych problemów. - Kolokwia (test) - obejmują zarówno zadania praktyczne, jak i teoretyczne, które wymagają zastosowania poznanych definicji oraz właściwego wykorzystania metod omawianych podczas kursu. <p>Wykład Obecność na wykładach jest obowiązkowa i stanowi warunek zaliczenia wykładu.</p> <p>Zaliczenie Studenci, którzy pomyślnie ukończyli zarówno wykłady, jak i zajęcia praktyczne, są dopuszczani do końcowego zaliczenia. Zaliczenie jest formą końcowej oceny poziomu przyswojonej wiedzy oraz nabytych umiejętności studenta.</p> <p>Skala ocen: ocena 2.0 — [0%, 50%] ocena 3.0 — (50%, 60%] ocena 3.5 — (60%, 70%] ocena 4.0 — (70%, 80%] ocena 4.5 — (80%, 90%] ocena 5.0 — (90%, 100%]</p>
Uwagi	Brak

Treści merytoryczne (wykaz tematów)

- Temat 1. Pojęcie i metody wojny informacyjnej
- Temat 2. Dezinformacja jako element wojny hybrydowej
- Temat 3. Szczególne cechy i metody zastosowania broni informacyjnej
- Temat 4. Ataki socjotechniczne w strategiach wojen informacyjnych
- Temat 5. Rola białego wywiadu w wojnach informacyjnych
- Temat 6. Modele grafowe i duże modele językowe w badaniach i modelowaniu wojen informacyjnych
- Temat 7. Metody budowy modeli sieciowych w badaniach wojen informacyjnych

Wykaz literatury podstawowej

1. Kachynskiy, A. B., Lande, D. V., & Novikov, O. M. (2025). *Teoretyko-grafovi modeli informatsiino-psychologichnykh viin. Modeliuvannya mentalnoi viiny iz zastosuvanniam heneratyvnoho shuchnoho intelektu: Navchalnyi posibnyk dlia zdobuvachiv stupeniv mahistra ta PhD za spets. 125 "Kiberbezpeka ta zakhyst informatsii"*. Kyiv: KPI im. Ihorii Sikorskoho.
2. Janczewski, Robert Adam. *Cyberwalka. Militarny wymiar działań*. Warszawa: Wydawnictwo Naukowe PWN, 2023. 444 s. ISBN: 978-83-01-23085-2.
3. Olejnik, Łukasz. *Propaganda: od dezinformacji i wpływu do operacji i wojny informacyjnej*. Warszawa: Wydawnictwo Naukowe PWN, 2022. Seria „Bezpieczeństwo”.
4. Pietras, M. (2021). Wojna informacyjna jako współczesne narzędzie działań nieregularnych. *Cybersecurity and Law*, 6(2), 21–41. <https://doi.org/10.35467/cal/146454>
5. Janczewski, R., & Janczewski, A. (Eds.). (2021). *Cyberbezpieczeństwo teoretycznie i empirycznie w naukach o bezpieczeństwie*. Gdynia: Wydawnictwo BP. ISBN 978-83-65763-50-1.

Wykaz literatury uzupełniającej

1. Wasiuta, O., & Wasiuta, S. (Eds.). (2021). *Encyklopedia bezpieczeństwa* (Vol. 1: A–C). Kraków: Wydawnictwo Libron. ISBN 978-83-66269-49-1.
2. Wasiuta, O., & Wasiuta, S. (Eds.). (2021). *Encyklopedia bezpieczeństwa* (Vol. 2: D–K). Kraków: Wydawnictwo Libron. ISBN 978-83-66269-49-1
3. Wasiuta, O., & Wasiuta, S. (Eds.). (2021). *Encyklopedia bezpieczeństwa* (Vol. 3: L–R). Kraków: Wydawnictwo Libron. ISBN 978-83-66269-49-1
4. Wasiuta, O., & Wasiuta, S. (Eds.). (2021). *Encyklopedia bezpieczeństwa* (Vol. 4: S–Ż). Kraków: Wydawnictwo Libron. ISBN 978-83-66269-49-1

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

liczba godzin w kontakcie z prowadzącymi	Wykład	15
	Konwersatorium (ćwiczenia, laboratorium itd.)	15
	Pozostałe godziny kontaktu studenta z prowadzącym	5
liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	5
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	0
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	0
	Przygotowanie do egzaminu/zaliczenia	10
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	10
	Konwersatorium (ćwiczenia, laboratorium itd.)	10
	Pozostałe godziny kontaktu studenta z prowadzącym	5
liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	15
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	0
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	0
	Przygotowanie do egzaminu/zaliczenia	10
Ogółem bilans czasu pracy		50
Liczba punktów ECTS w zależności od przyjętego przelicznika		2