KARTA OPISU MODUŁU KSZTAŁCENIA

Nazwa modułu/przedmiotu	Kod
Bezpieczeństwo systemów rozproszonych 1	**1010515311010504677**

Kierunek studiów	Profil kształcenia (ogólnoakademicki, praktyczny)	Rok / Semestr
Informatyka	**ogólnoakademicki**	**1 / 1**
Ścieżka obieralności/specjalność	Przedmiot oferowany w języku:	Kurs (obligatoryjny/obieralny)
Sieci komputerowe	**polski**	**obligatoryjny**

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

Godziny	Liczba punktów
Wykłady: **16** Ćwiczenia: **-** Laboratoria: **16** Projekty/seminaria: **-**	**3**

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 %)**

Odpowiedzialny za przedmiot / wykładowca:

dr inż. Michał Szychowiak
email: Michał.Szychowiak@put.poznan.pl
tel. 61 6652964
Wydział Informatyki
ul. Piotrowo 3 60-965 Poznań

Odpowiedzialny za przedmiot / wykładowca:

mgr inż. Rafał Skowroński
email: Rafal.Skowronski@cs.put.poznan.pl
tel. 61 665 2952
Wydział Informatyki
ul. Piotrowo 3 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 K1st_W1, K1st_W3, K1st_W4, K1st_W6, K1st_W7, 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 K1st_U1, K1st_U2, K1st_U15, K1st_U18, 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 K1st_K1 i K1st_K2, 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 zaawansowaną i pogłębioną wiedzę z zakresu architektury systemów komputerowych, systemów operacyjnych oraz technologii sieciowych - [K2st_W1]

2. 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. ma wiedzę o trendach rozwojowych i najistotniejszych nowych osiągnięciach w informatyce w dziedzinie bezpieczeństwa systemów informatycznych - [K2st_W4]

4. ma zaawansowaną i szczegółową wiedzę o cyklu życia systemów informatycznych sprzętowych lub programowych, w konteście zagrożeń bezpieczeństwa - [K2st_W5]

5. zna podstawowe metody, techniki i narzędzia stosowane przy rozwiązywaniu złożonych zadań inżynierskich z obszaru bezpieczeństwa systemów informatycznych - [K2st_W6]

Umiejętności:

1. potrafi ocenić przydatność i możliwość wykorzystania nowych osiągnięć (metod i narzędzi) oraz nowych produktów informatycznych - [K2st_U6]

2. 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. potrafi zaproponować ulepszenia (usprawnienia) istniejących rozwiązań technicznych - [K2st_U8]

4. 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. rozumie, że w informatyce wiedza i umiejętności bardzo szybko stają się przestarzałe - [K2st_K1]

2. rozumie znaczenie wykorzystywania najnowszej wiedzy z zakresu informatyki w rozwiązywaniu problemów badawczych i praktycznych z dziedziny bezpieczeństwa informatycznego - [K2st_K2]

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 kolokwium zaliczeniowym w formie testu wielokrotnego wyboru (10-20 pytań po 1 pkt. każde, zaliczenie wykładu od połowy pkt.)

- omówienie wyników kolokwium,

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:

Zagrożenia systemów informatycznych w kontekście poufności, integralności i dostępności informacji, ogólna analiza zagrożeń i ryzyka, przykładowe ataki. Modele bezpieczeństwa: model bezpieczeństwa ISO, klasy bezpieczeństwa systemów informatycznych (TCSEC, ITSEC, EAL). Elementy kryptografii: podstawy matematyczne szyfrowania, szyfrowanie symetryczne i asymetryczne, algorytmy szyfrowania, podpis elektroniczny, infrastruktura klucza publicznego, zastosowania kryptografii. Bezpieczeństwo systemów operacyjnych (w szcz. MS Windows oraz Linux), podstawowe modele uwierzytelniania, strategie kontroli dostępu. Bezpieczeństwo protokołów komunikacyjnych i usług komunikacyjnych, m.in. www, poczty elektronicznej oraz komunikatorów internetowych.

Program laboratorium obejmuje następujące zagadnienia:

Bezpieczeństwo kont systemu operacyjnego MS Windows, mechanizmy impersonation, MIC, UAC itp. Bezpieczeństwo systemu plików, kontrola dostępu (POSIX ACL, MS Windows DACL), szyfrowanie (EFS), ochrona strumieni ADS. Zabezpieczanie komunikacji sieciowej w środowisku MS Windows, ochrona zasobów udostępnianych sieciowo. Zabezpieczanie usług sieciowych na przykładzie poczty elektronicznej i usługi WWW. Wykorzystanie pakietu SSH do zabezpieczania zdalnego dostępu do systemu operacyjnego. Zabezpieczanie środowiska realizacji przetwarzania aplikacyjnego, ograniczanie powłoki systemu operacyjnego, mechanizmy SSO i filtracji dostępu do procesów aplikacyjnych.

Cześć wymienionych wyżej treści programowych realizowana jest w ramach pracy własnej studenta.

Literatura podstawowa:

1. William Stallings, Cryptography and Network Security: Principles and Practice, Pearson Education, 2016

2. Krzysztof Liderman, Bezpieczeństwo informacyjne. Nowe wyzwania, PWN, 2017

3. Michał Szychowiak, Bezpieczeństwo systemów informatycznych. Zaawansowane ćwiczenia w systemach Windows i Linux, WPP, 2017

Literatura uzupełniająca:

1. Neil Smyth, Security+ Essentials, Payload Media, 2012 (http://techotopia.com/index.php?title=Security%2B_Essentials)

2. John Savard, A Cryptographic Compendium (http://www.quadibloc.com/crypto/jscrypt.htm)

3. Bartosz Brodecki, Jerzy Brzeziński, Piotr Sasak, Michał Szychowiak, Problemy bezpieczeństwa w architekturze SOA, w Damian Niemir, Maciej Stroiński, Jan Węglarz (Eds.): Nauka w obliczu społeczeństwa cyfrowego, Ośrodek Wydawnictw Naukowych, 2010, ISBN 978-83-7712-032-3, str. 233-246

4. Michał Szychowiak, Bezpieczeństwo Systemów Informatycznych. http://wazniak.mimuw.edu.pl/index.php?title=Bezpieczeństwo_systemów_komputerowych

Bilans nakładu pracy przeciętnego studenta

Czynność	Czas (godz.)
1. udział w zajęciach laboratoryjnych	16
2. przygotowanie do ćwiczeń laboratoryjnych	8
3. dokończenie (w ramach pracy własnej) sprawozdań z ćwiczeń laboratoryjnych	8
4. udział w konsultacjach (mogą być realizowane drogą elektroniczną) związanych z realizacją procesu kształcenia, w szczególności ćwiczeń laboratoryjnych	2
5. przygotowanie do sprawdzianów / kolokwium i udział w kolokwium zaliczeniowym	10
6. udział w wykładach	16
7. zapoznanie się ze wskazaną literaturą / materiałami dydaktycznymi (10 stron tekstu naukowego = 1 godz.), 150 stron	15

Obciążenie pracą studenta

forma aktywności	godzin	ECTS
Łączny nakład pracy	75	3
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	34	1
Zajęcia o charakterze praktycznym	32	1