KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Bezpieczeństwo systemów teleinformatycznych [S1Teleinf1>BSI]

Przedmiot

Kierunek studiów
Teleinformatyka

Rok/Semestr
3/6

Studia w zakresie (specjalność)
–

Profil studiów
ogólnoakademicki

Poziom studiów
pierwszego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obligatoryjny

Liczba godzin

Wykład
15

Laboratorium
30

Inne
0

Ćwiczenia
0

Projekty/seminaria
0

Liczba punktów ECTS

3,00

Koordynatorzy

prof. dr hab. inż. Mieczysław Jessa
mieczyslaw.jessa@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student rozpoczynający ten przedmiot powinien posiadać podstawową usystematyzowaną wiedzę na temat działania sieci teleinformatycznych oraz umiejętność pozyskiwania informacji z literatury, baz danych oraz innych źródeł w języku polskim lub angielskim.

Cel przedmiotu

Celem nauczania przedmiotu jest przekazanie studentom wiedzy na temat atrybutów bezpieczeństwa, podstawowych zagrożeń dla danych przesyłanych i przetwarzanych w systemie teleinformatycznym, na temat administracyjnych metod ochrony danych, standardów międzynarodowych dotyczących bezpieczeństwa danych oraz wiedzy na temat kryptograficznych metod ochrony danych.

Przedmiotowe efekty uczenia się

Wiedza:
1. Ma wiedzę na temat atrybutów bezpieczeństwa, zagrożeń dla danych przesyłanych i przetwarzanych w systemie teleinformatycznym.
2. Zna podstawowe standardy międzynarodowe dotyczące bezpieczeństwa danych, metody analizy ryzyka, metody zarządzania ryzykiem oraz metody zarządzania bezpieczeństwem danych.

3. Zna podstawowe pojęcia kryptografii, ma wiedzę na temat kryptograficznych metod ochrony danych, rozumie znaczenie kryptografii dla zapewnienia bezpieczeństwa danych przesyłanych w sieciach teleinformatycznych i gromadzonych w bazach danych.

Umiejętności:
1. Potrafi przewidzieć skutki braku zabezpieczeń danych przesyłanych i gromadzonych w systemie teleinformatycznym.
2. Umie pracować w grupie nad rozwiązaniem problemu ochrony danych i sieci teleinformatycznej przed nieuprawnionym dostępem lub modyfikacją.

Kompetencje społeczne:
1. Jest gotów do pozyskania nowej wiedzy niezbędnej dla zapewnienia bezpieczeństwa systemom teleinformatycznym.
2. Ma poczucie odpowiedzialności za bezpieczeństwo zaprojektowanych systemów teleinformatycznych i zdaje sobie sprawę z potencjalnych niebezpieczeństw dla innych ludzi lub społeczeństwa ich nieodpowiedniego zabezpieczenia.

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wiedza nabyta w ramach wykładu jest weryfikowana na podstawie pisemnego zaliczenia, składającego się z 5 pytań otwartych, identycznie punktowanych. Próg zaliczeniowy wynosi 50% punktów. Rozkład progów dla ocen od 2 do 5 jest równomierny. Zestaw pytań jest losowany indywidualnie ze zbioru zagadnień. Zagadnienia zaliczeniowe, na podstawie których opracowywane są pytania otwarte, przesyłane są studentom elektronicznie.
Ocena z laboratorium jest średnią arytmetyczną ocen z trzech zrealizowanych implementacji uzupełnionych o raporty z przeprowadzonych badań.

Treści programowe

Program wykładu jest podzielony na trzy części. W części pierwszej studenci poznają podstawowe wymagania stawiane systemom teleinformatycznym, atrybuty bezpieczeństwa, klasyfikację zagrożeń, kategorie zagrożeń, zagrożenia charakterystyczne dla sieci teleinformatycznych przewodowych i bezprzewodowych.
Część druga jest poświęcona administracyjnym metodom ochrony danych.
Studenci poznają trójpoziomowy model odniesienia, podstawowe normy i standardy w obszarze bezpieczeństwa, definicję ryzyka, metody analizy ryzyka jakościowe, ilościowe, metody dedukcyjne oraz indukcyjne, poznają metody zarządzania ryzykiem, metody zarządzania bezpieczeństwem systemów teleinformatycznych, w tym schemat PDCA oraz zasady przeprowadzania audytu bezpieczeństwa teleinformatycznego.
Część trzecia dotyczy kryptograficznych metod ochrony danych.
Studenci poznają podstawowe pojęcia kryptografii takie jak system kryptograficzny symetryczny, asymetryczny, hybrydowy, bezpieczeństwo bezwarunkowe, obliczeniowe, udowadnialne, postulat Kerckhoffsa, szyfr blokowy, szyfr strumieniowy, dowiadują się o trybach pracy (użycia) szyfrów blokowych ECB, CBC, CFB, OFB, CTR, zapoznają się z pojęciem i konstrukcją szyfru strumieniowego, szyfru one-time-pad, z przykładami szyfrów blokowych i strumieniowych, ze schematem szyfrowania z kluczem publicznym RSA, Rabina, ElGamala, dowiadują się o wadach i zaletach szyfrowania symetrycznego (z kluczem tajnym) i asymetrycznego (z kluczem publicznym), poznają pojęcie i podstawowe właściwości funkcji skrótu, zapoznają się z metodami ataku przeciwko funkcji skrótu (atak słownikowy oraz atak wykorzystujący paradoks urodzinowy), poznają przykłady wykorzystania metod kryptograficznych w teleinformatyce.
Laboratorium obejmuje implementację w rzeczywistym środowisku przykładowych metod szyfrowania i ataku socjotechnicznego, wytwarzania ciągu losowego, wytwarzania bezpiecznego ciągu pseudolosowego oraz ocenę właściwości ciągu wyjściowego za pomocą testów statystycznych (realizacja distinguishing attack).

