(pieczęć wydziału)

KARTA PRZEDMIOTU

1. Nazwa przedmiotu: **ZASTOSOWANIA TECHNOLOGII SIECIOWYCH W ADMINISTRACJI I BIZNESIE**	**2. Kod przedmiotu:**

3. Karta przedmiotu ważna od roku akademickiego: 2012/2013

4. Forma kształcenia: studia drugiego stopnia

5. Forma studiów: niestacjonarne (zaoczne)

6. Kierunek studiów: INFORMATYKA (SYMBOL WYDZIAŁU) RAU

7. Profil studiów: ogólnoakademicki

8. Specjalność: wszystkie specjalności

9. Semestr: 4

10. Jednostka prowadząca przedmiot: Instytut Informatyki Pol. Śl.

11. Prowadzący przedmiot: dr inż. Mirosław Skrzewski

12. Przynależność do grupy przedmiotów: przedmioty wspólne

13. Status przedmiotu: obowiązkowy

14. Język prowadzenia zajęć: polski

15. Przedmioty wprowadzające oraz wymagania wstępne:
Sieci komputerowe, Bazy danych, Analiza i projektowanie systemów komputerowych

16. Cel przedmiotu:
Celem przedmiotu jest przedstawienie technologii sieciowych zapewniających bezpieczeństwo przesyłania, przechowywania i przetwarzania informacji, znajdujących zastosowanie w elektronicznym obiegu / uzgadnianiu treści i poświadczaniu autorstwa dokumentów, w elektronicznej realizacji transakcji finansowych oraz metod zapewniania wysokiej niezawodności i wydajności tych rozwiązań.

17. Efekty kształcenia:

Nr	Opis efektu kształcenia	Metoda sprawdzenia efektu kształcenia	Forma prowadzenia zajęć	Odniesienie do efektów dla kierunku studiów
1	Zna podstawowe algorytmy kryptograficzne, ich właściwości i obszary ich stosowania dla zapewnienia bezpieczeństwa przesyłania i przechowywania informacji.	Kolokwium, pytania na ćwiczeniach laboratoryjnych	Wykład, ćwiczenia laboratoryjne	K_W07, K_W08, K_W12, K_U12, K_U18
2	Ma podstawową wiedzę na temat metod uwierzytelniania i autoryzacji użytkowników przy dostępie do systemów przetwarzania informacji na różnych poziomach ochrony	Kolokwium, pytania na ćwiczeniach laboratoryjnych	Wykład, ćwiczenia laboratoryjne	K_W08, K_W13, K_U06, K_U18
3	Zna podstawowe metody zapewnienia wysokiego poziomu bezpieczeństwa przechowania i dostępności	Kolokwium	Wykład	K_W08, K_W12, K_U11,

	chronionych informacji w systemach komputerowych.			
4	Ma podstawową wiedzę na temat zasad budowy jedno- i wielo-warstwowych aplikacji klient-serwer i wpływu poszczególnych decyzji projektowych na wydajność aplikacji, zna metody testowania wydajności rozproszonych aplikacji.	Kolokwium, pytania na ćwiczeniach laboratoryjnych	Wykład, ćwiczenia laboratoryjne	K_W07, K_W08, K_W12, K_W13, K_U11, K_U15, K_U18, K_K03
5	Ma ogólną wiedzę na temat zasad obiegu dokumentów w instytucjach i urzędach, zna wymagania i metody zapewnienia poufności i bezpieczeństwa przepływu informacji w elektronicznym obiegu dokumentów.	Kolokwium, pytania na ćwiczeniach laboratoryjnych	Wykład, ćwiczenia laboratoryjne	K_W07, K_W12, K_W13, K_W15, K_U11, K_U15
6	Ma podstawową wiedzę na temat metod realizacji transakcji finansowych w aplikacjach internetowych, zna podstawowe rozwiązania zapewnienia bezpieczeństwa informacji wykorzystywanych przy realizacji transakcji.	Kolokwium	Wykład	K_W08, K_W12, K_W13, K_W15, K_U06, K_U10

18. Formy zajęć dydaktycznych i ich wymiar (liczba godzin)

W. 2 Ćw. 0 L. 2 P. 0 Sem. 0

19. Treści kształcenia:

Wykłady:

Elementy kryptografii i bezpieczeństwa informacji. Szyfry symetryczne DES, 3DES, IDEA, AES. Problemy rozwiązań z tajnym kluczem, algorytm Diffiego-Hellmana. Podstawy algorytmów szyfrowania asymetrycznego, szyfrowanie RSA, ElGamal. Szyfrowanie jednokierunkowe, funkcje MD5, SHA1, SHA256. Metody uwierzytelniania dokumentów – podpis elektroniczny, certyfikaty. Infrastruktura klucza publicznego, centrum certyfikatów, podpis kwalifikowany.

