

POLITECHNIKA KRAKOWSKA IM. TADEUSZA KOŚCIUSZKI

KARTA PRZEDMIOTU

obowiązuje studentów rozpoczynających studia w roku akademickim 2017/2018

Wydział Fizyki, Matematyki i Informatyki

Kierunek studiów: Informatyka

Profil: Ogólnoakademicki

Forma studiów: niestacjonarne

Kod kierunku: I

Stopień studiów: II

Specjalności: Informatyka stosowana dla inżynierów

1 INFORMACJE O PRZEDMIOCIE

NAZWA PRZEDMIOTU	Technologie ochrony systemów informatycznych
NAZWA PRZEDMIOTU W JĘZYKU ANGIELSKIM	Computer system security technologies
KOD PRZEDMIOTU	WFMiI I oIIN D7 17/18
KATEGORIA PRZEDMIOTU	Przedmioty specjalnościowe
LICZBA PUNKTÓW ECTS	5.00
SEMESTRY	3

2 RODZAJ ZAJĘĆ, LICZBA GODZIN W PLANIE STUDIÓW

SEMESTR	WYKŁAD	ĆWICZENIA	LABORATORIUM	LABORATORIUM KOMPUTERO- WE	SEMINARIUM	PROJEKT
3	9	0	9	0	0	0

3 CELE PRZEDMIOTU

Cel 1 Zapoznanie studentów z podstawowymi zagrożeniami systemów komputerowych.

Cel 2 Zapoznanie studentów z podstawowymi metodami zabezpieczenia systemu operacyjnego komputera i systemu komputerowego

4 WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

1 zaliczenie przedmiotów: algebra, matematyka dyskretna

5 EFEKTY KSZTAŁCENIA

EK1 Wiedza Student wymienia i objaśnia podstawowe zagrożenia dla systemu komputerowego.

EK2 Umiejętności Student potrafi rozpoznać podstawowe zagrożenia dla systemu komputerowego.

EK3 Wiedza Student objaśnia podstawowe metody zabezpieczenia systemu komputerowego.

EK4 Umiejętności Student potrafi stosować wybrane metody zabezpieczenia danych w systemie operacyjnym i w sieci komputerowej

EK5 Kompetencje społeczne Student potrafi pracować w zespole, współpracować przy wyborze metod rozwiązywania problemów i wspólnie ponosić odpowiedzialność za otrzymane rezultaty.

6 TREŚCI PROGRAMOWE

WYKŁAD		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
W1	Wstęp: potrzeba zabezpieczenia systemów komputerowych. Kryptografia i kryptoanaliza. Systemy kryptograficzne symetryczne i asymetryczne.	1
W2	Identyfikacja i uwierzytelnianie użytkownika: system hasel. Przechowywanie hasel, weryfikacja hasel. Ataki na system hasel. Słabe hasła. Weryfikacja hasel. Hasła jednorazowe. System Kerberos.	1
W3	Zabezpieczanie połączeń internetowych: pakiet Secure Shell-korzyści ze stosowania. Schemat nawiązywania połączenia. Pakiety WinSCP i PuTTY dla Windows. Nawiązywanie połączenia za pomocą klucza publicznego w systemie SSH.	1
W4	Zabezpieczanie połączeń internetowych: pakiet Secure Socket Layer. Korzystanie z pakietu. certyfikaty, elementy certyfikatu, instytucje certyfikujące.	1
W5	Wykrywanie włamań do systemów komputerowych. Analiza zachowań użytkowników. Analiza statystyczna i analiza na podstawie reguł.	1
W6	Szkodliwe programy: wirusy komputerowe, robaki, zombie, konie trojańskie i inne. Klasyfikacja, struktura, sposób działania wirusów i robaków.	1
W7	Ochrona przed wirusami i innymi złośliwymi programami: programy antywirusowe, klasyfikacja, metody działania. Systemy immunologiczne.	1
W8	Ściany ogniowe: zasady konstrukcji, funkcje, cele, rodzaje, konfiguracje. Kontrola dostępu do danych. Systemy zaufane.	1
W9	Zastosowania technik kryptograficznych: wybory elektroniczne, cyfrowe pieniądze.	1

