

KARTA KURSU

Nazwa	Wykład monograficzny 1
Nazwa w j. ang.	Monograph lecture 1

Koordynator	dr hab. prof. UKEN Serhii Semenov	Zespół dydaktyczny
		dr hab. prof. UKEN Serhii Semenov
Punktacja ECTS*	3	

Opis kursu (cele kształcenia)

Celami kursu są: 1. Przedstawienie podstawowych zasad i koncepcji cyberbezpieczeństwa. 2. Zapoznanie z głównymi aspektami ochrony informacji i danych w obszarze bezpieczeństwa cyfrowego. 3. Studiowanie strategii i metod zapobiegania cyberataków, w tym środków technicznych i organizacyjnych. 4. Określenie roli i odpowiedzialności specjalistów w zakresie zapewnienia cyberbezpieczeństwa we współczesnym społeczeństwie informacyjnym.

Studenci mogą nabyć następujące umiejętności: 1. Umiejętność analizowania współczesnych zagrożeń i wyzwań związanych z cyberbezpieczeństwem. 2. Opanowanie strategii i metod zapobiegania atakom cybernetycznym, w tym środków technicznych i organizacyjnych. 3. Praktyczne stosowanie narzędzi i technik zapewnienia bezpieczeństwa w środowisku cyfrowym. Kurs jest realizowany w języku polskim.

Warunki wstępne

Wiedza	Podstawowe zasady i koncepcji cyberbezpieczeństwa, pojęcia i definicje polityki bezpieczeństwa, zasady budowy profilu ochrony informacji w celu zapewnienia usług bezpieczeństwa. Znajomość i umiejętność korzystania z mechanizmów i protokołów zapewnienia poufności, zapewnienia autentyczności (dostępności) oraz integralności danych.
Umiejętności	Umiejętność analizowania metod cyberbezpieczeństwa w organizacji kompleksowych systemów ochrony danych. Wykorzystanie metod kryptograficznych do badania współczesnych protokołów i procedur zapewnienia podstawowych usług bezpieczeństwa zgodnie ze standardami ISO-7498-2, ISO/IEC 10181.
Kursy	Metody badawcze w informatyce

Efekty uczenia się

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Wiedza	Po zakończeniu kursu student: ma pogłębioną wiedzę na temat zasad działania współczesnych mechanizmów i narzędzi kryptograficznych oraz ich roli w zapewnianiu bezpieczeństwa systemów i sieci komputerowych.	K_W06, K_W08
	zna architekturę oraz mechanizmy bezpieczeństwa w sieciach komputerowych, systemach serwerowych i rozwiązaniach chmurowych, w tym wybrane standardy i protokoły z zakresu cyberbezpieczeństwa.	K_W06

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Umiejętności	Po zakończeniu kursu student: bada, opracowuje, wdraża i stosuje metody i środki kryptograficzne ochrony informacji potrafi analizować i projektować protokoły, sieci i systemy teleinformatyczne, stosując właściwe metody, techniki i narzędzia oraz biorąc pod uwagę aspekty związane z bezpieczeństwem ich użytkowania	K_U02, K_U05 K_U04

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Kompetencje społeczne	Po zakończeniu kursu student: potrafi formułować opinie na temat zagadnień związanych z branżą informatyczną ze szczególnym uwzględnieniem aspektów cyberbezpieczeństwa.	K_K02

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

1 Wykłady: Podczas wykładów wykładowcy wprowadzają materiał teoretyczny, wyjaśniają kluczowe pojęcia i metody oraz przedstawiają przykłady i ilustracje. Wykłady mogą być prowadzone w klasie lub online, a nagrania wykładów mogą być udostępniane do późniejszego przeglądania.

2. Dyskusje grupowe i zadania: dyskusje grupowe i zadania ułatwiają dzielenie się wiedzą między studentami i zachęcają do wspólnego uczenia się. Metody te mogą obejmować fora dyskusyjne, projekty grupowe i wspólne rozwiązywanie problemów.

3 Samodzielna nauka: Studenci mogą również mieć dostęp do materiałów do samodzielnej nauki, takich jak podręczniki, artykuły i kursy online. Pozwala to uczniom na pogłębienie wiedzy i zbadanie tematów, które ich szczególnie interesują.

4. Testy i ocena: w trakcie kursu uczniowie mogą brać udział w testach i quizach w celu oceny ich poziomu wiedzy i osiągnięć. Oceny te mogą obejmować zarówno egzaminy pisemne, jak i oceny projektów i laboratoriów.

