

# 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: stacjonarne

Kod kierunku: I

Stopień studiów: II

Specjalności: Teleinformatyka dla licencjatów

### 1 INFORMACJE O PRZEDMIOCIE

|                                         |                                             |
|-----------------------------------------|---------------------------------------------|
| NAZWA PRZEDMIOTU                        | Bezpieczeństwo systemów teleinformatycznych |
| NAZWA PRZEDMIOTU<br>W JĘZYKU ANGIELSKIM | Security of ICT systems                     |
| KOD PRZEDMIOTU                          | WFMiI I oIIS D8 17/18                       |
| KATEGORIA PRZEDMIOTU                    | Przedmioty specjalnościowe                  |
| LICZBA PUNKTÓW ECTS                     | 4.00                                        |
| SEMESTRY                                | 4                                           |

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

| SEMESTR | WYKŁAD | ĆWICZENIA | LABORATORIUM | LABORATORIUM<br>KOMPUTERO-<br>WE | SEMINARIUM | PROJEKT |
|---------|--------|-----------|--------------|----------------------------------|------------|---------|
| 4       | 30     | 0         | 30           | 0                                | 0          | 0       |

### 3 CELE PRZEDMIOTU

**Cel 1** Poszerzenie wiedzy studenta z zakresu bezpieczeństwa systemów teleinformatycznych zdobytą na przedmiocie bezpieczeństwo systemów komputerowych.

**Cel 2** Zapoznanie studentów z wybranymi technikami i rozwiązaniami, których zadaniem jest zapewnienie bezpiecznej komunikacji w sieciach teleinformatycznych.

**Cel 3** Zapoznanie studentów z wybranymi protokołami sieciowymi gwarantującymi bezpieczeństwo transmisji danych w systemach teleinformatycznych.

**Cel 4** Zapoznanie studentów z podstawowymi technikami testowania zabezpieczeń systemów teleinformatycznych.

## 4 WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

1 Zaliczenie przedmiotu sieci komputerowe.

2 Zaliczenie przedmiotu bezpieczeństwo systemów komputerowych.

## 5 EFEKTY KSZTAŁCENIA

**EK1 Wiedza** Student zna i potrafi omówić techniki odzyskiwania plików, zagadnienia bezpieczeństwa aplikacji mobilnych, .NET i aplikacji internetowych, zagadnienia cyberbezpieczeństwa i chmury obliczeniowej, podstawowe techniki biometryczne.

**EK2 Umiejętności** Student potrafi konfigurować urządzenia klasy SSL VPN Gateway.

**EK3 Umiejętności** Student potrafi przedstawić i omówić podstawowe techniki przeprowadzania testów zabezpieczeń systemów teleinformatycznych.

**EK4 Kompetencje społeczne** Umie - zgodnie z zadaną specyfikacją - zaprojektować oraz zrealizować prosty system informatyczny, używając właściwych metod, technik i narzędzi.

## 6 TREŚCI PROGRAMOWE

| LABORATORIUM |                                                                          |                  |
|--------------|--------------------------------------------------------------------------|------------------|
| LP           | TEMATYKA ZAJĘĆ<br>OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH                   | LICZBA<br>GODZIN |
| L1           | Bezpieczeństwo i odzyskiwanie danych                                     | 4                |
| L2           | Bezpieczeństwo aplikacji mobilnych, .NET i internetowych                 | 4                |
| L3           | Cyberbezpieczeństwo                                                      | 4                |
| L4           | Bezpieczeństwo chmury obliczeniowej                                      | 2                |
| L5           | Biometria                                                                | 4                |
| L6           | Podstawowe techniki zbierania informacji o systemach teleinformatycznych | 4                |
| L7           | Testowanie zabezpieczeń systemów teleinformatycznych                     | 4                |
| L8           | Bezpieczeństwo serwera sieciowego                                        | 4                |

| WYKŁAD |                                                        |                  |
|--------|--------------------------------------------------------|------------------|
| LP     | TEMATYKA ZAJĘĆ<br>OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH | LICZBA<br>GODZIN |

| WYKŁAD     |                                                                                      |                  |
|------------|--------------------------------------------------------------------------------------|------------------|
| LP         | TEMATYKA ZAJĘĆ<br>OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH                               | LICZBA<br>GODZIN |
| <b>W2</b>  | Bezpieczeństwo i odzyskiwanie danych                                                 | 4                |
| <b>W3</b>  | Bezpieczeństwo aplikacji mobilnych, .NET i internetowych                             | 4                |
| <b>W5</b>  | Cyberbezpieczeństwo                                                                  | 4                |
| <b>W7</b>  | Bezpieczeństwo chmury obliczeniowej                                                  | 2                |
| <b>W8</b>  | Biometria                                                                            | 4                |
| <b>W9</b>  | Omówienie podstawowych technik zbierania informacji o systemach teleinformatycznych. | 4                |
| <b>W10</b> | Omówienie technik testowania zabezpieczeń systemów teleinformatycznych.              | 4                |
| <b>W11</b> | Bezpieczeństwo serwera sieciowego.                                                   | 4                |

