

# POLITECHNIKA KRAKOWSKA IM. TADEUSZA KOŚCIUSZKI

## KARTA PRZEDMIOTU

obowiązuje studentów rozpoczynających studia w roku akademickim 2012/2013

Wydział Fizyki, Matematyki i Informatyki

Kierunek studiów: Informatyka

Profil: Ogólnoakademicki

Forma studiów: niestacjonarne

Kod kierunku: I

Stopień studiów: I

Specjalności: Brak specjalności

### 1 INFORMACJE O PRZEDMIOCIE

|                                         |                                       |
|-----------------------------------------|---------------------------------------|
| NAZWA PRZEDMIOTU                        | Bezpieczeństwo systemów komputerowych |
| NAZWA PRZEDMIOTU<br>W JĘZYKU ANGIELSKIM |                                       |
| KOD PRZEDMIOTU                          | WFMiI I oIN D1 12/13                  |
| KATEGORIA PRZEDMIOTU                    | Przedmioty specjalnościowe            |
| LICZBA PUNKTÓW ECTS                     | 5.00                                  |
| SEMESTRY                                | 6                                     |

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

| SEMESTR | WYKŁAD | ĆWICZENIA | LABORATORIUM | LABORATORIUM<br>KOMPUTERO-<br>WE | SEMINARIUM | PROJEKT |
|---------|--------|-----------|--------------|----------------------------------|------------|---------|
| 6       | 18     | 0         | 18           | 0                                | 0          | 0       |

### 3 CELE PRZEDMIOTU

**Cel 1** Wprowadzenie w tematykę bezpieczeństwa systemów komputerowych.

**Cel 2** Zapoznanie z tematyką zabezpieczania przesyłania informacji.

**Cel 3** Zapoznanie studentów z metodami bezpiecznego łączenia geograficznie rozproszonych lokalizacji w logiczną wirtualną sieć.

- Cel 4** Zapoznanie studentów z metodami zapewniania bezpiecznego zdalnego dostępu do zasobów sieci chronionej.
- Cel 5** Zapoznanie studentów z technikami filtrowania ruchu sieciowego w warstwach od 3 wzwyż siedmiowarstwowego modelu sieci.
- Cel 6** Zapoznanie studentów ze sposobami konfigurowania filtrów pakietów oraz proxy filtrujących.
- Cel 7** Prezentacja metod realizacji redundancji systemów zabezpieczeń sieciowych.

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

- 1 Znajomość podstawowych protokołów sieciowych (m.in. Ethernet, ARP, RARP, ICMP, IP, TCP, UDP, DNS, HTTP, SMTP) i zasad działania sieci komputerowych.
- 2 Zaliczenie przedmiotu sieci komputerowe.

## 5 EFEKTY KSZTAŁCENIA

- EK1 Umiejętności** Student potrafi konfigurować zintegrowane sprzętowe urządzenia zabezpieczające sieć klasy XTM.
- EK2 Wiedza** Student potrafi przedstawić zasadę działania podstawowych metod zabezpieczania systemów komputerowych.
- EK3 Wiedza** Student potrafi przedstawić podstawowe metody bezpiecznej transmisji danych.
- EK4 Wiedza** Student potrafi przedstawić podstawowe zagrożenia systemów komputerowych.

## 6 TREŚCI PROGRAMOWE

| WYKŁAD    |                                                                                            |                  |
|-----------|--------------------------------------------------------------------------------------------|------------------|
| LP        | TEMATYKA ZAJĘĆ<br>OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH                                     | LICZBA<br>GODZIN |
| <b>W1</b> | Wstęp, omówienie zasad zaliczenia, prezentacja wykorzystywanych na laboratorium urządzeń.  | 2                |
| <b>W2</b> | Przedstawienie aktualnych trendów w bezpieczeństwie i ostatnio zidentyfikowanych zagrożeń. | 2                |
| <b>W3</b> | Aspekty bezpieczeństwa systemów informatycznych.                                           | 2                |
| <b>W4</b> | Realizacja usług zapewnienia bezpieczeństwa informacji.                                    | 2                |
| <b>W5</b> | Podstawowe typy i własności systemów kryptograficznych.                                    | 2                |
| <b>W6</b> | Infrastruktura Klucza Publicznego PKI.                                                     | 2                |
| <b>W7</b> | Zagrożenia zewnętrzne.                                                                     | 2                |
| <b>W8</b> | Systemy wykrywania włamań (IDS).                                                           | 2                |
| <b>W9</b> | Protokół IPSec.                                                                            | 2                |

