

# POLITECHNIKA KRAKOWSKA IM. TADEUSZA KOŚCIUSZKI

## KARTA PRZEDMIOTU

obowiązuje studentów rozpoczynających studia w roku akademickim 2014/2015

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<br>W JĘZYKU ANGIELSKIM |                                              |
| KOD PRZEDMIOTU                          | WFMiI I oIIN D7 14/15                        |
| KATEGORIA PRZEDMIOTU                    | Przedmioty specjalnościowe                   |
| LICZBA PUNKTÓW ECTS                     | 5.00                                         |
| SEMESTRY                                | 3                                            |

### 2 RODZAJ ZAJĘĆ, LICZBA GODZIN W PLANIE STUDIÓW

| SEMESTR | WYKŁAD | ĆWICZENIA | LABORATORIUM | LABORATORIUM<br>KOMPUTERO-<br>WE | SEMINARIUM | PROJEKT |
|---------|--------|-----------|--------------|----------------------------------|------------|---------|
| 3       | 18     | 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

## 6 TREŚCI PROGRAMOWE

| WYKŁAD    |                                                                                                                                                                                                                              |                  |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| LP        | TEMATYKA ZAJĘĆ<br>OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH                                                                                                                                                                       | LICZBA<br>GODZIN |
| <b>W1</b> | Wstęp: potrzeba zabezpieczenia systemów komputerowych. Kryptografia i kryptoanaliza. Systemy kryptograficzne symetryczne i asymetryczne.                                                                                     | 2                |
| <b>W2</b> | Identyfikacja i uwierzytelnianie użytkownika: system hasel. Przechowywanie hasel, weryfikacja hasel. Ataki na system hasel. Słabe hasła. Weryfikacja hasel. Hasła jednorazowe. System Kerberos.                              | 2                |
| <b>W3</b> | 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. | 2                |
| <b>W4</b> | Zabezpieczanie połączeń internetowych: pakiet Secure Socket Layer. Korzystanie z pakietu. certyfikaty, elementy certyfikatu, instytucje certyfikujące.                                                                       | 2                |
| <b>W5</b> | Wykrywanie włamań do systemów komputerowych. Analiza zachowań użytkowników. Analiza statystyczna i analiza na podstawie reguł.                                                                                               | 2                |
| <b>W6</b> | Szkodliwe programy: wirusy komputerowe, robaki, zombie, konie trojańskie i inne. Klasyfikacja, struktura, sposób działania wirusów i robaków.                                                                                | 2                |
| <b>W7</b> | Ochrona przed wirusami i innymi złośliwymi programami: programy antywirusowe, klasyfikacja, metody działania. Systemy immunologiczne.                                                                                        | 2                |
| <b>W8</b> | Ściany ogniowe: zasady konstrukcji, funkcje, cele, rodzaje, konfiguracje. Kontrola dostępu do danych. Systemy zaufane.                                                                                                       | 2                |
| <b>W9</b> | Zastosowania technik kryptograficznych: wybory elektroniczne, cyfrowe pieniądze.                                                                                                                                             | 2                |

| LABORATORIUM |                                                                                                        |                  |
|--------------|--------------------------------------------------------------------------------------------------------|------------------|
| LP           | TEMATYKA ZAJĘĆ<br>OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH                                                 | LICZBA<br>GODZIN |
| <b>L1</b>    | Przypomnienie podstawowych pojęć z dziedziny algebry, wykorzystywanych w dalszym procesie kształcenia. | 1                |
| <b>L2</b>    | Bezpieczeństwo systemu operacyjnego Linux                                                              | 2                |
| <b>L3</b>    | Bezpieczeństwo systemu operacyjnego Windows                                                            | 2                |
| <b>L4</b>    | Wprowadzenie do pakietu OpenSSL.                                                                       | 2                |
| <b>L5</b>    | 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<br>NA ZREALIZOWANIE<br>AKTYWNOŚCI |
|--------------------------------------------------------------------------------------------------|---------------------------------------------------------|
| <b>Godziny kontaktowe z nauczycielem akademickim, w tym:</b>                                     |                                                         |
| Godziny wynikające z planu studiów                                                               | 0                                                       |
| Konsultacje przedmiotowe                                                                         | 13                                                      |
| Egzaminy i zaliczenia w sesji                                                                    | 10                                                      |
| <b>Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:</b> |                                                         |
| Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury                               | 50                                                      |
| Opracowanie wyników                                                                              | 0                                                       |
| Przygotowanie raportu, projektu, prezentacji, dyskusji                                           | 50                                                      |
| <b>SUMARYCZNA LICZBA GODZIN DLA PRZEDMIOTU WYNIKAJĄCA Z<br/>CAŁEGO NAKŁADU PRACY STUDENTA</b>    | <b>123</b>                                              |
| 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.

### 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 haseł.                                                                                                                                                                                    |
| NA OCENĘ 3.0        | Student zna ogólne zasady działania szkodliwych programów komputerowych (wirusy i inne), zasady wyboru i kontroli haseł.                                                                                                                                                                                           |
| NA OCENĘ 3.5        | Student zna różne zasady działania szkodliwych programów komputerowych (wirusy i inne), zasady wyboru i kontroli haseł.                                                                                                                                                                                            |
| NA OCENĘ 4.0        | Student zna i rozumie różne zasady działania szkodliwych programów komputerowych (wirusy i inne), zasady wyboru i kontroli haseł.                                                                                                                                                                                  |
| NA OCENĘ 4.5        | Student zna i prawidłowo rozumie różne zasady działania szkodliwych programów komputerowych (wirusy i inne), zasady wyboru i kontroli haseł. 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 haseł. 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 metody 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 metody 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 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 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 trybie z linii komend w celu budowy centrum certyfikującego, potrafi zaimplementować aplikacje, wykorzystując narzędzia OpenSSL z pełnym zrozumieniem wykorzystanych metod i algorytmów. |

## 10 MACIERZ REALIZACJI PRZEDMIOTU

| EFEKT KSZTAŁCENIA | ODNIESIENIE DANEGO EFEKTU DO SZCZEGÓŁOWYCH EFEKTÓW ZDEFINIOWANYCH DLA PROGRAMU | CELE PRZEDMIOTU | TREŚCI PROGRAMOWE       | NARZĘDZIA DYDAKTYCZNE | SPOSOBY OCENY  |
|-------------------|--------------------------------------------------------------------------------|-----------------|-------------------------|-----------------------|----------------|
| EK1               | I2_W03,<br>I2_W08                                                              | Cel 1           | W1 W2 W5 W6<br>L1 L2 L3 | N2 N3 N4              | F1 F2 F3 P1 P2 |
| EK2               | I2_W03,<br>I2_W08,<br>I2_U03, I2_U10                                           | Cel 1           | W1 W2 W5 W6<br>L1 L2 L3 | N1 N2 N4              | F1 F2 F3 P1 P2 |

| EFEKT KSZTAŁCENIA | ODNIESIENIE DANEGO EFEKTU DO SZCZEGÓŁOWYCH EFEKTÓW ZDEFINIOWANYCH DLA PROGRAMU | CELE PRZEDMIOTU | TREŚCI PROGRAMOWE                | NARZĘDZIA DYDAKTYCZNE | SPOSOBY OCENY  |
|-------------------|--------------------------------------------------------------------------------|-----------------|----------------------------------|-----------------------|----------------|
| EK3               | I2_W03,<br>I2_W08                                                              | Cel 2           | W1 W3 W4 W7<br>W8 W9 L1 L4<br>L5 | N2 N3 N4              | F1 F2 F3 P1 P2 |
| EK4               | I2_U03, I2_U10                                                                 | Cel 2           | W1 W3 W4 W7<br>W8 W9 L1 L4<br>L5 | N1 N3 N4              | F1 F2 F3 P1 P2 |

## 11 WYKAZ LITERATURY

### LITERATURA PODSTAWOWA

- [1] | M. Kutylowski, W.B. Strothmann — *Kryptografia. Teoria i praktyka zabezpieczania systemów komputerowych*, Warszawa, 1999, ReadMe
- [2] | J. Pieprzyk, T. Hardjono, J. Seeberry — *Teoria bezpieczeństwa systemów komputerowych*, Gliwice, 2004, Helion

### LITERATURA UZUPEŁNIAJĄCA

- [1] | M. Karpiński, I. P. Kurytnik — *Sieci komputerowe: bezpieczeństwo*, Bielsko - Biała, 2006, Wyd. ATH
- [2] | B. Schneier — *Kryptografia dla praktyków*, Warszawa, 2002, WNT

## 12 INFORMACJE O NAUCZYCIELACH AKADEMICKICH

### OSOBA ODPOWIEDZIALNA ZA KARTĘ

dr hab. Andrzej Karafiat (kontakt: akaraf@pk.edu.pl)

### OSOBY PROWADZĄCE PRZEDMIOT

- 1 Dr hab Andrzej Karafiat (kontakt: akaraf@pk.edu.pl)
- 2 Dr Agnieszka Krok (kontakt: agakrok@poczta.fm)

## 13 ZATWIERDZENIE KARTY PRZEDMIOTU DO REALIZACJI

(miejscowość, data) (odpowiedzialny za przedmiot) (dziekan)

PRZYJMUJĘ DO REALIZACJI (data i podpisy osób prowadzących przedmiot)

.....  
.....