



KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Programowanie kart elektronicznych

Przedmiot

Kierunek studiów

Informatyka

Studia w zakresie (specjalność)

Aplikacje Mobilne i Wbudowane dla Internetu Przedmiotów

Poziom studiów

drugiego stopnia

Forma studiów

niestacjonarne

Rok/semestr

2/3

Profil studiów

ogólnoakademicki

Język oferowanego przedmiotu

polski

Wymagalność

obieralny

Liczba godzin

Wykład

12

Laboratoria

20

Inne (np. online)

0

Ćwiczenia

0

Projekty/seminaria

0

Liczba punktów ECTS

3

Wykładowcy

Odpowiedzialny za przedmiot/wykładowca:

dr hab. inż. Marek Mika

Odpowiedzialny za przedmiot/wykładowca:

mgr inż. Marek Gosławski

Wymagania wstępne

Student rozpoczynający ten przedmiot powinien posiadać podstawową wiedzę z elektroniki, systemów operacyjnych i kryptografii. Powinien także posiadać umiejętności: rozwiązywania podstawowych problemów z zakresu projektowania aplikacji, programowania w językach wysokiego poziomu oraz pozyskiwania informacji ze wskazanych źródeł. Ponadto student powinien rozumieć konieczność poszerzania swoich kompetencji

Cel przedmiotu

Przekazanie studentom podstawowej wiedzy dotyczącej kart elektronicznych i systemów automatycznej identyfikacji stosowanych w logistyce, a także służących do identyfikacji obiektów w Internecie Przedmiotów, w zakresie standardów, zastosowań, a także projektowania systemów je wykorzystujących i programowania. Ponadto, rozwinięcie u studentów umiejętności projektowania i programowania systemów korzystających z kart elektronicznych i technologii związanych z automatyczną identyfikacją

Przedmiotowe efekty uczenia się

Wiedza



1. Ma uporządkowaną, podbudowaną teoretycznie wiedzę ogólną w zakresie budowy, zasad działania, programowania i zastosowań kart elektronicznych i urządzeń opartych na technologiach RFID, NFC i standardach kodów kreskowych.
2. Ma wiedzę dotyczącą: konstrukcji czytników i znaczników RFID, kart elektronicznych, protokołów transmisji stosowanych w kartach elektronicznych, systemów operacyjnych kart elektronicznych, komunikacja karty lub znacznika z czytnikiem, programowania oraz zastosowań kart elektronicznych, systemu GS1.
3. Ma wiedzę o trendach rozwojowych i najistotniejszych nowych osiągnięciach dotyczących kart elektronicznych oraz systemów automatycznej identyfikacji obiektów w Internecie Przedmiotów
4. Zna obszary i przykłady praktycznych zastosowań kart elektronicznych oraz systemów automatycznej identyfikacji.

Umiejętności

1. Potrafi zgodnie z zadaną specyfikacją, uwzględniającą aspekty pozatechniczne, zaprojektować oprogramowanie dla karty elektronicznej lub wybranego systemu automatycznej identyfikacji i zrealizować ten projekt co najmniej w części używając właściwych metod, technik i narzędzi
2. Podczas projektowania oprogramowania dla karty elektronicznej lub systemu automatycznej identyfikacji potrafi sięgnąć po właściwą normę lub standard i zastosować w praktyce przedstawioną w nich wiedzę specjalistyczną.

Kompetencje społeczne

1. Rozumie, że w zakresie kart elektronicznych i systemów automatycznej identyfikacji wiedza i umiejętności szybko mogą stać się przestarzałe. Zdaje sobie sprawę ze znaczenia norm i standardów w dziedzinie.

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Ocena wiedzy nabytej w ramach wykładu odbywa się na podstawie kolokwium pisemnego w formie testu, który może zawierać 20 do 50 pytań otwartych, jak i zamkniętych. W przypadku pytań zamkniętych jest to test wielokrotnego wyboru. Punktacja poszczególnych pytań podana jest w treści pytania. Forma testu i zagadnienia do niego obowiązujące omawiane są w trakcie jednego z ostatnich wykładów. Na ocenę 3,0 należy zdobyć co najmniej 50% punktów, ocenę 3,5 co najmniej 60% punktów, 4,0 za co najmniej 70% punktów itd.