| LABORATORIUM |                                                                                                    |                  |
|--------------|----------------------------------------------------------------------------------------------------|------------------|
| LP           | TEMATYKA ZAJĘĆ<br>OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH                                             | LICZBA<br>GODZIN |
| <b>L1</b>    | Quick Setup Wizard wstępna konfiguracja urządzeń klasy XTM.                                        | 2                |
| <b>L2</b>    | Konfiguracja filtrów pakietów.                                                                     | 2                |
| <b>L3</b>    | Konfiguracja Proxy filtrujących.                                                                   | 2                |
| <b>L4</b>    | Autentykacja użytkowników, tworzenie polityk bezpieczeństwa bazujących na tożsamości użytkowników. | 2                |
| <b>L5</b>    | Konfigurowanie tuneli VPN dla użytkowników mobilnych z wykorzystaniem PPTP, SSL oraz IPSec.        | 2                |
| <b>L6</b>    | Konfigurowanie statycznych tuneli VPN pomiędzy urządzeniami.                                       | 2                |
| <b>L7</b>    | Filtrowanie zawartości stron www (WebBlocker), kontrola aplikacji.                                 | 2                |
| <b>L8</b>    | Konfigurowanie modułu ochrony przed intruzami (IPS), klastrowanie urządzeń (Fire Cluster).         | 2                |
| <b>L9</b>    | Sprawdzian umiejętności konfigurowania urządzeń klasy XTM.                                         | 2                |

## 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                                                               | 0                                                       |
| 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                               | 114                                                     |
| Opracowanie wyników                                                                              | 0                                                       |
| Przygotowanie raportu, projektu, prezentacji, dyskusji                                           | 0                                                       |
| <b>SUMARYCZNA LICZBA GODZIN DLA PRZEDMIOTU WYNIKAJĄCA Z<br/>CAŁEGO NAKŁADU PRACY STUDENTA</b>    | <b>114</b>                                              |
| SUMARYCZNA LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU                                                    | 5.00                                                    |

## 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 podstawowych ustawień sieciowych urządzeń klasy XTM. Student nie potrafi konfigurować filtrów pakietów. |
| NA OCENĘ 3.0        | Student potrafi konfigurować podstawowe ustawienia sieciowe urządzeń klasy XTM. Student potrafi konfigurować filtry pakietów.            |

|                     |                                                                                                                                                                                                              |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NA OCENĘ 3.5        | Student potrafi konfigurować proxy filtrujące dla protokołów HTTP, HTTPS, DNS, FTP.                                                                                                                          |
| NA OCENĘ 4.0        | Student potrafi konfigurować tunele VPN, zarówno statyczne jak i mobilne. Student potrafi analizować zebrane logi oraz generować raporty aktywności użytkowników.                                            |
| NA OCENĘ 4.5        | Student potrafi konfigurować polityki bezpieczeństwa bazujące na tożsamości użytkowników. Student potrafi konfigurować zaawansowane ustawienia sieciowe urządzeń.                                            |
| NA OCENĘ 5.0        | Student potrafi konfigurować dodatkowe usługi bezpieczeństwa: ochrona przed spamem, IPS, ochrona antywirusowa, Application Control, filtrowanie zawartości stron www. Student potrafi klastrować urządzenia. |
| EFEKT KSZTAŁCENIA 2 |                                                                                                                                                                                                              |
| NA OCENĘ 2.0        | Student nie potrafi wymienić podstawowych metod zabezpieczania systemów komputerowych.                                                                                                                       |
| NA OCENĘ 3.0        | Student potrafi wymienić podstawowe metody zabezpieczania systemów komputerowych.                                                                                                                            |
| NA OCENĘ 3.5        | Student potrafi opisać zasadę działania zapory sieciowej, potrafi zaprezentować różnice pomiędzy poszczególnymi typami zapór sieciowych.                                                                     |
| NA OCENĘ 4.0        | Student potrafi zaprezentować zasadę działania oraz typy systemów ochrony przed intruzami (IDS).                                                                                                             |
| NA OCENĘ 4.5        | Student potrafi przedstawić typy ochrony antyspamowej oraz opisać ich zasadę działania.                                                                                                                      |
| NA OCENĘ 5.0        | Student potrafi opisać zasadę działania Proxy filtrujących.                                                                                                                                                  |
| EFEKT KSZTAŁCENIA 3 |                                                                                                                                                                                                              |
| NA OCENĘ 2.0        | Student nie potrafi wymienić podstawowych metod bezpiecznej transmisji danych.                                                                                                                               |
| NA OCENĘ 3.0        | Student potrafi wymienić podstawowe metody bezpiecznej transmisji danych.                                                                                                                                    |
| NA OCENĘ 3.5        | Student potrafi porównać zalety poszczególnych metod bezpiecznej transmisji danych.                                                                                                                          |
| NA OCENĘ 4.0        | Student potrafi opisać zasadę działania protokołu IPSec.                                                                                                                                                     |
| NA OCENĘ 4.5        | Student potrafi opisać zasadę działania, przedstawić strukturę oraz zależności pomiędzy elementami infrastruktury PKI.                                                                                       |
| NA OCENĘ 5.0        | Student potrafi opisać zasady ukrywania ruchu sieciowego w innych protokołach.                                                                                                                               |
| EFEKT KSZTAŁCENIA 4 |                                                                                                                                                                                                              |
| NA OCENĘ 2.0        | Student nie potrafi wymienić podstawowych zagrożeń systemów komputerowych.                                                                                                                                   |
| NA OCENĘ 3.0        | Student potrafi wymienić podstawowe zagrożenia systemów komputerowych.                                                                                                                                       |

