KARTA OPISU MODUŁU KSZTAŁCENIA

Nazwa modułu/przedmiotu	Kod
Bezpieczeństwo systemów rozproszonych	**1010512311010511658**

Kierunek studiów	Profil kształcenia (ogólnoakademicki, praktyczny)	Rok / Semestr
Informatyka	**ogólnoakademicki**	**1 / 1**

Ścieżka obieralności/specjalność	Przedmiot oferowany w języku:	Kurs (obligatoryjny/obieralny)
Systemy rozproszone	**polski**	**obligatoryjny**

Stopień studiów:	**Forma studiów** (stacjonarna/niestacjonarna)
II stopień	**stacjonarna**

Godziny	Liczba punktów
Wykłady: **15** Ćwiczenia: **-** Laboratoria: **45** Projekty/seminaria: **-**	**5**

Status przedmiotu w programie studiów (podstawowy, kierunkowy, inny)	(ogólnouczelniany, z innego kierunku)
kierunkowy	**z danego kierunku**

Obszar(y) kształcenia i dziedzina(y) nauki i sztuki	**Podział ECTS (liczba i %)**
nauki techniczne	**5 100%**

Odpowiedzialny za przedmiot / wykładowca:

dr inż. Michał Szychowiak
email: Michał.Szychowiak@put.poznan.pl,
http://www.cs.put.poznan.pl/mszychowiak
tel. 61 6652964
Instytut Informatyki
ul. Piotrowo 2, 60-965 Poznań

Wymagania wstępne w zakresie wiedzy, umiejętności, kompetencji społecznych:

1	**Wiedza:**	Efekty kształcenia ze studiów I stopnia zdefiniowane w Uchwale Senatu PP, a szczególnie efekty K_W1-2, K_W4, K_W6-15, weryfikowane w procesie rekrutacji na studia 2 stopnia ? efekty te prezentowane są w serwisie internetowym wydziału www.fc.put.poznan.pl Student rozpoczynający ten przedmiot powinien posiadać podstawową wiedzę z systemów operacyjnych, sieci komputerowych oraz bezpieczeństwa systemów informatycznych.
2	**Umiejętności:**	Efekty kształcenia ze studiów I stopnia zdefiniowane w Uchwale Senatu PP, a szczególnie efekty K_U1-2, K_U4, K_U7-8, K_U14-20, K_U22-23, K_U26, weryfikowane w procesie rekrutacji na studia 2 stopnia ? efekty te prezentowane są w serwisie internetowym wydziału www.fc.put.poznan.pl
3	**Kompetencje społeczne**	Efekty kształcenia ze studiów I stopnia zdefiniowane w Uchwale Senatu PP, a szczególnie efekty K_K1-9, weryfikowane w procesie rekrutacji na studia 2 stopnia ? efekty te prezentowane są w serwisie internetowym wydziału www.fc.put.poznan.pl 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.

Efekty kształcenia i odniesienie do kierunkowych efektów kształcenia

Wiedza:

1. ma uporządkowaną, podbudowaną teoretycznie wiedzę ogólną w zakresie algorytmów i złożoności, architektury systemów komputerowych, systemów operacyjnych oraz technologii sieciowych - [K_W4]
2. ma podbudowaną teoretycznie szczegółową wiedzę związaną z wybranymi zagadnieniami z zakresu informatyki, takimi jak: analiza stanu bezpieczeństwa systemu, testy penetracyjne, zabezpieczanie systemu operacyjnego, aplikacji i infrastruktury sieciowej - [K_W5]
3. ma wiedzę o trendach rozwojowych i najistotniejszych nowych osiągnięciach w informatyce w dziedzinie bezpieczeństwa systemów informatycznych - [K_W6]
4. ma podstawową wiedzę o cyklu życia systemów informatycznych sprzętowych lub programowych - [K_W7]
5. zna podstawowe metody, techniki i narzędzia stosowane przy rozwiązywaniu złożonych zadań inżynierskich z obszaru dotyczącego bezpieczeństwa systemów informatycznych - [K_W8]

