



## KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Bezpieczeństwo w sieciach komputerowych [S2EiT1-SKiTI>BwSK]

### Przedmiot

Kierunek studiów

Elektronika i telekomunikacja

Rok/Semestr

1/2

Studia w zakresie (specjalność)

Sieci komputerowe i technologie internetowe

Profil studiów

ogólnoakademicki

Poziom studiów

drugiego stopnia

Język oferowanego przedmiotu

polski

Forma studiów

stacjonarne

Wymagalność

obieralny

### Liczba godzin

Wykład

30

Laboratorium

15

Inne (np. online)

0

Ćwiczenia

15

Projekty/seminaria

0

### Liczba punktów ECTS

4,00

### Koordynatorzy

dr hab. inż. Sławomir Hanczewski  
slawomir.hanczewski@put.poznan.pl

### Wykładowcy

### Wymagania wstępne

Student rozpoczynający ten przedmiot powinien posiadać uporządkowaną wiedzę z zakresu budowy i działania sieci komputerowych obejmującą zarówno urządzania, jak i protokoły sieciowe. Powinien również rozumieć konieczność poszerzania swoich kompetencji oraz posiadać umiejętność pozyskiwania informacji ze wskazanych źródeł.

### Cel przedmiotu

Przekazanie studentom teoretycznych i praktycznych zagadnień związanych z budowaniem bezpiecznych sieci komputerowych (teleinformatycznych) i ich testowaniem oraz z świadomym i bezpiecznym korzystaniem z zasobów Internetu.

### Przedmiotowe efekty uczenia się

Wiedza:

Student posiada usystematyzowaną wiedzę z zakresu bezpieczeństwa sieci komputerowych obejmującą:

1. zasady działania rozwiązań zapewniających bezpieczeństwo sieci (zapory sieciowe, IPS/IDS),
2. budowę i działania sieci VPN,
3. mechanizmów kryptograficznych wykorzystywanych we współczesnych sieciach,

#### 4. testy bezpieczeństwa.

##### Umiejętności:

1. Potrafi konfigurować urządzenia sieciowe i oprogramowanie w sposób zapewniający bezpieczne przesyłanie danych.
2. Potrafi wykorzystać mechanizmy kryptograficzne do bezpiecznego przesyłania danych.
3. Potrafi zaplanować i przeprowadzić proste testy sieci komputerowych.
4. Potrafi świadomie korzystać z zasobów Internetu.

##### Kompetencje społeczne:

1. Jest świadomy zmian jakie zachodzą wraz z ewolucją sieci komputerowych. Zna ograniczenia własnej wiedzy i rozumie konieczność ciągłego jej uaktualniania. Jest otwarty na możliwości ciągłego dokształcania się.
2. Profesjonalnie podchodzi do rozwiązywania problemów związanych z bezpieczeństwem sieci.

#### Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wiedza zdobyta w trakcie wykładów jest weryfikowana przez kolokwium realizowane na ostatnim wykładzie. Kolokwium składa się z 30 pytań testowych, w których proponowane są 4 odpowiedzi, przy czym tylko jedna odpowiedź jest poprawna. Próg zaliczeniowy wynosi 50%. Zagadnienia zaliczeniowe, na podstawie których opracowywane są pytania zostaną przesłane studentom drogą mailową z wykorzystaniem systemu uczelnianej poczty elektronicznej.

Wiedza zdobyta w trakcie ćwiczeń jest weryfikowana przez kolokwium realizowane na ostatnich zajęciach. Kolokwium składa się z 4 pytań otwartych, różnie punktowanych w zależności od ich trudności. Próg zaliczeniowy wynosi 50%. Zagadnienia, na podstawie których opracowywane są pytania odpowiadają treściom programowym realizowanym na ćwiczeniach.

Wiedza i umiejętności zdobyte w trakcie ćwiczeń laboratoryjnych weryfikowane jest poprzez kontrolę poprawności wykonania ćwiczenia np. kontrolując poprawność skonfigurowania urządzeń sieciowych oraz zadawanie pytań dotyczących realizowanego ćwiczenia. Brak zaliczenia ćwiczenia skutkuje koniecznością jego powtórzenia w terminie wskazanym przez prowadzącego.

#### Treści programowe

Zajęcia dotyczą problematyki bezpieczeństwa sieci teleinformatycznych.

#### Tematyka zajęć

##### Wykłady:

1. Analiza zagrożeń płynących z Internetu
2. Sprzętowe i programowe zapory sieciowe (firawalls)
3. Bezpieczeństwo urządzeń sieciowych
4. Systemy wykrywania włamań (IDS/IPS)
5. Podstawy kryptografii
6. Protokoły sieciowe zapewniające bezpieczne przesyłanie danych
7. Wirtualne Sieci Prywatne - VPN (Virtual Private Network)
8. Testy bezpieczeństwa systemów informatycznych

##### Ćwiczenia

1. Analiza zagrożeń czyhających na użytkowników Internetu.
2. Analiza mechanizmów kryptograficznych zapewniających bezpieczne przesyłanie danych.
3. Analiza protokołów sieciowych zapewniających bezpieczne przesyłanie danych.

##### Ćwiczenia laboratoryjne:

1. Konfiguracja sprzętowych zapór sieciowych.
2. Konfiguracja urządzeń sieciowych zapewniająca bezpieczny zdalny dostęp.
3. Konfiguracja sprzętowego systemu wykrywania intruzów (IDS).
4. Budowa sieci VPN.
5. Przeprowadzenie prostych testów bezpieczeństwa sieci komputerowych z wykorzystaniem Kali Linux.

#### Metody dydaktyczne

Wykład: prezentacja multimedialna uzupełniana przykładami i dodatkowymi wyjaśnieniami na tablicy.

Wykłady są prowadzone z godnie z zasadami wykładu tradycyjnego, w uzasadnionych przypadkach przybierającego formę wykładu konwersatoryjnego.

Ćwiczenia: prezentacja multimedialna, ćwiczenia tablicowe obejmujące omawiane algorytmy kryptograficzne oraz protokoły sieciowe.

Ćwiczenia laboratoryjne: prezentacja multimedialna prezentacja ilustrowana przykładami podawanymi na tablicy oraz wykonanie zadań podanych przez prowadzącego - ćwiczenia praktyczne.

## Literatura

Podstawowa

1. Serafin M., Sieci VPN : zdalna praca i bezpieczeństwo danych, Helion 2008.
2. Kim P., Podręcznik pentestera : bezpieczeństwo systemów informatycznych, Helion 2015.
3. Stallings W., Kryptografia i bezpieczeństwo sieci komputerowych : matematyka szyfrów i techniki kryptologii, Helion 2012.
4. Amato V., Akademia sieci Cisco : drugi rok nauki, Mikon 2001

Uzupełniająca

1. [www.cisco.com](http://www.cisco.com)
2. Erickson J., Hacking, Sztuka penetracji, Helion 2004

## Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	100	4,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	70	3,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwium/egzaminu, wykonanie projektu)	30	1,00