KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Bezpieczeństwo sieci bezprzewodowych [S2Inf1E-CYB>BSB]

Przedmiot

Kierunek studiów
Informatyka/Computing

Rok/Semestr
1/1

Studia w zakresie (specjalność)
Cyberbezpieczeństwo

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
angielski

Forma studiów
stacjonarne

Wymagalność
obligatoryjny

Liczba godzin

Wykład
30

Laboratorium
15

Inne (np. online)
0

Ćwiczenia
0

Projekty/seminaria
0

Liczba punktów ECTS

3,00

Koordynatorzy

dr inż. Tomasz Bilski
tomasz.bilski@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student rozpoczynający ten przedmiot powinien mieć ogólną wiedzę na temat architektury systemów komputerowych, systemów operacyjnych, sieci komputerowych, ze szczególnym uwzględnieniem sieci bezprzewodowych.

Cel przedmiotu

Przekazanie studentom wiedzy i umiejętności dotyczących bezpieczeństwa w bezprzewodowych systemach komunikacji z uwzględnieniem różnych rodzajów sieci (lokalnych, miejskich, rozległych, IoT).

Przedmiotowe efekty uczenia się

Wiedza:
1. student ma wiedzę na temat różnych technologii budowy bezprzewodowych systemów komunikacji
2. student ma wiedzę na temat podatności i zagrożeń charakterystycznych dla bezprzewodowych systemów transmisji danych
3. student ma wiedzę na temat metod, narzędzi i zasad ochrony stosowanych w bezprzewodowych systemach komunikacji

Umiejętności:
1. student potrafi opracować założenia, koncepcję i projekt bezprzewodowego systemu transmisji danych
2. student potrafi dokonać analizy budowy i funkcjonowania bezprzewodowego systemu transmisji danych z uwzględnieniem poziomu bezpieczeństwa
3. student potrafi zapewnić wysoki poziom bezpieczeństwa w bezprzewodowych systemach transmisji danych

Kompetencje społeczne:
1. student rozumie, że posługiwanie się narzędziami informatycznymi musi gwarantować wysoki poziom bezpieczeństwa transmisji danych
2. student rozumie, że konieczne jest aktualizowanie wiedzy i umiejętności z zakresu konkretnych narzędzi, metod i zasad ochrony.

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wykład
Kolokwium (45 minut) z pytaniami otwartymi. Kolokwium jest przeprowadzane na ostatnich zajęciach w semestrze. W celu uzyskania oceny pozytywnej trzeba otrzymać ponad 50% wszystkich możliwych do zdobycia punktów. Zagadnienia zaliczeniowe, na podstawie których opracowywane są pytania są przekazywane studentom na początku semestru.
Umiejętności nabyte w ramach zajęć praktycznych weryfikowane są na bieżąco podczas zajęć (przy omawianiu kolejnych etapów ćwiczeń i części zadań projektowych) oraz przez dokonanie końcowej oceny projektu i jego dokumentacji przez prowadzącego zajęcia.

Treści programowe

Program modułu obejmuje następujące zagadnienia:
1. Wprowadzenie
2. Standardy transmisji bezprzewodowej
3. Podatności i zagrożenia
4. Przykłady ataków
5. Bezpieczeństwo w lokalnych sieciach bezprzewodowych IEEE 802.11. T
6. Bezpieczeństwo w bezprzewodowych systemach IoT.
7. Systemy uwierzytelniania pozapasmowego.
8. Aktualne problemy i kierunki rozwoju.
.

Tematyka zajęć

Program wykładu obejmuje następujące zagadnienia
1. Wprowadzenie – klasyfikacja i charakterystyka bezprzewodowych systemów transmisji (pasma transmisyjne, technologie).
2. Standardy transmisji bezprzewodowej (w tym: Bluetooth, ZigBee, 6LoWPAN, rodzina standardów IEEE 802, NFC, VLC).
3. Podatności i zagrożenia charakterystyczne dla systemów bezprzewodowej transmisji danych ze szczególnym uwzględnieniem systemów IoT. Ogólna charakterystyka narzędzi, metod i zasad ochrony.
4. Przykłady ataków: RF jamming, scrambling, skyjacking, ASLEAP, association flood, probe request flood, RTS/CTS flood, …).
5. Bezpieczeństwo w lokalnych sieciach bezprzewodowych IEEE 802.11. Techniki szyfrowania, uwierzytelniania i kontroli integralności.
6. Bezpieczeństwo w bezprzewodowych systemach IoT.
7. Systemy uwierzytelniania pozapasmowego.
8. Aktualne problemy i kierunki rozwoju.

Program laboratorium obejmuje następujące zagadnienia:
Zajęcia 1-5: konfiguracja sieci WLAN w standardach 802.11 (tryby: IBSS, ESS); mechanizmy kryptograficzne z kluczem współdzielonym; mechanizmy kryptograficzne oparte na certyfikatach (zastosowanie serwerów RADIUS / Kerberos); mechanizmy kontroli dostępu, izolacji ruchu (user

isolation / multi SSID / VLAN), podatności w sieciach WLAN 802.11 i testy penetracyjne.
Zajęcia 6-8: Opracowanie koncepcji sieci bezprzewodowej dla wybranego zastosowania ze szczególnym uwzględnieniem metod, narzędzi i zasad ochrony. Przygotowanie założeń dla systemu. Wybór odpowiednich protokołów, urządzeń sieciowych, oprogramowania. Opracowanie dokumentacji projektowanego systemu z uwzględnieniem kosztów wdrożenia. Oszacowanie bezpieczeństwa systemu. Uwzględnienie najnowszych technologii w zakresie ochrony danych.

Metody dydaktyczne

Wykład z prezentacją multimedialną. Prowadzenie dyskusji w trakcie wykładu. Dodatkowe materiały udostępnione w systemie elearningu.
Laboratorium prowadzone w formie konsultacji i weryfikacji kolejnych zadań. Zadania wykonywane przy użyciu sprzętu komputerowego, narzędzi programistycznych oraz Internetu.

Literatura

Podstawowa
M. Apolinarski, T. Bilski, M. Retinger, Sieci komputerowe. Laboratorium. Wyd. PP, Poznań, 2020
Uzupełniająca
standards.ieee.org/getieee802/index.html
morse.colorado.edu/~tlen5510/text/classwebch1.html
www.wi-fiplanet.com
www.wifialliance.com
www.wlana.org
www.wi-fi.org
www.bluetooth.com
www.dmoz.org/Computers/Data_Communications/Wireless/

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	75	3,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	45	2,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	30	1,00