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		
W03								X			X		
U01								X			X		
U04								X			X		
K01								X			X		

Kryteria oceny	Ocena końcowa zależy od ocen częściowych, regularności wykonywania zadań oraz oceny otrzymanej za projekt zespołowy (indywidualny). W szczególności ocenę dobrą i bardzo dobrą z zadań może uzyskać student, który: - samodzielnie tworzy oprogramowanie wykorzystujące rozważane metody steganograficznej ochrony danych, - potrafi analizować uwarunkowania i obszary stosowalności badanych algorytmów
----------------	---

Uwagi	
-------	--

Treści merytoryczne (wykaz tematów)

<p>Temat 1. Podstawowe pojęcia i definicje cyberbezpieczeństwa</p> <p>Temat 2. Podstawy kryptografii. Proste algorytmy szyfrowania</p> <p>Temat 3. Algorytmy kryptograficzne z kluczem</p> <p>Temat 4. System PGP. Schemat działania</p> <p>Temat 5. System PGP. Zasady stosowania i algorytmy działania</p> <p>Temat 6. Integralność danych. Algorytm Hamminga</p> <p>Temat 7. Zarządzanie dostępem.</p> <p>Temat 8. Protokoły uwierzytelniania</p> <p>Temat 9. Podpisy cyfrowe</p> <p>Temat 10. Ochrona antywirusowa SPAMu. Metody zwalczania SPAMu</p> <p>Temat 11. Translacja adresów sieciowych. Kompleksowe wykorzystanie translacji adresów sieciowych</p> <p>Temat 12. IPSec.</p> <p>Temat 13. Przeszłość i nowoczesne technologie klucza dla aplikacji internetowych</p> <p>Temat 14. Zbieranie informacji o aplikacjach internetowych</p> <p>Temat 15. Sieci standardu 802.11. Zapewnienie usług bezpieczeństwa.</p>
--

Wykaz literatury podstawowej

<p>1. Stinson, D. R.; Paterson, M. B. <i>Kryptografia. W teorii i praktyce</i>. Warszawa: Wydawnictwo Naukowe PWN, 2021. ISBN 978-83-01-21667-2.</p> <p>2. Kurose, J. F.; Ross, K. W. <i>Sieci komputerowe. Ujęcie całościowe. Wydanie VII</i>. Gliwice: Helion, 2018. ISBN 978-83-289-2935-7.</p> <p>3. Muravskiy, Volodymyr. <i>Accounting and Cybersecurity: Monograph</i>. Scientific Editor – Z.-M. Zadorozhnyi. Kindle Publishing, KDP, Seattle. USA. 2021. 200 p.</p>
--

Wykaz literatury uzupełniającej

<p>1. Semenov Serhii. <i>Data protection in computerised control systems (monograph)</i> LAP LAMBERT Academic Publishing Saarbrücken, Germany, 2014</p> <p>2. Semenov, S.; Krupska-Klimczak, M.; Wasiuta, O.; Krzaczek, B.; Mieczkowski, P.; Głowacki, L.; Yu, J.; He, J.; Chernykh, O. Intelligent Assurance of Resilient UAV Navigation Under Visual Data Deficiency for Sustainable Development of Smart Regions. <i>Sustainability</i> 2025, 17, 6030. https://doi.org/10.3390/su17136030</p> <p>3. Leroy, I.; Zolotaryova, I.; Semenov, S. Impact of Critical Infrastructure Cyber Security on the Sustainable Development of Smart Cities: Insights from Internal Specialists and External Information Security</p>
--

Auditors. *Sustainability* 2025, 17, 1188. <https://doi.org/10.3390/su17031188>
 4. Semenov, S.; Krupska-Klimczak, M.; Mazurek, P.; Zhang, M.; Chernikh, O. Improving Unmanned Aerial Vehicle Security as a Factor in Sustainable Development of Smart City Infrastructure: Automatic Dependent Surveillance–Broadcast (ADS-B) Data Protection. *Sustainability* 2025, 17, 1553. <https://doi.org/10.3390/su17041553>

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

liczba godzin w kontakcie z prowadzącymi	Wykład	30
	Pozostałe godziny kontaktu studenta z prowadzącym	10
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	5
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	10
	Przygotowanie do egzaminu/zaliczenia	10
Ogółem bilans czasu pracy		70
Liczba punktów ECTS w zależności od przyjętego przelicznika		3

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

liczba godzin w kontakcie z prowadzącymi	Wykład	15
	Pozostałe godziny kontaktu studenta z prowadzącym	10
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	10
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	10
	Przygotowanie do egzaminu/zaliczenia	10
Ogółem bilans czasu pracy		70
Liczba punktów ECTS w zależności od przyjętego przelicznika		3