

KARTA OPISU MODUŁU KSZTAŁCENIA		
Nazwa modułu/przedmiotu Bezpieczeństwo systemów informatycznych		Kod 1010514371010510599
Kierunek studiów Informatyka	Profil kształcenia (ogólnoakademicki, praktyczny) ogólnoakademicki	Rok / Semestr 4 / 7
Ścieżka obieralności/specjalność -	Przedmiot oferowany w języku: polski	Kurs (obligatoryjny/obieralny) obligatoryjny
Stopień studiów: I stopień	Forma studiów (stacjonarna/niestacjonarna) niestacjonarna	
Godziny Wykłady: 16 Ćwiczenia: - Laboratoria: 16 Projekty/seminaria: -		Liczba punktów 3
Status przedmiotu w programie studiów (podstawowy, kierunkowy, inny) kierunkowy		(ogólnouczelniany, z innego kierunku) z danego kierunku
Obszar(y) kształcenia i dziedzina(y) nauki i sztuki nauki techniczne		Podział ECTS (liczba i %) 3 100%
Odpowiedzialny za przedmiot / wykładowca:		
<p>Dr inż. Michał Szychowiak email: Michal.Szychowiak@cs.put.poznan.pl, http://www.cs.put.poznan.pl/mszychowiak tel. (0-61) 665-2901 Instytut Informatyki ul. Piotrowo 2, 60-965 Poznań</p>		
Wymagania wstępne w zakresie wiedzy, umiejętności, kompetencji społecznych:		
1	Wiedza:	Student rozpoczynający ten przedmiot powinien posiadać podstawową wiedzę z dziedziny systemów operacyjnych i sieci komputerowych.
2	Umiejętności:	Powinien posiadać umiejętność sprawnego posługiwania się systemem operacyjnym klasy Unix i MS Windows, programowania (w podstawowym zakresie wykorzystania funkcji systemowych) oraz pozyskiwania informacji ze wskazanych źródeł.
3	Kompetencje społeczne	Powinien również rozumieć konieczność poszerzania swoich kompetencji. 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:		
<p>1. Zapoznanie studentów z podstawowymi problemami bezpieczeństwa systemów informatycznych, w zakresie wykorzystywania, konfigurowania i administrowania mechanizmami bezpieczeństwa na poziomie systemowym i aplikacyjnym, ze szczególnym uwzględnieniem mechanizmów i protokołów sieciowych.</p> <p>2. Uzyskanie przez studentów umiejętności efektywnego posługiwania się mechanizmami kryptograficznymi, kontroli dostępu, filtracji ruchu sieciowego, tuneli wirtualnych oraz narzędziami zabezpieczeń warstwy aplikacyjnej.</p>		
Efekty kształcenia i odniesienie do kierunkowych efektów kształcenia		
Wiedza:		
<p>1. zna podstawowe metody, techniki i narzędzia stosowane przy rozwiązywaniu prostych zadań informatycznych z zakresu zabezpieczeń systemów operacyjnych, sieci komputerowych, usług sieciowych i aplikacji użytkowych, w tym korzystania z narzędzi kryptograficznych, tuneli VPN, zapór sieciowych i systemów IDS - [K_W8]</p> <p>2. ma wiedzę nt. kodeksów etycznych dotyczących informatyki, rozumie zagrożenia związane z przestępczością elektroniczną, rozumie specyfikę systemów krytycznych ze względu na bezpieczeństwo (ang. mission-critical systems) - [K_W10]</p> <p>3. ma wiedzę o trendach rozwojowych i najistotniejszych nowych osiągnięciach w informatyce, w szczególności odnośnie zagrożeń bezpieczeństwa i metod ochrony - [K_W6]</p> <p>4. zna i rozumie zasady poprawnej i bezpiecznej eksploatacji systemów informatycznych - [-]</p> <p>5. ma podstawową wiedzę niezbędną rozpoznania zagrożeń bezpiecznej eksploatacji systemów operacyjnych, sieci komputerowych i aplikacji użytkowych - [-]</p> <p>6. ma wiedzę niezbędną do właściwego doboru i zastosowania podstawowych mechanizmów uwierzytelniania, ochrony poufności i integralności danych i komunikacji - [-]</p>		
Umiejętności:		

1. potrafi zabezpieczyć przesyłane dane przed nieuprawnionym odczytem - [K_U23]
2. potrafi ocenić architekturę oprogramowania z punktu widzenia wymagań pozafunkcyjnych, dotyczących bezpieczeństwa informacji - [K_U15]
3. 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]
4. dokonywać konfiguracji systemu operacyjnego i urządzeń sieciowych zmierzającej do podnoszenia bezpieczeństwa ich pracy - [-]
5. posługiwać się zaporami sieciowymi, pakietami kryptograficznymi na poziomie podstawowych usług aplikacyjnych (m.in. SSH, PGP) - [-]
6. zbudować prawidłowe środowisko komunikacji przy wykorzystaniu tuneli VPN (za pomocą protokołu IPsec) i mechanizmów SSO - [-]

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 - [K_K4]
3. prawidłowo identyfikuje i rozstrzyga dylematy związane z wykonywaniem zawodu - [-]
4. ma świadomość roli społecznej absolwenta uczelni technicznej, a zwłaszcza rozumie potrzebę formułowania i przekazywania społeczeństwu informacji i opinii dotyczących zagrożeń bezpieczeństwa systemów informatycznych - [-]
5. ma świadomość wagi zachowania się w sposób profesjonalny, przestrzegania zasad etyki zawodowej - [-]

