

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	Kontrola jakości systemów informatycznych

Efekty uczenia się

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Wiedza	Po zakończeniu kursu student: Posiada pogłębioną wiedzę na temat bezpieczeństwa sieci komputerowych, w tym technologii takich jak IPSec, translacja adresów, mechanizmy zapobiegania SPAM-owi i ochrony antywirusowej.	K_W06
	Ma pogłębioną wiedzę na temat metod, technik i narzędzi stosowanych w projektowaniu i analizie zabezpieczeń danych, w tym algorytmów kryptograficznych, systemów uwierzytelniania i podpisów cyfrowych.	K_W08

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Umiejętności	Po zakończeniu kursu student: Potrafi zaprojektować i skonfigurować bezpieczne sieci komputerowe z uwzględnieniem protokołów uwierzytelniania, translacji adresów i standardów 802.11. Projektuje i wdraża systemy informatyczne z uwzględnieniem mechanizmów ochrony danych, w tym stosowania algorytmów kryptograficznych (PGP, algorytmy symetryczne i asymetryczne, Hamming, podpisy cyfrowe).	K_U04 K_U07

	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 cząstkowych, 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)

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

Wykaz literatury podstawowej

1. Semenov Serhii. Data protection in computerised control systems (monograph) LAP LAMBERT Academic Publishing Saarbrücken, Germany, 2014
2. Muravskiy, Volodymyr. Accounting and Cybersecurity: Monograph. Scientific Editor – Z.-M. Zadorozhnyi. Kindle Publishing, KDP, Seattle. USA. 2021. 200 p.

Wykaz literatury uzupełniającej

1. S. Semenov, Z. Liqiang and C. Weiling, "Penetration Testing Process Mathematical Model," 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, Ukraine, 2020, pp. 142-146, doi: 10.1109/PICST51311.2020.9468039.
2. Serhii Semenov, Viacheslav Davydov, Oksana Lipchanska, Maksym Lipchanskyi Development of unified mathematical model of programming modules obfuscation process based on graphic evaluation and review method // Eastern-european journal of enterprise technologies.– Kharkiv. 2020 Вип. 3/2(105). P.6-16
3. S. Semenov, V. Davydov, N. Kuchuk and I. Petrovskaya, "Software security threat research," 2021 XXXI International Scientific Symposium Metrology and Metrology Assurance (MMA), Sozopol, Bulgaria, 2021, pp. 1-4, doi: 10.1109/MMA52675.2021.9610877.

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