Tematyka zajęć

Program wykładu jest podzielony na trzy części. W części pierwszej studenci poznają podstawowe wymagania stawiane systemom teleinformatycznym, atrybuty bezpieczeństwa, klasyfikację zagrożeń,

kategorie zagrożeń, zagrożenia charakterystyczne dla sieci teleinformatycznych przewodowych i bezprzewodowych.
Część druga jest poświęcona administracyjnym metodom ochrony danych.
Studenci poznają trójpoziomowy model odniesienia, podstawowe normy i standardy w obszarze bezpieczeństwa, definicję ryzyka, metody analizy ryzyka jakościowe, ilościowe, metody dedukcyjne oraz indukcyjne, poznają metody zarządzania ryzykiem, metody zarządzania bezpieczeństwem systemów teleinformatycznych, w tym schemat PDCA oraz zasady przeprowadzania audytu bezpieczeństwa teleinformatycznego.
Część trzecia dotyczy kryptograficznych metod ochrony danych.
Studenci poznają podstawowe pojęcia kryptografii takie jak system kryptograficzny symetryczny, asymetryczny, hybrydowy, bezpieczeństwo bezwarunkowe, obliczeniowe, udowadnialne, postulat Kerckhoffsa, szyfr blokowy, szyfr strumieniowy, dowiadują się o trybach pracy (użycia) szyfrów blokowych ECB, CBC, CFB, OFB, CTR, zapoznają się z pojęciem i konstrukcją szyfru strumieniowego, szyfru one-time-pad, z przykładami szyfrów blokowych i strumieniowych, ze schematem szyfrowania z kluczem publicznym RSA, Rabina, ElGamala, dowiadują się o wadach i zaletach szyfrowania symetrycznego (z kluczem tajnym) i asymetrycznego (z kluczem publicznym), poznają pojęcie i podstawowe właściwości funkcji skrótu, zapoznają się z metodami ataku przeciwko funkcji skrótu (atak słownikowy oraz atak wykorzystujący paradoks urodzinowy), poznają przykłady wykorzystania metod kryptograficznych w teleinformatyce.
Laboratorium obejmuje implementację w rzeczywistym środowisku przykładowych metod szyfrowania i ataku socjotechnicznego, wytwarzania ciągu losowego, wytwarzania bezpiecznego ciągu pseudolosowego oraz ocenę właściwości ciągu wyjściowego za pomocą testów statystycznych (realizacja distinguishing attack).

Metody dydaktyczne

1. Wykład: prezentacja multimedialna, ilustrowana przykładami podawanymi na tablicy.
2. Laboratorium: klasyczna problemowa.

Literatura

Podstawowa:
1. A. Białas, Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, WNT, Warszawa, 2007.
2. K. Liderman, Analiza ryzyka i ochrona informacji w systemach komputerowych, PWN, Warszawa, 2008.
3. K. Liderman, Bezpieczeństwo informacyjne, nowe wyzwania, PWN, 2017.
4. A. J. Menezes, P. C. van Oorschot, S. A. Vanstone „Kryptografia stosowana”, WNT, Warszawa 2005.
5. B. Schneier „Kryptografia dla praktyków”, WNT, Warszawa, 2002.
6. W. Stallings „Kryptografia i bezpieczeństwo sieci komputerowych”, Wyd. V, Helion 2012.

Uzupełniająca:
1. R. Andersson, Inżynieria zabezpieczeń, WNT, 2005.
2. J. Stokłosa, T. Bilski, T. Pankowski, Bezpieczeństwo danych w systemach informacyjnych, PWN, 2001.
3. J. A. Buchmann „Wprowadzenie do kryptografii”, PWN, 2006.
4. M. Karbowski, Podstawy kryptografii, Helion, 2014.
5. M. Kutyłowski, W-B. Strothmann „Kryptografia, teoria i praktyka zabezpieczania systemów komputerowych”, Read Me, Warszawa, 1999.
6. N. Ferguson, B. Schneier „Kryptografia w praktyce”, Helion, 2004.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	90	3,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	49	2,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	41	1,00