KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Przygotowanie pracy dyplomowej [S1Cybez1>PPD]

Przedmiot

Kierunek studiów
Cyberbezpieczeństwo

Rok/Semestr
4/7

Studia w zakresie (specjalność)
–

Profil studiów
ogólnoakademicki

Poziom studiów
pierwszego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obligatoryjny

Liczba godzin

Wykład
0

Laboratorium
0

Inne
0

Ćwiczenia
0

Projekty/seminaria
90

Liczba punktów ECTS

10,00

Koordynatorzy

dr hab. inż. Mariusz Żal
mariusz.zal@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student przystępujący do tego przedmiotu powinien dysponować podstawową wiedzą, umiejętnościami i kompetencjami wyniesionymi z wcześniejszych etapów studiów, umożliwiającymi udział w zespołowej realizacji inżynierskiej pracy dyplomowej. Ponadto student powinien posiadać wiedzę i umiejętności techniczne niezbędne do realizacji pracy dyplomowej. W obszarze kompetencji społecznych powinien wykazywać się takimi postawami jak: uczciwość, odpowiedzialność, wytrwałość, ciekawość poznawcza, kreatywność, wysoka kultura osobista oraz szacunek wobec innych.

Cel przedmiotu

Proces dyplomowania służy pogłębieniu wiedzy teoretycznej dotyczącej wybranego tematu oraz rozwojowi umiejętności rozwiązywania praktycznych problemów inżynierskich, w tym wspólnej realizacji rozwiązania będącego przedmiotem pracy. Głównym zadaniem studentów jest wykonanie złożonego projektu informatycznego zgodnie z wybraną metodyką projektową opartą na zasadach przyjętych dla danego typu projektu, a następnie przygotowanie inżynierskiej pracy dyplomowej. Istotnym celem przedmiotu jest również doskonalenie umiejętności samodzielnej i zespołowej pracy projektowej.

Przedmiotowe efekty uczenia się

Wiedza:
W trakcie realizacji pracy inżynierskiej, student pogłębi wiedzę w zakresie złożonych struktur danych, zasad administrowania danymi i związanymi z nimi standardami; rozszerzy swoją wiedzę o zasady cyberbezpieczeństwa i prywatności wykorzystywane do zarządzania ryzykiem związanym z wykorzystywaniem, przetwarzaniem, przechowywaniem i przesyłaniem informacji lub danych. [K1_W02]
Pogłębi wiedzę na temat cyklu życia, projektowania oraz eksploatacji odpornych na ataki programowych systemów informatycznych. [K1_W09]
Pogłębi wiedzę na temat projektowania, konfigurowania oraz utrzymania systemów informatycznych. [K1_W11]
Ma wiedzę na temat zarządania projektami, jakim jest niewątpliwie praca inżynierska [K1_W18]

Umiejętności:
Potrafi korzystać ze źródeł literaturowych, integrować pozyskane informacje, oceniać je oraz dokonywać ich interpretacji i wyciągać wnioski w celu rozwiązania złożonych i nietypowych problemów w obszarze cyberbezpieczeństwa w związku z realizacją pracy dyplomowej [K1_U01]
Potrafi korzystać z odpowiednio dobranych metod i narzędzi, w tym zaawansowanych technik informacyjno-komunikacyjnych [K1_U02]
Potrafi zaplanować i przeprowadzić testy oprogramowania oraz systemów i sieci komputerowych w celu wykrycia w nich podatności na ataki; potrafi zaproponować rozwiązania poprawiające bezpieczeństwo działania rozwiązania zaproonowanego w pracy dyplomowej [K1_U03]
Potrafi zaplanować i przeprowadzić symulacje komputerowe i pomiary, w tym symulacje i pomiary dotyczące działania systemów teleinformatycznych, potrafi przedstawić otrzymane wyniki w formie liczbowej i graficznej, dokonać ich interpretacji i wyciągnąć właściwe wnioski [K1_U04]
Potrafi, przy formułowaniu i rozwiązywaniu zadań dotyczących realizacji pracy inżynierskiej, dostrzegać ich aspekty systemowe i pozatechniczne, w tym etyczne, ekonomiczne i prawne. [K1_U07]
Potrafi przygotować i przedstawić prezentację w języku polskim na temat realizowanej pracy inżynierskiej [K1_U11]
Potrafi przygotować i ustnie przedstawić w języku polskim i obcym zwarte opracowanie o aktualnych problemach i osiągnieciach pracy inżynierskiej [K1_U12]
Potrafi planować oraz organizować pracę indywidualną i w zespole (w tym opracować i zrealizować harmonogram prac zapewniający dotrzymanie terminu), stosuje zasady bezpieczeństwa i higieny pracy, a także umie pracować w zespołach o charakterze interdyscyplinarnym i wielokulturowym [K1_U15]