Bezpieczeństwo sieci i przesyłu informacji, kontrola dostępu do zasobów. Protokoły z szyfrowaniem informacji – ssh, tsl, VPN. Aplikacje sieciowe oparte o protokół http, metody zapewnienia bezpieczeństwa przy współpracy systemów sieciowych, metody weryfikacji tożsamości uczestników transakcji elektronicznych, Metody uwierzytelniania użytkowników systemów, rodzaje uwierzytelnienia. Algorytmy challenge-response, kerberos, metody biometryczne, metody dwuskładnikowe, wykorzystanie certyfikatów.

Zasady konstrukcji aplikacji e-wszystko, rozwiązania jedno, dwu, wielowarstwowe. Metody monitorowania i zwiększania wydajności aplikacji, rozwiązania wielo-serwerowe, farmy serwerów. Protokół snmp, organizacja baz MIB, RMON. Narzędzia monitorowania wydajności systemów, czasowe wymagania użytkownika. Bezpieczeństwo przechowywania informacji, problem „disaster recovery", rozwiązania systemów backup-u, replikacja, tryby replikacji, centra zapasowe. Wymagania bezpieczeństwa danych klientów, zabezpieczenia dostępności i poufności informacji medycznych, ochrona bezpieczeństwa danych osobowych.

Pojecie obiegu dokumentu, zasady sterowania i rejestracji obiegu, rejestracja podejmowania i dokumentowania decyzji, wymagania kodeksowe. Problemy elektronizacji obiegu dokumentów, wykorzystanie podpisu elektronicznego. Zasady działania e-urzędu, przykłady rozwiązań, moduł elektronicznej skrzynki podawczej. Transakcje biznesowe, zasady przygotowania, uzgadniania i finalizacji transakcji. Zasady płatności kartami bankowymi, klasyczny schemat płatności kartami, schematy płatności internetowych.

Laboratorium:

W trakcie zajęć laboratoryjnych studenci zapoznają się z metodami konfiguracji i testowania wybranych usług i protokołów komunikacyjnych sieci. Tematyka ćwiczeń:

1. Podstawy kryptografii
2. Usługi uwierzytelniania - karty chipowe
3. Ocena wydajności serwisu WWW
4. System CMS (zarządzania zawartością)
5. Usługi kryptograficzne – certyfikaty
6. Protokoły zarządzania siecią

20. Egzamin: nie

21. Literatura podstawowa:

- Stallings W., Kryptografia i bezpieczeństwo sieci komputerowych. Koncepcje i metody bezpiecznej komunikacji, Helion 2011
- Souders S., Wydajne witryny internetowe. Przyspieszanie działania serwisów WWW, Helion, 2008

22. Literatura uzupełniająca:

- Foristal, J., Traxler, J., Hack Proofing Your Web Applications, edycja polska, wyd. Helion, 2003
- Stallings W., Kryptografia i bezpieczeństwo sieci komputerowych. Matematyka szyfrów i techniki kryptologii, Helion 2011
- Adams C., Lloyd S., PKI. Podstawy i zasady działania, PWN, 2007
- Blinowski G., Systemy poczty elektronicznej. Standardy, architektura, bezpieczeństwo, BTC 2012

23. Nakład pracy studenta potrzebny do osiągnięcia efektów kształcenia

Lp.	Forma zajęć	Liczba godzin kontaktowych / pracy studenta
1	Wykład	30/30
2	Ćwiczenia	/
3	Laboratorium	30/30
4	Projekt	/
5	Seminarium	/
6	Inne	/
	Suma godzin	60/60

24. Suma wszystkich godzin: 120

25. Liczba punktów ECTS: 4

26. Liczba punktów ECTS uzyskanych na zajęciach z bezpośrednim udziałem nauczyciela akademickiego 2

27. Liczba punktów ECTS uzyskanych na zajęciach o charakterze praktycznym (laboratoria, projekty) 2

26. Uwagi:

Zatwierdzono:

…….
(data i podpis prowadzącego)

……
(*data i podpis dyrektora instytutu/kierownika katedry/ Dyrektora Kolegium Języków Obcych/kierownika lub dyrektora jednostki międzywydziałowej)*