## 7 NARZĘDZIA DYDAKTYCZNE

**N1** Wykłady

**N2** Ćwiczenia laboratoryjne

**N3** Prezentacje multimedialne

**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                                                               | 60                                                      |
| Konsultacje przedmiotowe                                                                         | 0                                                       |
| Egzaminy i zaliczenia w sesji                                                                    | 0                                                       |
| <b>Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:</b> |                                                         |
| Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury                               | 60                                                      |
| Opracowanie wyników                                                                              | 0                                                       |
| Przygotowanie raportu, projektu, prezentacji, dyskusji                                           | 0                                                       |
| <b>SUMARYCZNA LICZBA GODZIN DLA PRZEDMIOTU WYNIKAJĄCA Z<br/>CAŁEGO NAKŁADU PRACY STUDENTA</b>    | <b>120</b>                                              |
| SUMARYCZNA LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU                                                    | 4.00                                                    |

## 9 SPOSOBY OCENY

### OCENA FORMUJĄCA

**F1** Ćwiczenie praktyczne

**F2** Kolokwium

### OCENA PODSUMOWUJĄCA

**P1** Egzamin pisemny

**P2** Średnia ważona ocen formujących

### WARUNKI ZALICZENIA PRZEDMIOTU

**W1** Konieczność zaliczenia wszystkich kolokwiów oraz ćwiczenia praktycznego przed przystąpieniem do egzaminu.

### KRYTERIA OCENY

| EFEKT KSZTAŁCENIA 1 |                                                                                                        |
|---------------------|--------------------------------------------------------------------------------------------------------|
| NA OCENĘ 2.0        | Student nie potrafi konfigurować zaawansowanych funkcjonalności bezpieczeństwa dla urządzeń klasy XTM. |
| NA OCENĘ 3.0        | Student potrafi integrować urządzenie klasy XTM z zewnętrzną bazą autentykacji.                        |

|                     |                                                                                                                                                                                                                  |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NA OCENĘ 3.5        | Student potrafi konfigurować funkcjonalność SSO dla urządzeń klasy XTM.                                                                                                                                          |
| NA OCENĘ 4.0        | Student potrafi konfigurować filtr ochrony antyspamowej w urządzeniach klasy XTM.                                                                                                                                |
| NA OCENĘ 4.5        | Student potrafi konfigurować filtr ochrony przed intruzami w urządzeniach klasy XTM.                                                                                                                             |
| NA OCENĘ 5.0        | Student potrafi testować jakość ochrony realizowanej przez urządzenie klasy XTM.                                                                                                                                 |
| EFEKT KSZTAŁCENIA 2 |                                                                                                                                                                                                                  |
| NA OCENĘ 2.0        | Student nie potrafi konfigurować podstawowych funkcjonalności urządzeń klasy SSL VPN Gateway.                                                                                                                    |
| NA OCENĘ 3.0        | Student nie potrafi konfigurować podstawowe funkcjonalności urządzeń klasy SSL VPN Gateway.                                                                                                                      |
| NA OCENĘ 3.5        | Student potrafi integrować urządzenie SSL VPN Gateway z zewnętrzną bazą autentykacji.                                                                                                                            |
| NA OCENĘ 4.0        | Student potrafi konfigurować wszystkie typy autentykacji dostępne w urządzeniu SSL VPN Gateway. Student potrafi tworzyć nowe zasoby.                                                                             |
| NA OCENĘ 4.5        | Student potrafi konfigurować reguły dostępu do zasobów obejmujące weryfikacje zabezpieczeń systemu operacyjnego, z którego następuje połączenie oraz usuwanie wszelkich danych po zakończonej sesji użytkownika. |
| NA OCENĘ 5.0        | Student potrafi personalizować portal z zasobami oraz analizować logi i generować raporty aktywności.                                                                                                            |
| EFEKT KSZTAŁCENIA 3 |                                                                                                                                                                                                                  |
| NA OCENĘ 2.0        | Student nie potrafi wymienić podstawowych protokołów sieciowych gwarantujących bezpieczeństwo transmisji danych w systemach teleinformatycznych.                                                                 |
| NA OCENĘ 3.0        | Student potrafi wymienić podstawowe protokoły sieciowe gwarantujące bezpieczeństwo transmisji danych w systemach teleinformatycznych.                                                                            |
| NA OCENĘ 3.5        | Student potrafi wskazać zmiany wprowadzone w bezpiecznych protokołach względem standardowych protokołów i uzasadnić ich znaczenie dla bezpieczeństwa transmisji w systemach teleinformatycznych.                 |
| NA OCENĘ 4.0        | Student potrafi zaprezentować zasadę działania protokołu DNSSec.                                                                                                                                                 |
| NA OCENĘ 4.5        | Student potrafi przedstawić zasadę działania protokołu SSL.                                                                                                                                                      |
| NA OCENĘ 5.0        | Student potrafi ze szczegółami omówić proces nawiązywania połączenia SSL.                                                                                                                                        |
| EFEKT KSZTAŁCENIA 4 |                                                                                                                                                                                                                  |
| NA OCENĘ 2.0        | Student nie potrafi wymienić podstawowych technik przeprowadzania testów zabezpieczeń systemów teleinformatycznych.                                                                                              |