Sposoby sprawdzenia efektów kształcenia

Efekty kształcenia 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 ćwiczeń:
- na podstawie oceny bieżącego postępu realizacji zadań,

Ocena podsumowująca:

Sprawdzanie założonych efektów kształcenia realizowane jest przez:

- ocenę przygotowania studenta do poszczególnych sesji zajęć laboratoryjnych (sprawdzian

Treści programowe

Wykład obejmuje następujące główne obszary zagadnień:

- zagrożenia bezpieczeństwa, w tym m.in. zagrożenia systemów informatycznych w kontekście poufności, integralności i dostępności informacji, ogólna analiza zagrożeń i ryzyka, przykładowe ataki. Omawiane są również modele bezpieczeństwa oraz klasy bezpieczeństwa systemów informatycznych (TCSEC, ITSEC, CC EAL),
- elementy kryptografii, w tym m.in. podstawy matematyczne szyfrowania, szyfrowanie symetryczne i asymetryczne, algorytmy szyfrowania, podpis elektroniczny, infrastruktura klucza publicznego, zastosowania kryptografii (EFS, PGP, S/MIME),
- bezpieczeństwo systemów operacyjnych, w tym m.in. szczególnie wrażliwe komponenty i sposoby ich sondowania, podstawowe modele uwierzytelniania, uwierzytelnianie biometryczne, systemy haseł jednorazowych i środowiska jednokrotnego uwierzytelniania (SSO), strategie kontroli dostępu (POSIX ACL, Windows DACL, Trustees), problematyka bezpiecznego składowania danych i ochrony systemu plików, szyfrowane systemy plików,
- bezpieczeństwo infrastruktury sieciowej, w tym m.in. problematyka bezpieczeństwa protokołów komunikacyjnych, rodzaje i sposoby działania zapór sieciowych (firewall), strefy zdemilitaryzowane, wirtualne sieci prywatne (VPN) i protokoły wykorzystywane do ich realizacji, uwierzytelnianie sieciowe (Kerberos),
- bezpieczeństwo aplikacji, w tym m.in. bezpieczeństwo aplikacji i usług komunikacyjnych, m.in. usługi www, poczty elektronicznej oraz komunikatorów internetowych. Poruszone są zagadnienia dotyczące bezpiecznego programowania, w szczególności w kontekście konstrukcji aplikacji sieciowych. Omawiane są standardy API do usług bezpieczeństwa (GSSAPI). Analizowane są mechanizmy ograniczania środowiska wykonania aplikacji, piaskownice systemowe i aplikacyjne,
- zarządzanie bezpieczeństwem, w tym m.in. projektowanie i wdrażanie polityki bezpieczeństwa systemu informatycznego, zarządzanie bezpieczeństwem, narzędzia analizy zabezpieczeń i monitoringu, systemu IDP/IPS, pułapki i przynęty. Omawiane są również narzędzia zarządzania stanem aktualizacji systemu operacyjnego. Przedstawiane są instytucje wsparcia w zarządzaniu bezpieczeństwem, jednostki reagowania na incydenty oraz ich procedury pracy.

Metody dydaktyczne:

1. wykład: prezentacja multimedialna, pokaz multimedialny, demonstracja.
2. ćwiczenia laboratoryjne: ćwiczenia praktyczne, dyskusja, praca indywidualna i z podziałem na role.

Literatura podstawowa:		
1. Janusz Stokłosa, Tomasz Bliski, Tadeusz Pankowski, Bezpieczeństwo danych w systemach informatycznych, PWN, 2001		
2. Ross Anderson, Security Engineering, John Wiley; Sons, 2003		
3. William Stallings, Cryptography and Network Security Principles and Practices, IV ed., Prentice Hall, 2005		
4. David Salomon, Elements of Computer Security, Springer-Verlag, 2010		
5. Jie Wang, Computer Network Security Theory and Practice, Higher Education Press, 2009		
Literatura uzupełniająca:		
1. William R. Cheswick, Firewalle i bezpieczeństwo w sieci, Helion, 2003		
2. Christof Paar, Jan Pelzl, Understanding Cryptography, Springer-Verlag, 2010.		
3. Niels Ferguson, Bruce Schneier, Kryptografia w praktyce, Helion, 2004		
4. Michael Howard, David LeBlanc, Writing Secure Code, Microsoft Press, 2003		
5. Wenbo Mao, Modern Cryptography - Theory and Practice, Prentice Hall, 2003		
6. Dorothy E. R. Denning, Wojna informacyjna i bezpieczeństwo informacji, WNT, 2002		
Bilans nakładu pracy przeciętnego studenta		
Czynność	Czas (godz.)	
1. udział w wykładach	16	
2. zapoznanie się ze wskazaną literaturą / materiałami dydaktycznymi (10 stron tekstu naukowego = 1 godz.), 100 stron	10 16	
3. udział w zajęciach laboratoryjnych:	15	
4. przygotowanie do ćwiczeń laboratoryjnych:	10	
5. dokończenie (w ramach pracy własnej) sprawozdań z ćwiczeń laboratoryjnych:	2	
6. udział w konsultacjach związanych z realizacją procesu kształcenia, w szczególności ćwiczeń laboratoryjnych	2 6	
7. przygotowanie do zaliczenia i udział w kolokwium zaliczeniowym:	6	
8. przygotowanie do egzaminu i obecność na egzaminie: 4 godz. + 2 godz.		
Obciążenie pracą studenta		
forma aktywności	godzin	ECTS
Łączny nakład pracy	77	3
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	34	1
Zajęcia o charakterze praktycznym	41	2