



KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Bezpieczeństwo systemów informatycznych

Przedmiot

Kierunek studiów

Informatyka

Studia w zakresie (specjalność)

—

Poziom studiów

pierwszego stopnia

Forma studiów

stacjonarne

Rok/semestr

4/7

Profil studiów

ogólnoakademicki

Język oferowanego przedmiotu

polski

Wymagalność

obligatoryjny

Liczba godzin

Wykład

30

Ćwiczenia

Laboratoria

30

Projekty/seminaria

Inne (np. online)

Liczba punktów ECTS

4

Wykładowcy

Odpowiedzialny za przedmiot/wykładowca:

dr inż. Michał Szychowiak

email: Michal.Szychowiak@cs.put.poznan.pl

tel. 61 665 2964

Wydział Informatyki i Telekomunikacji

ul. Piotrowo 3 60-965 Poznań

Odpowiedzialny za przedmiot/wykładowca:

mgr inż. Rafał Budka

email: Rafal.Budka@cs.put.poznan.pl

tel. 61 665 2963

Wydział Informatyki i Telekomunikacji

ul. Piotrowo 3 60-965 Poznań

Wymagania wstępne

Student rozpoczynający ten przedmiot powinien posiadać podstawową wiedzę z dziedziny systemów operacyjnych i sieci komputerowych. 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. 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.

Przedmiotowe efekty uczenia się

Wiedza

1. student ma podstawową wiedzę niezbędną rozpoznania zagrożeń bezpiecznej eksploatacji systemów operacyjnych, sieci komputerowych i aplikacji użytkowych – [K1st_W4]
2. student ma wiedzę o trendach rozwojowych i najistotniejszych nowych osiągnięciach w informatyce, w szczególności odnośnie zagrożeń bezpieczeństwa i metod ochrony – [K1st_W5]
3. student zna i rozumie zasady poprawnej i bezpiecznej eksploatacji systemów informatycznych – [K1st_W6]
4. student 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, zapor sieciowych i systemów IDS – [K1st_W7]
5. student ma wiedzę niezbędną do właściwego doboru i zastosowania podstawowych mechanizmów uwierzytelniania, ochrony poufności i integralności danych i komunikacji – [K1st_W7]
6. student 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. student 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. student potrafi dokonywać konfiguracji systemu operacyjnego i urządzeń sieciowych zmierzającej do podnoszenia bezpieczeństwa ich pracy – [K1st_U3]
3. student potrafi zbudować prawidłowe środowisko komunikacji przy wykorzystaniu tuneli VPN (za pomocą protokołu IPsec) i mechanizmów SSO – [K1st_U3]
4. student potrafi posługiwać się zaporami sieciowymi, pakietami kryptograficznymi na poziomie podstawowych usług aplikacyjnych (m.in. SSH, PGP) – [K1st_U4]
5. student potrafi ocenić ryzyko zagrożeniami cyber-bezpieczeństwa – [K1st_U6]



6. student potrafi ocenić architekturę oprogramowania z punktu widzenia wymagań pozafunkcyjnych, dotyczących bezpieczeństwa informacji – [K1st_U9]
7. student potrafi zabezpieczyć przesyłane dane przed nieuprawnionym odczytem – [K1st_U12]
8. student potrafi organizować, współdziałać i pracować w grupie nad rozwiązaniem problemu z dziedziny bezpieczeństwa informatycznego – [K1st_U18]

Kompetencje społeczne

1. student rozumie, że w informatyce wiedza i umiejętności bardzo szybko stają się przestarzałe – [K1st_K1]
2. student zna przykłady i rozumie przyczyny wadliwie działających systemów informatycznych, które doprowadziły do poważnych strat finansowych, społecznych – [K1st_K2]
3. student 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. student ma świadomość wagi zachowania się w sposób profesjonalny, przestrzegania zasad etyki zawodowej – [K1st_K4]
5. student prawidłowo identyfikuje i rozstrzyga dylematy związane z wykonywaniem zawodu – [K1st_K5]

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 ćwiczeń na podstawie:

- oceny przygotowania studenta do poszczególnych sesji zajęć laboratoryjnych (sprawdzian "wejściowy") oraz ocenę umiejętności związanych z realizacją ćwiczeń laboratoryjnych,
- oceny sprawozdania przygotowywanego częściowo w trakcie zajęć, a częściowo po ich zakończeniu; ocena ta obejmuje także umiejętność pracy w zespole,
- oceny wiedzy i umiejętności związanych z realizacją zadań laboratoryjnych poprzez 1 kolokwium w semestrze.

Ocena podsumowująca:

a) w zakresie wykładów na podstawie:

- oceny wiedzy i umiejętności związanych z realizacją zadań laboratoryjnych poprzez kolokwium,



b) w zakresie ćwiczeń na podstawie:

– oceny 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 1/4 pkt za pojedynczą odpowiedź, zaliczenie egzaminu wymaga zdobycia przynajmniej połowy punktów).

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

Treści programowe

Program przedmiotu 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.
- elementy kryptografii, w tym m.in. podstawy matematyczne szyfrowania, szyfrowanie symetryczne i asymetryczne, algorytmy szyfrowania, podpis elektroniczny, infrastruktura klucza publicznego, zastosowania kryptografii (EFS, 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, CAP, RBAC, ABAC...), 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 (DMZ), wirtualne sieci prywatne (VPN) i protokoły wykorzystywane do ich realizacji (IPsec, TLS, ...), uwierzytelnianie sieciowe (Kerberos),
- bezpieczeństwo aplikacji, w tym m.in. bezpieczeństwo aplikacji i usług komunikacyjnych, m.in. usługi www, poczty elektronicznej oraz komunikatorów internetowych, zagadnienia dotyczące bezpiecznego programowania, w szczególności konstrukcji aplikacji sieciowych, standardy API do usług



bezpieczeństwa, 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, Lawrie Brown, "Computer Security: Principles and Practice", Pearson Education, 2018
2. William Stallings, "Cryptography and Network Security: Principles and Practice", Pearson Education, 2017
3. Mark Stamp, "Information Security: Principles and Practice", Wiley, 2011
4. David Salomon, "Elements of Computer Security", Springer-Verlag, 2010
5. Michał Szychowiak, "Bezpieczeństwo systemów informatycznych. Zaawansowane ćwiczenia w systemach Windows i Linux", WPP, 2017

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/jsencrypt.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



Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	100	4,0
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	60	2,5
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych, przygotowanie do kolokwium/egzaminu) ¹	40	1,5

¹ niepotrzebne skreślić lub dopisać inne czynności