Umiejętności:

1. potrafi pozyskiwać informacje z literatury, baz danych oraz innych źródeł (w języku ojczystym i angielskim), integrować je, dokonywać ich interpretacji i krytycznej oceny, wyciągać wnioski oraz formułować i wyczerpująco uzasadniać opinie - [K_U1]
2. potrafi określić kierunki dalszego uczenia się i zrealizować proces samokształcenia - [K_U5]
3. potrafi wykorzystać do formułowania i rozwiązywania zadań inżynierskich i prostych problemów badawczych metody analityczne, symulacyjne oraz eksperymentalne - [K_U9]
4. 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 - [K_U10]
5. potrafi formułować i testować hipotezy związane z problemami inżynierskimi i prostymi problemami badawczymi - [K_U12]
6. potrafi ocenić przydatność i możliwość wykorzystania nowych osiągnięć (metod i narzędzi) oraz nowych produktów informatycznych - [K_U13]
7. potrafi zaproponować ulepszenia (usprawnienia) istniejących rozwiązań technicznych - [K_U21]
8. 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 - [K_U24]
9. potrafi - zgodnie z zadaną specyfikacją - zaprojektować system informatyczny o podwyższonym bezpieczeństwie oraz zrealizować ten projekt - co najmniej w części - używając właściwych metod, technik i narzędzi, w tym przystosowując do tego celu istniejące lub opracowując nowe narzędzia - [K_U27]
Kompetencje społeczne:
1. rozumie, że w informatyce wiedza i umiejętności bardzo szybko stają się przestarzałe - [K_K1]
2. zna przykłady i rozumie przyczyny wadliwie działających systemów informatycznych, które doprowadziły do poważnych strat finansowych, społecznych lub też do poważnej utraty zdrowia, a nawet życie - [K_K4]
3. potrafi odpowiednio określić priorytety służące realizacji określonego przez siebie lub innych zadania - [K_K6]

Sposoby sprawdzenia efektów kształcenia
Ocena formująca:
a) w zakresie wykładów:
- na podstawie odpowiedzi na pytania dotyczące materiału omówionego na poprzednich wykładach,
b) w zakresie laboratoriów / ćwiczeń:
- na podstawie oceny bieżącego postępu realizacji zadań,
Ocena podsumowująca:
a) w zakresie wykładów weryfikowanie założonych efektów kształcenia realizowane jest przez:
- ocenę wiedzy i umiejętności wykazanych na zaliczeniu w formie testu wielokrotnego wyboru (25 pytań, do zdobycia 25 pkt., zaliczenie wykładu od 12 pkt.)
- omówienie wyników zaliczenia,
b) w zakresie laboratoriów weryfikowanie założonych efektów kształcenia realizowane jest przez:
- ocenę przygotowania studenta do poszczególnych sesji zajęć laboratoryjnych (sprawdzian wejściowy) oraz ocenę umiejętności związanych z realizacją ćwiczeń laboratoryjnych,
- ocenę sprawozdania przygotowywanego częściowo w trakcie zajęć, a częściowo po ich zakończeniu; ocena ta obejmuje także umiejętność pracy w zespole,
- ocenę wiedzy i umiejętności związanych z realizacją zadań laboratoryjnych poprzez 1 kolokwium w semestrze,
Uzyskiwanie punktów dodatkowych 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 wykładu obejmuje następujące zagadnienia:

1. Bezpieczna infrastruktura sieciowa, mechanizmy bezpieczeństwa dostępne we współczesnych urządzeniach sieciowych. Zaawansowane zapory sieciowe i systemy IDS/IPS. Model Distributed Firewall. Ochrona przed atakami DDoS. Monitoring i analiza zabezpieczeń.
2. Formalne modele kontroli dostępu (DAC, CAP, DTE, MAC i RBAC) i ich współczesne praktyczne implementacje, na przykładzie systemów GRsecurity i RSBAC. Środowiska systemowe o podwyższonym bezpieczeństwie: AppArmor i SELinux. Utwardzanie systemu operacyjnego Windows
3. Bezpieczeństwo środowisk zwirtualizowanych. Zagrożenia aplikacji tworzonych z wykorzystaniem manager code.
4. Bezpieczeństwo aplikacji internetowych: zagrożenia i podatności technologii (HTML, XML, XHTML, JavaScript, ActionScript, Silverlight, Ajax, iFrames i in.).
5. Bezpieczeństwo aplikacji internetowych: mechanizmy obrony (SOP, Same-Origin Policy, Cross-Origin Resource Sharing, Content-Security-Policy, XSS Filtering, HTTP Public Key Pinning i in.)
6. Zarządzanie tożsamością. Systemy tożsamości federacyjnej.
7. Bezpieczeństwo w środowisku Web Services. Standardy bezpieczeństwa WS-*

Program laboratorium obejmuje następujące zagadnienia:

Bezpieczeństwo infrastruktury sieciowej, konfiguracja i wykorzystanie usługi DNSsec. Konfiguracja i wykorzystanie usługi RADIUS. Utwardzanie ochrony systemu operacyjnego (na przykładzie Application Armor lub podobnym). Utwardzanie ochrony systemu operacyjnego: RSBAC. Konfiguracja i wykorzystanie systemów IDS/IPS (na przykładzie snort lub podobnym). Wieloplatformowe sieci VPN (Windows-Linux). Systemy zapór sieciowych (na przykładzie MS ISA oraz Cisco ASA lub podobnych). Zabezpieczanie środowiska domenowego z użyciem mechanizmów Active Directory. Zabezpieczanie środowiska Web Services. Testy penetracyjne infrastruktury sieciowej i aplikacji internetowych. Monitoring i analiza zabezpieczeń. Bezpieczeństwo środowisk Cloud (na przykładzie Windows Azure, Amazon WS, OpenStack lub podobnych). Bezpieczeństwo środowisk wirtualnych (na przykładzie XEN lub podobnym).

Metody dydaktyczne:

1. wykład: prezentacja multimedialna, pokaz multimedialny, demonstracja.
2. ćwiczenia laboratoryjne: demonstracja, dyskusja, warsztaty, ćwiczenia praktyczne, praca w zespole

Literatura podstawowa:

1. David Salomon, Elements of Computer Security, Springer-Verlag, 2010
2. Neil Smyth, Security+ Essentials, Payload Media, 2012
3. Ramarao Kanneganti, Prasad Chodavarapu,SOA Security, Manning Publications, 2008
4. Bret Hartman et al. Mastering Web Services Security, Wiley, 2003

Literatura uzupełniająca:

1. Elisa Bertina et al., Security for Web Services And Service-Orineted Architectures, Springer, 2010
2. Tim Mather et al., Cloud Security and Privacy, O?Reilly, 2009
3. Shreeraj Shah, Web 2.0 Security, Charles River Media, 2008
4. Rolf Opplinger, Internet and Intranet Security, II ed. Artech House, 2002

Bilans nakładu pracy przeciętnego studenta

Czynność	Czas (godz.)
1. udział w zajęciach laboratoryjnych / ćwiczeniach	45
2. przygotowanie do ćwiczeń laboratoryjnych	15
3. dokończenie (w ramach pracy własnej) sprawozdań z ćwiczeń laboratoryjnych	15
4. udział w konsultacjach związanych z realizacją procesu kształcenia, w szczególności ćwiczeń laboratoryjnych (częściowo mogą być realizowane drogą elektroniczną)	8
5. przygotowanie do sprawdzianów / kolokwium i udział w kolokwium zaliczeniowym	15
6. udział w wykładach	15
7. przygotowanie do zaliczenia wykładu i obecność na zaliczeniu: 9 godz. + 1 godz.	10
8. omówienie wyników zaliczenia	1

Obciążenie pracą studenta

forma aktywności	godzin	ECTS
Łączny nakład pracy	124	5
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	69	3
Zajęcia o charakterze praktycznym	75	3