



Bezpieczeństwo informacji Karta opisu przedmiotu (sylabus)

Informacje podstawowe

<p>Kierunek studiów Informatyka i analityka danych</p> <p>Specjalność Technologie informacyjne w biznesie</p> <p>Jednostka organizacyjna UEP</p> <p>Poziom kształcenia studia pierwszego stopnia (licencjackie)</p> <p>Forma studiów stacjonarne</p> <p>Profil kształcenia ogólnoakademicki</p>	<p>Cykl dydaktyczny 2025/2026</p> <p>Kod przedmiotu UEPIADTIBS.110C.6222.25</p> <p>Język wykładowy Polski</p> <p>Obligatoryjność Obowiązkowy</p> <p>Blok zajęciowy Blok C</p>	
<p>Osoba odpowiedzialna za treść sylabusu</p>	<p>Adam Wójtowicz</p>	
<p>Okres Semestr 5</p>	<p>Forma zaliczenia Zaliczenie</p> <p>Forma prowadzenia i godziny zajęć • Uczestnictwo w wykładach: 30</p>	<p>Liczba punktów ECTS 3</p>

Cele uczenia się dla przedmiotu

C1	Uświadomienie wyzwań związanych z cyberatakami oraz innymi zagrożeniami bezpieczeństwa informacji w warunkach transformacji cyfrowej
C2	Uzyskanie wiedzy na temat sposobu działania narzędzi oraz technologii podwyższających poziom bezpieczeństwa informacji, a także rozwijanie umiejętności łączenia zagrożeń z odpowiednimi technologiami zabezpieczającymi
C3	Rozwinięcie umiejętności oceny wpływu nowych technologii na bezpieczeństwo informacji, a także na prywatność użytkowników usług internetowych
C4	Uzyskanie wiedzy na temat zasad projektowania i implementacji bezpiecznego oprogramowania
C5	Wykształcenie umiejętności zarządzania ryzykami związanymi z bezpieczeństwem informacji

Cele kształcenia UEP

Kod	Treść celu
CS1_1.1	student rozumie strukturę i elementy problemu gospodarczego
CS1_1.2	student właściwie wykorzystuje techniki, metody i modele analityczne
CS1_2.1	student rozumie i stosuje zasady pracy grupowej
CS1_2.2	student skutecznie komunikuje się w formie ustnej i pisemnej
CS1_3.1	student rozumie i docenia zasady zrównoważonego rozwoju i ich zastosowanie w biznesie
CS1_3.2	student stosuje etyczne standardy akademickie i biznesowe, uwzględniając aspekty środowiskowe i społeczne

Wymagania wstępne

Technologie informacyjne, Programowanie obiektowe

Efekty uczenia się dla przedmiotu

Kod	Efekty w zakresie	Kierunkowe efekty uczenia się	Metody weryfikacji
Wiedzy			
W1	Wyjaśnia pojęcia z dziedziny bezpieczeństwa informacji	K1_W01, K1_W03, K1_W04, K1_W05, K1_W06	Quiz na platformie moodle
W2	Rozumie sposób działania i klasyfikuje cyberataki oraz inne zagrożenia bezpieczeństwa informacji	K1_W01, K1_W03, K1_W04, K1_W05, K1_W06	Esej / referat, Quiz na platformie moodle
W3	Rozumie sposób działania i kategoryzuje narzędzia oraz technologie zwiększające poziom bezpieczeństwa	K1_W01, K1_W03, K1_W04, K1_W06	Esej / referat, Quiz na platformie moodle
W4	Zna zasady projektowania i implementacji bezpiecznego oprogramowania	K1_W01, K1_W03, K1_W04, K1_W05, K1_W06	Esej / referat, Quiz na platformie moodle
Umiejętności			
U1	Łączy zagrożenia bezpieczeństwa informacji z odpowiednimi technologiami zabezpieczającymi	K1_U01, K1_U02, K1_U03, K1_U04, K1_U05, K1_U06	Esej / referat, Quiz na platformie moodle
U2	Przeprowadza analizę ryzyka związanego z bezpieczeństwem informacji	K1_U01, K1_U02, K1_U03, K1_U04, K1_U05, K1_U06	Esej / referat, Quiz na platformie moodle
U3	Ocenia wpływ zastosowania poszczególnych technologii na bezpieczeństwo informacji	K1_U01, K1_U02, K1_U03, K1_U04, K1_U05, K1_U06	Esej / referat, Quiz na platformie moodle
U4	Stosuje zasady projektowania bezpiecznego oprogramowania	K1_U01, K1_U02, K1_U03, K1_U04, K1_U05, K1_U06	Esej / referat, Quiz na platformie moodle
Kompetencji społecznych			
K1	Wykazuje odpowiedzialność za zapewnienie bezpieczeństwa informacji w przedsiębiorstwach i administracji	K1_K01, K1_K02, K1_K03, K1_K04, K1_K05	Esej / referat

