KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Bezpieczeństwo informacji w instytucji [S1MiKC1>BIwI]

Przedmiot

Kierunek studiów
Mikroelektronika i komunikacja cyfrowa

Rok/Semestr
3/6

Studia w zakresie (specjalność)
–

Profil studiów
ogólnoakademicki

Poziom studiów
pierwszego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład
30

Laboratorium
24

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 telekomunikacyjnych i komputerowych oraz umiejętność pozyskiwania informacji z literatury, baz danych oraz innych źródeł w języku polskim lub angielskim. Powinien posiadać wiedzę ogólną na poziomie maturalnym, znać model OSI, protokół TCP/IP oraz metody statystycznej oceny danych.

Cel przedmiotu

Celem nauczania przedmiotu jest przekazanie studentom wiedzy na temat atrybutów bezpieczeństwa, podstawowych zagrożeń dla danych przechowywanych i przetwarzanych w instytucji (firma, szpital, jednostka samorządu terytorialnego itp.), sposobu zorganizowania bezpiecznego obiegu danych w instytucji, standardów międzynarodowych dotyczących bezpieczeństwa danych oraz podstawowej 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 instytucji.
2. Zna podstawowe standardy międzynarodowe dotyczące bezpieczeństwa danych, metody analizy ryzyka, metody zarządzania ryzykiem oraz metody zarządzania bezpieczeństwem danych.
3. Zna podstawowe zagadnienia kryptografii, metod szyfrowania, bezpieczeństwa systemów telekomunikacyjnych, posiada umiejętność identyfikacji zagrożeń i stosowania metod ochrony danych w systemach elektronicznych i sieciach komputerowych, rozumie znaczenie kryptografii dla zapewnienia bezpieczeństwa danych przesyłanych w sieciach teleinformatycznych i gromadzonych w bazach danych

Umiejętności:
1. Potrafi zastosować narzędzia kryptograficzne dla zapewnienia podstawowych atrybutów bezpieczeństwa urządzeń elektronicznych oraz danych przetwarzanych przez te urządzenia.
2. Potrafi przewidzieć skutki braku zabezpieczeń danych przesyłanych i gromadzonych w instytucji.
3. Umie pracować w grupie nad rozwiązaniem problemu ochrony danych przed nieuprawnionym dostępem lub modyfikacją.

Kompetencje społeczne:
1. Zna ograniczenia własnej wiedzy i umiejętności, rozumie konieczność dalszego dokształcania się.
2. Ma poczucie odpowiedzialności za bezpieczeństwo zaprojektowanych systemów ochrony danych i zdaje sobie sprawę z potencjalnych niebezpieczeństw dla innych ludzi lub społeczeństwa ich nieodpowiedniego zabezpieczenia.
3. Jest gotów do pozyskania nowej wiedzy niezbędnej dla zapewnienia bezpieczeństwa instytucji.

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. Zagadnienia zaliczeniowe, na podstawie których opracowywane są pytania otwarte, udostępniane są w systemie eKursy i/lub przesyłane są studentom drogą mailową z wykorzystaniem uczelnianej poczty elektronicznej. Zaliczenie laboratorium wymaga uzyskania pozytywnej oceny ze sprawdzianu końcowego oraz z co najmniej połowy sprawozdań z wykonanych zadań.

Treści programowe

Treści programowe obejmują trzy moduły tematyczne. W części pierwszej studenci poznają podstawowe atrybuty bezpieczeństwa, klasyfikację zagrożeń oraz kategorie zagrożeń. Część druga jest poświęcona administracyjnym metodom ochrony danych. Studenci poznają trójpoziomowy model odniesienia, podstawowe normy i standardy w obszarze bezpieczeństwa danych, definicję ryzyka, metody analizy ryzyka, metody zarządzania ryzykiem, metody budowy i zarządzania bezpieczeństwem danych i systemów teleinformatycznych instytucji. Część trzecia dotyczy kryptograficznych metod ochrony danych. Studenci poznają podstawowe pojęcia kryptografii i przykłady wykorzystania metod kryptograficznych w życiu codziennym.

Tematyka zajęć

Program wykładu jest podzielony na trzy części. W części pierwszej studenci poznają podstawowe atrybuty bezpieczeństwa, klasyfikację zagrożeń, kategorie zagrożeń, zagrożenia charakterystyczne dla instytucji. Część druga jest poświęcona administracyjnym metodom ochrony danych. Studenci poznają trójpoziomowy model odniesienia, podstawowe normy i standardy w obszarze bezpieczeństwa danych, definicję ryzyka, metody analizy ryzyka jakościowe, ilościowe, metody dedukcyjne oraz indukcyjne, poznają metody zarządzania ryzykiem, metody budowania i zarządzania bezpieczeństwem danych i systemów teleinformatycznych instytucji, 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 życiu codziennym (mechanizm AKA, protokół SSL, TLS oraz SSH), zapoznają się z podstawowymi pojęciami kryptografii postkwantowej (PQC).
Laboratorium obejmuje implementację w rzeczywistym środowisku przykładowych metod szyfrowania, 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 z elementami seminarium.
2. Laboratorium: połączenie klasycznej metody problemowej z seminaryjną

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	84	3,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	54	2,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	30	1,00