KARTA OPISU MODUŁU KSZTAŁCENIA

Nazwa modułu/przedmiotu	Kod
Bezpieczeństwo systemów informatycznych	**1010511371010510599**

Kierunek studiów	Profil kształcenia (ogólnoakademicki, praktyczny)	Rok / Semestr
Informatyka	**ogólnoakademicki**	**4 / 7**
Ścieżka obieralności/specjalność	Przedmiot oferowany w języku:	Kurs (obligatoryjny/obieralny)
-	**polski**	**obligatoryjny**

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

Godziny	Liczba punktów
Wykłady: **30** Ćwiczenia: **-** Laboratoria: **30** Projekty/seminaria: **-**	**4**

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: Michal.Szychowiak@cs.put.poznan.pl,
http://www.cs.put.poznan.pl/mszychowiak
tel. 61 665 2964
Instytut Informatyki
ul. Piotrowo 2, 60-965 Poznań

Odpowiedzialny za przedmiot / wykładowca:

Mgr inż. Bartosz Brodecki
email: Bartosz.Brodecki@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:**	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:

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.

2. Uzyskanie przez studentów umiejętności efektywnego posługiwania się mechanizmami kryptograficznymi, kontroli dostępu, filtracji ruchu sieciowego, tuneli wirtualnych oraz narzędziami zabezpieczeń warstwy aplikacyjnej.

Efekty kształcenia i odniesienie do kierunkowych efektów kształcenia

Wiedza:

1. ma podstawową wiedzę niezbędną rozpoznania zagrożeń bezpiecznej eksploatacji systemów operacyjnych, sieci komputerowych i aplikacji użytkowych - [K1st_W4]

2. ma wiedzę o trendach rozwojowych i najistotniejszych nowych osiągnięciach w informatyce, w szczególności odnośnie zagrożeń bezpieczeństwa i metod ochrony - [K1st_W5]

3. zna i rozumie zasady poprawnej i bezpiecznej eksploatacji systemów informatycznych - [K1st_W6]

4. 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 - [K1st_W7]

5. ma wiedzę niezbędną do właściwego doboru i zastosowania podstawowych mechanizmów uwierzytelniania, ochrony poufności i integralności danych i komunikacji - [K1st_W7]

6. 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) - [K1st_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 - [K1st_U1]

2. potrafi dokonywać konfiguracji systemu operacyjnego i urządzeń sieciowych zmierzającej do podnoszenia bezpieczeństwa ich pracy - [K1st_U3]

3. potrafi zbudować prawidłowe środowisko komunikacji przy wykorzystaniu tuneli VPN (za pomocą protokołu IPsec) i mechanizmów SSO - [K1st_U3]

4. potrafi posługiwać się zaporami sieciowymi, pakietami kryptograficznymi na poziomie podstawowych usług aplikacyjnych (m.in. SSH, PGP) - [K1st_U4]

5. potrafi ocenić ryzyko zagrożeniami cyber-bezpieczeństwa - [K1st_U6]

6. potrafi ocenić architekturę oprogramowania z punktu widzenia wymagań pozafunkcjonalnych, dotyczących bezpieczeństwa informacji - [K1st_U9]

7. potrafi zabezpieczyć przesyłane dane przed nieuprawnionym odczytem - [K1st_U12]

8. potrafi organizować, współdziałać i pracować w grupie nad rozwiązaniem problemu z dziedziny bezpieczeństwa informatycznego - [K1st_U18]

Kompetencje społeczne:

1. rozumie, że w informatyce wiedza i umiejętności bardzo szybko stają się przestarzałe - [K1st_K1]

2. zna przykłady i rozumie przyczyny wadliwie działających systemów informatycznych, które doprowadziły do poważnych strat finansowych, społecznych - [K1st_K2]

3. ma świadomość roli społecznej absolwenta uczelni technicznej, a zwłaszcza rozumie potrzebę formułowania i przekazywania społeczeństwu informacji i opinii dotyczących zagrożeń bezpieczeństwa systemów informatycznych - [K1st_K4]

4. ma świadomość wagi zachowania się w sposób profesjonalny, przestrzegania zasad etyki zawodowej - [K1st_K4]

5. prawidłowo identyfikuje i rozstrzyga dylematy związane z wykonywaniem zawodu - [K1st_K5]

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 "wejściowy") oraz ocenę umiejętności związanych z realizacją ćwiczeń laboratoryjnych,
- ocenę sprawozdania przygotowywanego częściowo w trakcie zajęć, a częściowo po ich zakończeniu,
- ocenę wiedzy i umiejętności związanych z realizacją zadań projektowych / laboratoryjnych poprzez kolokwium,
- ocenę wiedzy i umiejętności wykazanych na egzaminie pisemnym o charakterze problemowym lub w formie testu wielokrotnego wyboru (15-20 pytań, ocenianych od 0-1 pkt. za każde, z dokładnością do ? pkt za pojedynczą odpowiedź, zaliczenie egzaminu wymaga zdobycia przynajmniej połowy punktów)

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,
- wskazywanie trudności percepcyjnych studentów umożliwiające bieżące doskonalenia procesu dydaktycznego.

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 uwierzytelniani (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. Poruszane 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. William Stallings, Cryptography and Network Security: Principles and Practice, Pearson Education, 2016
2. David Salomon, Elements of Computer Security, Springer-Verlag, 2010
3. Michał Szychowiak, Bezpieczeństwo systemów informatycznych. Zaawansowane ćwiczenia w systemach Windows i Linux, WPP, 2017

Literatura uzupełniająca:

1. Ross Anderson, Security Engineering, John Wiley & Sons, 2003 (http://www.cl.cam.ac.uk/~rja14/book.html)
2. Neil Smyth, Security+ Essentials, Payload Media, 2012 (http://techotopia.com/index.php?title=Security%2B_Essentials)
3. John Savard, A Cryptographic Compendium (http://www.quadibloc.com/crypto/jscrypt.htm)
4. 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.
5. 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 wykładach	30
2. zapoznanie się ze wskazaną literaturą / materiałami dydaktycznymi (10 stron tekstu naukowego = 1 godz.), 100 stron	20
3. udział w zajęciach laboratoryjnych:	30
4. przygotowanie do ćwiczeń laboratoryjnych:	5
5. dokończenie (w ramach pracy własnej) sprawozdań z ćwiczeń laboratoryjnych:	5
6. udział w konsultacjach związanych z realizacją procesu kształcenia, w szczególności ćwiczeń laboratoryjnych	2
7. przygotowanie do zaliczenia i udział w kolokwium zaliczeniowym:	5
8. przygotowanie do egzaminu i obecność na egzaminie: 8 godz. + 2 godz.	10

Obciążenie pracą studenta

forma aktywności	godzin	ECTS
Łączny nakład pracy	107	4
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	62	2
Zajęcia o charakterze praktycznym	40	2