Kod	Efekty w zakresie	Kierunkowe efekty uczenia się	Metody weryfikacji
K2	Docenia wagę problemów związanych z zapewnieniem prywatności użytkowników w gospodarce elektronicznej	K1_K01, K1_K02, K1_K03, K1_K04, K1_K05	Esej / referat
K3	Podejmuje wyzwania związane z nowymi technologiami wpływającymi na bezpieczeństwo informacji i prywatność użytkowników	K1_K01, K1_K02, K1_K03, K1_K04, K1_K05	Esej / referat

Treści programowe

Lp.	Treści programowe	Cele kształcenia dla przedmiotu	Efekty uczenia się dla przedmiotu
1.	Bezpieczeństwo informacji - podstawowe pojęcia z zakresu bezpieczeństwa informacji, kontroli dostępu i kryptografii	C1, C2, C5	W1, U1, K1, K2
2.	Wyzwania związane z praktycznym zapewnieniem bezpieczeństwa informacji w przedsiębiorstwie	C1, C2, C3, C5	W2, W3, U3, K1, K2, K3
3.	Włamania do systemów informatycznych i ataki sieciowe	C1, C2, C3, C5	W1, W2, W3, U1, U3, K1
4.	Ataki na użytkowników końcowych i socjotechniki	C1, C2, C3, C5	W1, W2, W3, U1, U3, K1, K2
5.	Prywatność użytkowników systemów informatycznych	C1, C2, C3, C5	W1, W2, W3, W4, U1, U3, K1, K2, K3
6.	Filtrowanie treści	C1, C2, C3, C5	W2, W3, W4, U1, U3, K1, K2, K3
7.	Bezpieczeństwo w procesie rozwoju oprogramowania	C1, C2, C3, C4, C5	W2, W3, W4, U1, U2, U3, U4, K1, K2, K3
8.	Zarządzanie ryzykami związanymi z przechowywaniem, przesyłaniem i przetwarzaniem informacji	C1, C2, C3, C5	W1, W2, W3, U1, U2, U3, K1, K3
9.	Przetwarzanie w chmurze - wyzwania bezpieczeństwa	C1, C2, C3, C5	W2, W3, U1, U2, U3, K1, K2, K3
10.	Internet rzeczy - wyzwania bezpieczeństwa	C1, C2, C3, C4, C5	W2, W3, W4, U1, U2, U3, U4, K1, K2, K3
11.	Sztuczna inteligencja, uczenie maszynowe - wyzwania bezpieczeństwa	C1, C2, C3, C4, C5	W2, W3, W4, U1, U2, U3, U4, K1, K2, K3
12.	Bezpieczeństwo procesów uwierzytelniania użytkownika i autoryzacji transakcji. Zarządzanie kluczami kryptograficznymi	C2, C3, C4	W3, W4, U1, U3, U4, K1, K3
13.	Zabezpieczenia biometryczne: linie papilarne, twarz, głos, tęczęwka, biometria naczyniowa, biometria behawioralna; uwierzytelnianie ciągłe, adaptacyjne, kontekstowe; obszary zastosowań i ograniczenia technologii biometrycznych	C2, C3, C4	W3, W4, U1, U3, U4, K1, K3

Literatura

Obowiązkowa

1. Conklin, A., White, G., Cothren, C., Davis, R., Williams, D. (2022). Principles of Computer Security, CompTIA Security+ and Beyond, 6th ed., McGraw-Hill
2. OWASP Foundation. (2024). OWASP Projects, <https://owasp.org/projects/>

Zalecana

1. Vacca, J.R. (2017). Computer and Information Security Handbook, 3rd ed., Morgan Kaufmann
2. Whitman, M.E., Mattord, H. (2018). Management of Information Security, 6th ed., Cengage Learning

Informacje rozszerzone

Metody nauczania:

Burza mózgow, Wykład z prezentacją multimedialną, Dyskusja, Metody e-learningowe

Metody nauczania	Sposób zaliczenia	Warunki zaliczenia przedmiotu
Wykład	Esej / referat, Quiz na platformie moodle	Warunkiem zaliczenia przedmiotu jest uzyskanie co najmniej 50 punktów na 100 możliwych. Punkty są przyznawane za raporty tematyczne pisane podczas całego semestru oraz za test końcowy z wykładanych treści.

Rozliczenie punktów ECTS

Forma aktywności studenta	Średnia liczba godzin* przeznaczonych na zrealizowane aktywności	
Uczestnictwo w wykładach	30	
Przygotowanie referatu	20	
Przygotowanie do sprawdzianu/ kolokwium	20	
Zbieranie informacji do zadanej pracy	18	
Konsultacje z prowadzącym/i zajęcia	2	
Łączny nakład pracy studenta	Liczba godzin 90	ECTS 3.0
Zajęcia z bezpośrednim udziałem nauczyciela	Liczba godzin 32	ECTS 1.0

* godzina (lekcyjna) oznacza 45 minut

Kierunkowe efekty uczenia się

Kod	Treść
K1_K01	absolwent jest gotów do obiektywnej, krytycznej oceny swojej wiedzy i umiejętności
K1_K02	absolwent jest gotów do myślenia i działania w sposób przedsiębiorczy
K1_K03	absolwent jest gotów do uczestnictwa w rozwiązywaniu współczesnych problemów z zakresu zrównoważonego rozwoju wynikających z masowego zastosowania nowych technologii, w szczególności do dbania o środowisko naturalne i etykę biznesową
K1_K04	absolwent rozumie społeczne, prawne i etyczne aspekty pracy z danymi, w tym związane z ochroną prywatności i bezpieczeństwem informacji
K1_K05	absolwent jest gotów do kierowania się uczciwością intelektualną w działaniach własnych i wymagania jej od innych osób, jest wyczulony na kwestie plagiatu, auto-plagiatu i wykorzystania sztucznej inteligencji z poszanowaniem zasad etyki
K1_U01	absolwent potrafi poprawnie dobrać i efektywnie wykorzystywać metody i narzędzia ilościowe i informatyczne do opisu i analizy zjawisk społeczno-gospodarczych
K1_U02	absolwent potrafi właściwie dobierać źródła informacji, dokonywać ich oceny oraz przeprowadzać krytyczną analizę i syntezę danych z różnych źródeł, w celu wyciągania trafnych wniosków i podejmowania optymalnych decyzji w warunkach nie w pełni przewidywalnych
K1_U03	absolwent potrafi w sposób precyzyjny i spójny wyrażać myśli i poglądy, zaprezentować wyniki swojej pracy oraz brać udział w debacie z poszanowaniem opinii i stanowisk innych osób
K1_U04	absolwent potrafi posługiwać się językiem obcym w zakresie nauk społeczno-gospodarczych zgodnie z wymogami określonymi dla poziomu B2 Europejskiego Systemu Opisu Kształcenia Językowego
K1_U05	absolwent potrafi planować i organizować pracę indywidualną oraz zespołową zorientowaną na rozwiązywanie specjalistycznych problemów
K1_U06	absolwent jest gotów do systematycznego podnoszenia swoich kompetencji poprzez ciągłe samokształcenie w oparciu o zaawansowaną literaturę specjalistyczną
K1_W01	absolwent zna w zaawansowanym stopniu szeroki wachlarz metod ilościowych oraz narzędzi informatycznych stosowanych w analizach zjawisk społeczno-gospodarczych
K1_W03	absolwent zna i rozumie najnowsze trendy rozwojowe i osiągnięcia z zakresu informatyki i analizy danych
K1_W04	absolwent zna i rozumie podstawy prawa, ochrony własności i prawa autorskiego, a także prawa i etyki w zakresie stosowania nowoczesnych technologii informacyjnych z uwzględnieniem wykorzystania sztucznej inteligencji
K1_W05	absolwent zna i rozumie zasady tworzenia i rozwoju różnych form przedsiębiorczości, w szczególności opartych na wykorzystaniu nowoczesnych technologii informacyjno-komunikacyjnych
K1_W06	absolwent zna i rozumie dylematy związane z transformacją cyfrową oraz potrzebą uwzględnienia zasad zrównoważonego rozwoju w działalności gospodarczej

Ten utwór jest dostępny na licencji Creative Commons Uznanie autorstwa 4.0 Międzynarodowa (CC BY 4.0). Autor: Adam Wójtowicz