Kompetencje społeczne:
Rozumie znaczenie podnoszenia kompetencji zawodowych, osobistych i społecznych; ma świadomość, że wiedza i umiejętności w obszarze cyberbezpieczeństwa szybko ewoluują [K1_K01]
Rozumie znaczenie wiedzy w rozwiązywaniu problemów z zakresu cyberbezpieczeństwa; jest świadomy konieczności wykorzystania wiedzy ekspertów podczas rozwiązywania zadań inżynierskich w zakresie wykraczającym poza własne kompetencje [K1_K02]
Ma świadomość znaczenia pracy własnej i konieczności przestrzegania zasad etyki zawodowej, jest gotowy do podporządkowania się zasadom pracy w zespole i ponoszenia odpowiedzialności za wspólnie realizowane zadania, a także dbałości o dorobek i tradycje zawodu [K1_K05]

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:
Efekty kształcenia weryfikowane są poprzez:
- bieżącą kontrolę postępów realizowanych prac,
- ocenę wzrostu umiejętności i zastosowania poznanych metod,
- analizę sprawozdań z wybranych zagadnień projektowych,
- ocenę współpracy w zespole,
- ocenę rezultatów projektu pod kątem zgodności z założeniami, pozyskiwania nowej wiedzy i umiejętności oraz złożoności proponowanego rozwiązania,
- ocenę jakości dokumentacji i terminowości wykonania poszczególnych etapów.
Promotor przyznaje zarówno ocenę zbiorową dla całej pracy dyplomowej, jak i oceny indywidualne poszczególnych członków zespołu, uzasadniając ewentualne rozbieżności. Na podstawie tych ocen wystawiana jest ostateczna ocena dla każdego studenta. Recenzent przygotowuje ocenę całościową projektu, która jest wspólna dla wszystkich członków zespołu.Warunkiem pozytywnego zaliczenia jest

otrzymanie co najmniej 50% punktów możliwych do zdobycia.

Treści programowe

Inżynierska praca dyplomowa z zakresu cyberbezpieczeństwa powinna uwzględniać zarówno standardy projektów informatycznych, jak i specyficzne wymagania branży bezpieczeństwa. Konieczne jest precyzyjne określenie tematu oraz celów, które mogą obejmować opracowanie narzędzia wykrywającego określony typ ataków, analizę wybranego algorytmu szyfrującego czy przygotowanie polityki bezpieczeństwa dla konkretnej organizacji. W dalszej kolejności warto przeprowadzić przegląd dostępnej literatury, raportów branżowych i norm (takich jak NIST, ISO/IEC 27000 czy OWASP), by dobrać odpowiednią metodykę realizacji projektu oraz przyjąć harmonogram z wyznaczonymi kamieniami milowymi. Podczas projektowania i implementacji należy zadbać o stosowanie dobrych praktyk: separację środowisk, szyfrowanie danych, odpowiednie polityki dostępu czy monitorowanie logów. Efekt tych prac musi zostać zweryfikowany w procesie testowania, który obejmuje zarówno funkcjonalność rozwiązania, jak i jego odporność na ataki. Kluczowym elementem jest również rzetelna dokumentacja techniczna i użytkowa, opisująca architekturę systemu, zastosowane algorytmy oraz procedury bezpieczeństwa, a także instrukcje i rekomendacje wdrożeniowe. W kontekście cyberbezpieczeństwa szczególną uwagę należy zwracać na etykę oraz zgodność z przepisami prawa, zwłaszcza dotyczącymi ochrony danych osobowych.

Tematyka zajęć

brak

Metody dydaktyczne

• Konsultacje z promotorem dotyczące realizowanych projektów.
• Warsztaty zespołowe - dyskusje i analiza postępów w pracy.

Literatura

Podstawowa:
Zależna od obszaru badań związanych z przygotowywaną pracą dyplomową
Uzupełniająca

Uzupełniająca:
Uzupełniająca

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	265	10,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	90	3,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	175	7,00