(pieczęć wydziału)

KARTA PRZEDMIOTU

1. Nazwa przedmiotu: Kryptograficzne metody ochrony informacji	**2. Kod przedmiotu:** Spec2
3. Karta przedmiotu ważna od roku akademickiego: 2017/18	
4. Forma kształcenia: studia pierwszego stopnia	
5. Forma studiów: studia stacjonarne	
6. Kierunek studiów: INFORMATYKA (SYMBOL WYDZIAŁU) **RMS**	
7. Profil studiów: ogólnoakademicki	
8. Specjalność: Zarządzanie bezpiecznymi sieciami komputerowymi	
9. Semestr: V	
10. Jednostka prowadząca przedmiot: Instytut Matematyki	
11. Prowadzący przedmiot: dr inż. Jarosław Karcewicz	
12. Przynależność do grupy przedmiotów: Zarządzanie sieciami komputerowymi oraz bezpieczeństwem systemów teleinformatycznych	
13. Status przedmiotu: specjalnościowy	
14. Język prowadzenia zajęć: polski	
15. