KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Bezpieczeństwo systemów rozproszonych [S2Inf1-SRC>BSR]

Przedmiot

Kierunek studiów
Informatyka

Rok/Semestr
1/1

Studia w zakresie (specjalność)
Systemy rozproszone i chmurowe

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obligatoryjny

Liczba godzin

Wykład
15

Laboratorium
45

Inne
0

Ćwiczenia
0

Projekty/seminaria
0

Liczba punktów ECTS

4,00

Koordynatorzy

dr inż. Michał Szychowiak prof. PP
michal.szychowiak@put.poznan.pl

Wykładowcy

Wymagania wstępne

Efekty kształcenia ze studiów I stopnia zdefiniowane w Uchwale Senatu PP, a szczególnie efekty K1st_W1, K1st_W3, K1st_W4, K1st_W6, K1st_W7, K1st_U1, K1st_U2, K1st_U15, K1st_U18, K1st_K1 i K1st_K2, weryfikowane w procesie rekrutacji na studia 2 stopnia. Student rozpoczynający ten przedmiot powinien posiadać podstawową wiedzę z systemów operacyjnych, sieci komputerowych oraz bezpieczeństwa systemów informatycznych. Ponadto w zakresie kompetencji społecznych student musi prezentować takie postawy jak uczciwość, odpowiedzialność, wytrwałość, ciekawość poznawcza, kreatywność, kultura osobista, szacunek dla innych ludzi.

Cel przedmiotu

1. Przekazanie studentom szczegółowej wiedzy z dziedziny bezpieczeństwa systemów komputerowych wiarygodności przetwarzania, w zakresie sieci komputerowych i systemów przetwarzania rozproszonego.
2. Rozwijanie u studentów umiejętności rozwiązywania problemów bezpieczeństwa przetwarzania oraz ochrony danych środowisku rozproszonym.

Przedmiotowe efekty uczenia się

Wiedza:

1. student ma zaawansowaną i pogłębioną wiedzę z zakresu architektury systemów komputerowych, systemów operacyjnych oraz technologii sieciowych – [k2st_w1]
2. student ma zaawansowaną wiedzę szczegółową związaną z takimi zagadnieniami jak: analiza stanu bezpieczeństwa systemu, testy penetracyjne, zabezpieczanie systemu operacyjnego, aplikacji i infrastruktury sieciowej – [k2st_w3]
3. student ma wiedzę o trendach rozwojowych i najistotniejszych nowych osiągnięciach w informatyce w dziedzinie bezpieczeństwa systemów informatycznych – [k2st_w4]
4. student ma zaawansowaną i szczegółową wiedzę o cyklu życia systemów informatycznych sprzętowych lub programowych, w kontekście zagrożeń bezpieczeństwa – [k2st_w5]
5. student zna podstawowe metody, techniki i narzędzia stosowane przy rozwiązywaniu złożonych zadań inżynierskich z obszaru bezpieczeństwa systemów informatycznych – [k2st_w6]

Umiejętności:
1. student potrafi ocenić przydatność i możliwość wykorzystania nowych osiągnięć (metod i narzędzi) oraz nowych produktów informatycznych – [k2st_u6]
2. student potrafi - przy formułowaniu i rozwiązywaniu zadań inżynierskich – integrować wiedzę z różnych obszarów informatyki (a w razie potrzeby także wiedzę z innych dyscyplin naukowych) oraz zastosować podejście systemowe, uwzględniające także aspekty pozatechniczne – [k2st_u5]
3. student potrafi zaproponować ulepszenia (usprawnienia) istniejących rozwiązań technicznych – [k2st_u8]
4. student potrafi ocenić przydatność metod i narzędzi służących do rozwiązania zadania inżynierskiego, polegającego na budowie lub ocenie systemu informatycznego lub jego składowych pod kątem bezpieczeństwa, w tym dostrzec ograniczenia tych metod i narzędzi – [k2st_u9]

Kompetencje społeczne:
1. student rozumie, że w informatyce wiedza i umiejętności bardzo szybko stają się przestarzałe – [k2st_k1]
2. student rozumie znaczenie wykorzystywania najnowszej wiedzy z zakresu informatyki w rozwiązywaniu problemów badawczych i praktycznych z dziedziny bezpieczeństwa informatycznego – [k2st_k2]