W zakresie laboratoriów weryfikowanie założonych efektów kształcenia realizowane jest przez:

1. Ocenę zadań wykonywanych w ramach kolejnych zajęć, za każde poprawnie wykonane zadanie można otrzymać maksymalnie 1 punkt, na podstawie liczby zdobytych punktów wystawiana jest ocena częściowa.
2. Test końcowy obejmujący zagadnienia przećwiczone w ramach zajęć laboratoryjnych, test składa się z losowo wybranych pytań dotyczących każdego z tematów ćwiczeń, za każdą poprawną odpowiedź



można otrzymać 1 punkt, na podstawie liczby zdobytych punktów wystawiana jest druga ocena częściowa

3. Wykonanie i obrona projektu, za które wystawiana jest trzecia ocena częściowa

4. Ocena końcowa wystawiana jest na podstawie trzech ocen częściowych, jako średnia ważona

Treści programowe

Program wykładu obejmuje następujące zagadnienia:

Rola i znaczenie systemów identyfikacji stosowanych w obiektach Internetu Przedmiotów. System GS1: rola standardu, identyfikacja różnych typów obiektów, zastosowania. Kody kreskowe: zasada działania, parametry kodów kreskowych, typy kodów kreskowych, drukowanie i weryfikacja jakości, odczyt kodów kreskowych. RFID: zasada działania, kategorie znaczników, zapis i odczyt. EPC: standard, zasady, korzyści z zastosowania. GSDN, czyli globalna synchronizacja danych. Geneza kart elektronicznych. Przegląd podstawowych zastosowań KE. Rola standaryzacji. Rodzaje kart (wypukłe, z paskiem magnetycznym, pamięciowe stykowe i bezstykowe, procesorowe stykowe i bezstykowe, wielomegabajtowe, optyczne). Cechy fizyczne KE (formaty, styki, materiały, cechy zabezpieczające, moduły z chipem). Cechy elektryczne KE (styki, napięcie i prąd zasilania, zegar, transmisja danych, sekwencje aktywujące i dezaktywujące). Mikrokontrolery KE (technologie półprzewodnikowe, typy procesorów, typy pamięci, moduły komunikacyjne, zegar i inne moduły). Struktury danych. Kodowanie danych alfanumerycznych. Notacja SDL. KE jako automat skończony. Kody wykrywające i korygujące błędy. Kompresja danych. Kryptologia (symetryczne algorytmy szyfrujące: DES, AES, IDEA, COMP128, Milanage; asymetryczne algorytmy szyfrujące: RSA, DSS, algorytm krzywych eliptycznych; wielokrotne szyfrowanie; wyrównywanie danych; uwierzytelnianie komunikatów i kryptograficzna suma kontrolna), funkcje haszujące, generowanie i testowanie liczb losowych, uwierzytelnianie kart i czytników (jednostronne symetryczne, dwustronne symetryczne, statyczne asynchroniczne, dynamiczne asynchroniczne), podpisy cyfrowe, certyfikaty, zarządzanie kluczami, uwierzytelnianie osób. Komunikacja z kartą (komunikaty: ATR, PPS, APDU). Bezpieczna transmisja danych pomiędzy kartą a czytnikiem. Kanały i protokoły logiczne. Łączenie terminali z systemami wyższego poziomu. Transmisja danych dla kart stykowych (warstwa transportowa, protokoły kart pamięci, protokoły transmisyjne T=0 i T=1, protokoły USB, MMC i SWP). Transmisja danych dla kart bezstykowych (sprzężenia indukcyjne i pojemnościowe, transfer zasilania, transfer danych, NFC, karty bezstykowe bliskiego i dalekiego zasięgu, karty zbliżeniowe). Programowanie KE (polecenia: plikowe, odczytu i zapisu, wyszukiwania, uwierzytelniania osób i urzędzeń, kryptograficzne, zarządzania plikami i aplikacjami, kompletujące, testowania sprzętu, bazodanowe, transmisji danych). Polecenia związane z zastosowaniem karty (dla portmonetek elektronicznych, dla kart kredytowych i debetowych). Zarządzane plikami karty elektronicznej (struktura pliku, cykl życia pliku, typy plików, nazwy plików, wybór pliku, struktura pliku EF, warunki dostępu, atrybuty). Systemy operacyjne KE (podstawowe założenia i funkcje, przetwarzanie poleceń, zasady projektowania i implementacji, kompletowanie karty, organizacja i zarządzanie pamięcią, zarządzanie plikami, dostęp do zasobów, operacje atomowe, wielozadaniowość, wydajność, zarządzanie aplikacjami, kody narodowe). Typy systemów operacyjnych KE: JavaCard, Multos, BasicCard, Linux, Small-OS. Produkcja i zapewnienie jakości kart elektronicznych. Bezpieczeństwo kart elektronicznych (typy ataków,