|              |                                                                                                                |
|--------------|----------------------------------------------------------------------------------------------------------------|
| NA OCENĘ 3.0 | Student potrafi wymienić podstawowe techniki przeprowadzania testów zabezpieczeń systemów teleinformatycznych. |
| NA OCENĘ 3.5 | Student potrafi zaprezentować podstawowe techniki zbierania informacji o systemach teleinformatycznych.        |
| NA OCENĘ 4.0 | Student potrafi zaprezentować techniki łamania haseł.                                                          |
| NA OCENĘ 4.5 | Student potrafi omówić podstawowe narzędzia i techniki weryfikowania zabezpieczeń usług sieciowych.            |
| NA OCENĘ 5.0 | Student potrafi omówić zastosowanie narzędzi zgromadzonych w ramach dystrybucji BackTrack.                     |

## 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_W02                                                                         | Cel 1           | W2 W3 W5 W7<br>W8 W9 W10<br>W11 | N1 N3 N4              | F1 F2 P1 P2   |
| EK2               | I2_U06                                                                         | Cel 2           | L1 L2 L3 L4 L5<br>L6 L7 L8      | N1 N2 N3 N4           | F1 F2 P1 P2   |
| EK3               | I2_U11                                                                         | Cel 3           | L1 L2 L3 L4 L5<br>L6 L7 L8      | N1 N3 N4              | F2 P1         |
| EK4               | I2_K02                                                                         | Cel 2 Cel 3     | L1 L2 L3 L4 L5<br>L6 L7 L8      | N2 N3 N4              | F1            |

## 11 WYKAZ LITERATURY

### LITERATURA PODSTAWOWA

- [1] | **RFC** — *Dokumenty RFC dla DNSSec, SSL.*, RFC, 2011, RFC
- [2] | **Honeypots.net** — <http://www.honeypots.net/>, www, 2011, Honeypots.net
- [3] | **Dnssec.net** — <http://www.dnssec.net/>, www, 2011, Dnssec.net
- [4] | **Sourcefire** — <http://www.snort.org/>, www, 2011, Sourcefire

- [5] | **Michał Piotrowski** — *Królicza nora : ochrona sieci komputerowych za pomocą technologii honeypot*, Warszawa, 2007, PWN
- [6] | **Rolf Oppliger** — *SSL and TLS Theory and Practice*, Norwood, 2009, Artech House
- [7] | **Bauer, Michael D.** — *Linux : serwery : bezpieczeństwo : kompendium wiedzy o ochronie serwerów linuxowych przed atakami z sieci*, Gliwice, 2005, Helion

#### LITERATURA UZUPEŁNIAJĄCA

- [1] | **Alex Lukatsky** — *Wykrywanie włamań i aktywna ochrona danych : elita rosyjskich hakerów prezentuje*, Gliwice, 2005, Helion
- [2] | **Łuczak Jacek** — *Zarządzanie bezpieczeństwem informacji : praca zbiorowa / Jacek Łuczak (red.)*, Poznań, 2004, Oficyna Współczesna

## 12 INFORMACJE O NAUCZYCIELACH AKADEMICKICH

### OSOBA ODPOWIEDZIALNA ZA KARTĘ

dr inż. Krzysztof Rzecki (kontakt: [krz@pk.edu.pl](mailto:krz@pk.edu.pl))

### OSOBY PROWADZĄCE PRZEDMIOT

1 mgr inż. Tomasz Sośnicki (kontakt: [tsosnicki@pk.edu.pl](mailto:tsosnicki@pk.edu.pl))

2 dr inż. Krzysztof Rzecki (kontakt: [krz@itt.pk.edu.pl](mailto:krz@itt.pk.edu.pl))

## 13 ZATWIERDZENIE KARTY PRZEDMIOTU DO REALIZACJI

---

(miejscowość, data)

(odpowiedzialny za przedmiot)

(dziekan)

PRZYJMUJĘ DO REALIZACJI (data i podpisy osób prowadzących przedmiot)

.....  
.....