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Ocena formująca:
a) w zakresie wykładów na podstawie:
– odpowiedzi na pytania dotyczące materiału omówionego na poprzednich wykładach,
b) w zakresie laboratoriów na podstawie:
– oceny bieżącego postępu realizacji zadań,
Ocena podsumowująca:
a) w zakresie wykładów na podstawie:
– oceny wiedzy i umiejętności wykazanych na zaliczeniu w formie testu wielokrotnego wyboru (20-25 pytań; próg zaliczeniowy: 50% punktów);
b) w zakresie laboratoriów na podstawie:
– oceny przygotowania studenta do poszczególnych sesji zajęć laboratoryjnych (sprawdzian "wejściowy") oraz ocenę umiejętności związanych z realizacją ćwiczeń laboratoryjnych,
– oceny wiedzy i umiejętności związanych z realizacją zadań laboratoryjnych poprzez 1 kolokwium w semestrze,
– oceny wiedzy i umiejętności wykazanych na sprawdzianie zaliczeniowym w formie testu wielokrotnego wyboru (15-20 pytań, ocenianych od 0-1 pkt. za każde, z dokładnością do 1/4 pkt za pojedynczą odpowiedź, zaliczenie wymaga zdobycia przynajmniej połowy punktów, skala ocen zgodnie z Regulaminem Studiów).
Dodatkowe punkty za aktywność podczas zajęć, a szczególnie za:
– omówienia dodatkowych aspektów zagadnienia,
– efektywność zastosowania zdobytej wiedzy podczas rozwiązywania zadanego problemu,
– umiejętność współpracy w ramach zespołu praktycznie realizującego zadanie szczegółowe w laboratorium,
– uwagi związane z udoskonaleniem materiałów dydaktycznych.

Treści programowe

Program przedmiotu obejmuje następujące zagadnienia:
Formalne modele bezpieczeństwa. Bezpieczeństwo aplikacji w architekturze SOA (Service Oriented Architecture) i usług Web Services. Środowiska systemowe o podwyższonym bezpieczeństwie. Polityki uwierzytelniania i kontroli dostępu. Rozproszone systemy uwierzytelniania i kontroli dostępu. Bezpieczna infrastruktura sieciowa. Monitoring zabezpieczeń.

Tematyka zajęć

Tematyka zajęć obejmuje następujące zagadnienia szczegółowe:
Formalne modele bezpieczeństwa, ze szczególnym uwzględnieniem modeli DAC, CAP, MAC, RBAC i ABAC. Bezpieczeństwo aplikacji w architekturze SOA (Service Oriented Architecture) i usług Web Services. Piaskownice systemowe (chroot) i kontenery (docker). Środowiska systemowe o podwyższonym bezpieczeństwie (RSBAC, AppArmor i SELinux). Rozproszone systemy uwierzytelniania i kontroli dostępu (Kerberos, Active Directory, Radius). Bezpieczna infrastruktura sieciowa, wieloplatformowe sieci VPN (IPsec i OpenVPN, Linux, Windows, Cisco IOS), konfiguracja i wykorzystanie usługi DNSsec. Zaawansowane zapory sieciowe i systemy IDS/IPS (NextGeneration Firewalls, Snort/Suricata, ModSecurity). Testy penetracyjne systemu operacyjnego i usług aplikacyjnych (Kali Linux, DVWA, BurpSuite). Monitoring i analiza zabezpieczeń.

Metody dydaktyczne

1. wykład: prezentacja multimedialna, pokaz multimedialny, demonstracja.
2. ćwiczenia laboratoryjne: demonstracja, dyskusja, warsztaty, ćwiczenia praktyczne, praca w zespole.
Obie formy zajęć stosują wybrane techniki metodologii Flipped Blended Learning.

Literatura

Podstawowa
1. William Stallings, "Cryptography and Network Security: Principles and Practice", VII ed., Pearson Education, 2016
2. Andrew Hoffman, "Web Application Security", O'Reilly, 2020
3. Mullder et al. (ed.), "Trends in Data Protection and Encryption Technologies", Springer, 2023

Uzupełniająca
1. Hakima Chaouchi, Maryline Laurent-Maknavicius, "Wireless and Mobile Networks Security", Wiley, 2009
2. Song Y.Yan, "Cybercryptography: Applicable Cryptography for Cyberspace Security", Springer, 2019
3. Chris Fry, Martin Nystrom, "Security Monitoring", O"Reilly, 2009
4. Bartosz Brodecki, Piotr Sasak, Michał Szychowiak: "Security policy conflicts in service-oriented systems", In New Generation Computing, vol. 30, no. 2-3, pp. 215-240; Ohmsha Ltd. & Springer-Verlag, 2012
5. Michał Jabczyński, Michał Szychowiak: "Orwell. From Bitcoin to secure Domain Name System", Proceedings of the 3rd Workshop on Social and Algorithmic Issues In Business Support (SAIBS 2015), 2015

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	100	4,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	60	2,50
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	40	1,50