|              |                                                                                                 |
|--------------|-------------------------------------------------------------------------------------------------|
| NA OCENĘ 3.5 | Student potrafi porównać poziom niebezpieczeństwa podstawowych zagrożeń systemów komputerowych. |
| NA OCENĘ 4.0 | Student potrafi opisać i porównać różne typy ataków DoS.                                        |
| NA OCENĘ 4.5 | Student potrafi opisać istotę i zasadę przeprowadzania ataków typu APT.                         |
| NA OCENĘ 5.0 | Student potrafi przedstawić podstawowe ataki kierowane przeciwko sieci Web.                     |

## 10 MACIERZ REALIZACJI PRZEDMIOTU

| EFEKT KSZTAŁCENIA | ODNIESIENIE DANEGO EFEKTU DO SZCZEGÓŁOWYCH EFEKTÓW ZDEFINIOWANYCH DLA PROGRAMU | CELE PRZEDMIOTU            | TREŚCI PROGRAMOWE                | NARZĘDZIA DYDAKTYCZNE | SPOSOBY OCENY |
|-------------------|--------------------------------------------------------------------------------|----------------------------|----------------------------------|-----------------------|---------------|
| EK1               | I1_U15,<br>I1_U16,<br>I1_U22, I1_U24                                           | Cel 3 Cel 5<br>Cel 6 Cel 7 | W1 L1 L2 L3 L4<br>L5 L6 L7 L8 L9 | N1 N2 N3 N4           | F1 P2         |
| EK2               | I1_W05                                                                         | Cel 2                      | W3 W4 W5 W6<br>W8                | N1 N2 N3 N4           | F2 P1 P2      |
| EK3               | I1_W11                                                                         | Cel 4                      | W9                               | N1 N2 N3 N4           | F2 P1 P2      |
| EK4               | I1_W14                                                                         | Cel 1                      | W2 W3 W7                         | N1 N3 N4              | F2 P1 P2      |

## 11 WYKAZ LITERATURY

### LITERATURA PODSTAWOWA

- [1 ] **WatchGuard** — <http://www.watchguard.com/help/docs/wsm/11/en-US/index.html>, www, 2011, WatchGuard
- [2 ] **Steve Friedl** — <http://unixwiz.net/techtips/iguide-ipsec.ht>, www, 2005, Steve Friedl
- [3 ] **Karen Scarfone, Peter Mell** — <http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf>, www, 2007, National Institute of Standards and Technology
- [4 ] **Carlisle Adams, Steve Lloyd** — *PKI podstawy i zasady działania : koncepcje, standardy i wdrażanie infrastruktury kluczy publicznych*, Warszawa, 2007, PWN

## 12 INFORMACJE O NAUCZYCIELACH AKADEMICKICH

### OSOBA ODPOWIEDZIALNA ZA KARTĘ

Marcin Klamra (kontakt: [mklamra@15.pk.edu.pl](mailto:mklamra@15.pk.edu.pl))

**OSOBY PROWADZĄCE PRZEDMIOT**

1 mgr inż. Marcin Klamra (kontakt: mklamra@iti.pk.edu.pl)

2 mgr inż. Tomasz Sośnicki (kontakt: tom.sosnicki@gmail.com)

**13 ZATWIERDZENIE KARTY PRZEDMIOTU DO REALIZACJI**

---

(miejscowość, data)

(odpowiedzialny za przedmiot)

(dziekan)

**PRZYJMUJĘ DO REALIZACJI** (data i podpisy osób prowadzących przedmiot)

.....

.....