LABORATORIUM		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
L1	Przypomnienie podstawowych pojęć z dziedziny algebry, wykorzystywanych w dalszym procesie kształcenia.	1
L2	Bezpieczeństwo systemu operacyjnego Linux	2
L3	Bezpieczeństwo systemu operacyjnego Windows	2
L4	Wprowadzenie do pakietu OpenSSL.	2
L5	Wykorzystanie pakietu OpenSSL do budowy bezpiecznych aplikacji.	2

7 NARZĘDZIA DYDAKTYCZNE

N1 Ćwiczenia laboratoryjne

N2 Dyskusja

N3 Wykłady

N4 Konsultacje

8 OBCIĄŻENIE PRACĄ STUDENTA

FORMA AKTYWNOŚCI	ŚREDNIA LICZBA GODZIN NA ZREALIZOWANIE AKTYWNOŚCI
Godziny kontaktowe z nauczycielem akademickim, w tym:	
Godziny wynikające z planu studiów	18
Konsultacje przedmiotowe	13
Egzaminy i zaliczenia w sesji	10
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	50
Opracowanie wyników	20
Przygotowanie raportu, projektu, prezentacji, dyskusji	30
SUMARYCZNA LICZBA GODZIN DLA PRZEDMIOTU WYNIKAJĄCA Z CAŁEGO NAKŁADU PRACY STUDENTA	141
SUMARYCZNA LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU	5.00

9 SPOSOBY OCENY

OCENA FORMUJĄCA

F1 Ćwiczenie praktyczne

F2 Odpowiedź ustna

F3 Sprawozdanie z ćwiczenia laboratoryjnego

OCENA PODSUMOWUJĄCA

P1 Średnia ważona ocen formujących

P2 Test

WARUNKI ZALICZENIA PRZEDMIOTU

W1 Zaliczenie ćwiczeń mogą uzyskać studenci, którzy regularnie uczęszczali na ćwiczenia

W2 Do egzaminu mogą przystąpić studenci, którzy wcześniej uzyskali zaliczenie ćwiczeń laboratoryjnych.

W3 Egzamin ma formę testu lub odpowiedzi ustnej

W4 Ocena końcowa jest średnią z ocen P1-P2.

OCENA AKTYWNOŚCI BEZ UDZIAŁU NAUCZYCIELA

B1 Podstawą oceny aktywności bez udziału nauczyciela jest ocena przygotowanego przez studenta sprawozdania z laboratorium.

KRYTERIA OCENY

EFEKT KSZTAŁCENIA 1	
NA OCENĘ 2.0	Student nie zna ogólnych zasad działania szkodliwych programów komputerowych (wirusy i inne) lub zasad wyboru i kontroli hasel.
NA OCENĘ 3.0	Student zna ogólne zasady działania szkodliwych programów komputerowych (wirusy i inne), zasady wyboru i kontroli hasel.
NA OCENĘ 3.5	Student zna różne zasady działania szkodliwych programów komputerowych (wirusy i inne), zasady wyboru i kontroli hasel.
NA OCENĘ 4.0	Student zna i rozumie różne zasady działania szkodliwych programów komputerowych (wirusy i inne), zasady wyboru i kontroli hasel.
NA OCENĘ 4.5	Student zna i prawidłowo rozumie różne zasady działania szkodliwych programów komputerowych (wirusy i inne), zasady wyboru i kontroli hasel. Potrafi uzupełniać wiadomości uzyskane podczas zajęć informacjami z innych źródeł.
NA OCENĘ 5.0	Student zna i w pełni prawidłowo rozumie różne zasady działania szkodliwych programów komputerowych (wirusy i inne), zasady wyboru i kontroli hasel. Potrafi uzupełniać wiadomości uzyskane podczas zajęć informacjami z innych źródeł. Potrafi wyciągać logiczne wnioski z posiadanych w tym zakresie informacji.