historia ataków, ataki i obrona w trakcie projektowania, produkcji i użytkowania). Czytniki kart elektronicznych (cechy fizyczne i elektryczne, interfejs użytkownika, interfejs aplikacji, bezpieczeństwo). Zastosowania KE w: systemach płatności, systemach telekomunikacyjnych, systemach służby zdrowia, systemach transportu, identyfikacji, paszportach, w zabezpieczeniach IT. Projektowanie aplikacji.

Zajęcia laboratoryjne prowadzone są w formie 2-godzinnych ćwiczeń, odbywających się w laboratorium. Ćwiczenia podzielone są na dwie części. W pierwszej studenci wykonują kolejne ćwiczenia praktyczne zapoznając się z różnymi technologiami. Część ta kończy się testem sprawdzającym zdobytą wiedzę. Druga część związana jest z realizacją projektu praktycznego lub teoretycznego. Program laboratorium obejmuje następujące zagadnienia:

Obsługa następujących typów kart elektronicznych: JavaCard, SIM, BasicCard, .NET oraz legitymacja studencka. Szyfrowanie. Obsługę i przechowywanie na karcie kluczy szyfrujących i podpisu cyfrowego. Języki i techniki programowania kart elektronicznych. Zastosowania kart elektronicznych. Obsługę kodów kreskowych: kodowanie, wydruk, odczyt. Technologia RFID odczyt i zapis znaczników RFID. Ćwiczenia z zakresu technologii NFC.

Metody dydaktyczne

1. Wykład: prezentacja multimedialna.
2. Ćwiczenia laboratoryjne: rozwiązywanie zadań, ćwiczenia praktyczne, zadania o charakterze projektowym

Literatura

Podstawowa

1. E. Hałas (red.): Kody kreskowe i inne globalne standardy w biznesie. Instytut Logistyki i Magazynowania 2012.
2. B. Gładysz, M. Grabia, K. Santarek: RFID od koncepcji do wdrożenia : polska perspektywa, PWN, 2017..
3. K. Mayes, K. Markantonakis (red.), Smart cards, tokens, security and applications (wyd. 2), Springer, 2017 (<https://link.springer.com/content/pdf/10.1007%2F978-3-319-50500-8.pdf>)
4. M. Kubas, M. Molski: Karta elektroniczna : bezpieczny nośnik informacji, Mikom, 2002
5. W. Rankl, W. Effing: Smart card handbook (wyd. 4), Wiley, 2010
6. U. Hansmann, M. S. Nicklous, T. Schäck, A. Schneider, F. Seliger: Smart Card Application Development Using Java (wyd. 2), Springer 2012. (<https://link.springer.com/book/10.1007%2F978-3-642-55969-3>)
7. S. A. Ahson, M Ilyas: Near Field Communications Handbook, Taylor & Francis, 2016 (<http://library.put.poznan.pl/do/access?TandFbooks9781420088151>)
8. www.smartcardbasics.com



Uzupełniająca

1. S. Mangard, E. Oswald, T. Popp: Power analysis attacks: Revealing the secrets of smart cards, Springer, 2007 (<https://link.springer.com/content/pdf/10.1007%2F978-0-387-38162-6.pdf>)
2. Kody kreskowe: rodzaje, standardy, sprzęt, zastosowania (wyd. 2). Instytut logistyki i magazynowania, 2000
3. K. Finkenzeller: RFID Handbook, (wyd. 3), Wiley, 2010
4. W. Wieczerzycki (red.) E-Logistyka.. Polskie Wydawnictwo Ekonomiczne, 2012
5. U. Chirico: Smart Card Programming, (wyd. 2), Lulu, 2015.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	80	3,0
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	32	1
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwium, wykonanie projektu) ¹	48	2

¹ niepotrzebne skreślić lub dopisać inne czynności