EFEKT KSZTAŁCENIA 2	
NA OCENĘ 2.0	Student nie potrafi wymienić i opisać podstawowych zagrożeń dla systemu komputerowego i sieci komputerowej.
NA OCENĘ 3.0	Student potrafi wymienić i opisać podstawowe zagrożenia dla systemu komputerowego i sieci komputerowej.
NA OCENĘ 3.5	Student potrafi wymienić i opisać różne zagrożenia dla systemu komputerowego i sieci komputerowej.
NA OCENĘ 4.0	Student potrafi wymienić i prawidłowo opisać różne zagrożenia dla systemu komputerowego i sieci komputerowej.
NA OCENĘ 4.5	Student potrafi wymienić i prawidłowo opisać różne zagrożenia dla systemu komputerowego i sieci komputerowej. Potrafi uzupełniać wiadomości uzyskane podczas zajęć informacjami z innych źródeł.
NA OCENĘ 5.0	Student potrafi wymienić i prawidłowo opisać różne zagrożenia dla systemu komputerowego i sieci komputerowej. Potrafi uzupełniać wiadomości uzyskane podczas zajęć informacjami z innych źródeł. Potrafi wskazać zagrożenia dla systemu komputerowego i sieci komputerowej w konkretnych sytuacjach.
EFEKT KSZTAŁCENIA 3	
NA OCENĘ 2.0	Student nie zna podstawowych metod identyfikacji i uwierzytelniania użytkownika, zabezpieczenia połączeń internetowych, sposobów ochrony przed wirusami, metod wykrywania intruzów, zasad działania ścian ogniowych.
NA OCENĘ 3.0	Student zna podstawowe metody identyfikacji i uwierzytelniania użytkownika, zabezpieczenia połączeń internetowych, sposoby ochrony przed wirusami, metody wykrywania intruzów, zasady działania ścian ogniowych.
NA OCENĘ 3.5	Student zna różne metody identyfikacji i uwierzytelniania użytkownika, zabezpieczenia połączeń internetowych, sposoby ochrony przed wirusami, metody wykrywania intruzów, zasady działania ścian ogniowych.
NA OCENĘ 4.0	Student zna i rozumie różne metody identyfikacji i uwierzytelniania użytkownika, zabezpieczenia połączeń internetowych, sposoby ochrony przed wirusami, metody wykrywania intruzów, zasady działania ścian ogniowych.
NA OCENĘ 4.5	Student zna i prawidłowo rozumie różne metody identyfikacji i uwierzytelniania użytkownika, zabezpieczenia połączeń internetowych, sposoby ochrony przed wirusami, metody wykrywania intruzów, zasady działania ścian ogniowych. Potrafi uzupełniać wiadomości uzyskane podczas zajęć informacjami z innych źródeł.
NA OCENĘ 5.0	Student zna i i w pełni prawidłowo rozumie różne metody identyfikacji i uwierzytelniania użytkownika, zabezpieczenia połączeń internetowych, sposoby ochrony przed wirusami, metody wykrywania intruzów, zasady działania ścian ogniowych. Potrafi uzupełniać wiadomości uzyskane podczas zajęć informacjami z innych źródeł. Potrafi wyciągać logiczne wnioski z posiadanych w tym zakresie informacji.
EFEKT KSZTAŁCENIA 4	

NA OCENĘ 2.0	Student nie potrafi wykonać poprawnie dwóch z następujących zadań: zastosować wybraną metodę zapewnienia bezpieczeństwa danych w wybranym systemie operacyjnym, zaszyfrować plik danych szyfrem blokowym DES, wykorzystać podstawowe komendy pakietu OpenSSL w trybie z linii komend w celu budowy centrum certyfikującego.
NA OCENĘ 3.0	Student potrafi wykonać poprawnie dwa z następujących zadań: zastosować wybraną metodę zapewnienia bezpieczeństwa danych w wybranym systemie operacyjnym, zaszyfrować plik danych szyfrem blokowym DES, wykorzystać podstawowe komendy pakietu OpenSSL w trybie z linii komend w celu budowy centrum certyfikującego.
NA OCENĘ 3.5	Student potrafi wykonać poprawnie wszystkich następujących zadań: zastosować wybraną metodę zapewnienia bezpieczeństwa danych w systemie operacyjnym, zaszyfrować plik danych szyfrem blokowym DES, wykorzystać podstawowe komendy pakietu OpenSSL w trybie z linii komend w celu budowy centrum certyfikującego
NA OCENĘ 4.0	Student potrafi wykonać poprawnie wszystkie z następujących zadań: zastosować wybraną metodę zapewnienia bezpieczeństwa danych w systemie operacyjnym, zaszyfrować plik danych szyfrem blokowym DES, wykorzystać podstawowe komendy pakietu OpenSSL w trybie z linii komend w celu budowy centrum certyfikującego
NA OCENĘ 4.5	Student potrafi wykonać w pełni prawidłowo wszystkie z następujących zadań: zastosować wybraną metodę zapewnienia bezpieczeństwa danych w systemie operacyjnym, zaszyfrować plik danych szyfrem blokowym DES, wykorzystać zaawansowane komendy pakietu OpenSSL w trybie z linii komend w celu budowy centrum certyfikującego, potrafi zaimplementować aplikacje, wykorzystując narzędzia OpenSSL
NA OCENĘ 5.0	Student potrafi wykonać w pełni prawidłowo wszystkie z następujących zadań: zastosować wybrane metody zapewnienia bezpieczeństwa danych w systemie operacyjnym Linux i Windows, zaszyfrować plik danych szyfrem blokowym DES, wykorzystać zaawansowane komendy pakietu OpenSSL w trybie z linii komend w celu budowy centrum certyfikującego, potrafi zaimplementować aplikacje, wykorzystując narzędzia OpenSSL z pełnym zrozumieniem wykorzystanych metod i algorytmów.
EFEKT KSZTAŁCENIA 5	
NA OCENĘ 2.0	Student nie potrafi pracować w zespole.
NA OCENĘ 3.0	Student potrafi pracować w zespole.
NA OCENĘ 4.0	Student potrafi pracować twórczo w zespole, wywiera wpływ na kierunek jego pracy.
NA OCENĘ 5.0	Student potrafi pracować twórczo w zespole, wywiera wpływ na kierunek jego pracy, potrafi zmotywować innych do podjęcia wysiłków celem realizacji zamierzonych wyników.

10 MACIERZ REALIZACJI PRZEDMIOTU

EFEKT KSZTAŁCENIA	ODNIESIENIE DANEGO EFEKTU DO SZCZEGÓŁOWYCH EFEKTÓW ZDEFINIOWANYCH DLA PROGRAMU	CELE PRZEDMIOTU	TREŚCI PROGRAMOWE	NARZĘDZIA DYDAKTYCZNE	SPOSOBY OCENY
EK1		Cel 1	W1 W2 W5 W6 L1 L2 L3	N2 N3 N4	F1 F2 F3 P1 P2
EK2		Cel 1	W1 W2 W5 W6 L1 L2 L3	N1 N2 N4	F1 F2 F3 P1 P2
EK3		Cel 2	W1 W3 W4 W7 W8 W9 L1 L4 L5	N2 N3 N4	F1 F2 F3 P1 P2
EK4		Cel 2	W1 W3 W4 W7 W8 W9 L1 L4 L5	N1 N3 N4	F1 F2 F3 P1 P2
EK5		Cel 1 Cel 2	L1 L2 L3 L4 L5	N2 N3 N4	F1 F3

11 WYKAZ LITERATURY

LITERATURA PODSTAWOWA

- [1] | Ogiela M. — *Bezpieczeństwo systemów komputerowych*,, Kraków, 2002, Wyd. AGH
- [2] | Stallings W. — *Kryptografia i bezpieczeństwo sieci komputerowych : koncepcje i metody bezpiecznej komunikacji*, Gliwice, 2012, Helion

LITERATURA UZUPEŁNIAJĄCA

- [1] | Stallings, W — *Kryptografia i bezpieczeństwo sieci komputerowych : matematyka szyfrów i techniki kryptologii*,, Gliwice, 2012, Helion
- [2] | B. Schneier — *Kryptografia dla praktyków*, Warszawa, 2002, WNT

LITERATURA DODATKOWA

- [1] | Karbowski M. — *Podstawy kryptografii*, Gliwice, 2014, Helion
- [2] | Szeliga M — *Bezpieczeństwo w sieciach Windows : kompendium administratora sieci*, Gliwice, 2003, Helion

12 INFORMACJE O NAUCZYCIELACH AKADEMICKICH

OSOBA ODPOWIEDZIALNA ZA KARTĘ

dr Agnieszka Jakóbik (kontakt: akrok@pk.edu.pl)

OSOBY PROWADZĄCE PRZEDMIOT

1 Dr Agnieszka Jakóbik (kontakt: akrok@pk.edu.pl)

2 Mgr Jacek Tchórzewski (kontakt: jacek.tchorzewski@onet.pl)

13 ZATWIERDZENIE KARTY PRZEDMIOTU DO REALIZACJI

(miejscowość, data)

(odpowiedzialny za przedmiot)

(dziekan)

PRZYJMUJĘ DO REALIZACJI (data i podpisy osób prowadzących przedmiot)

.....

.....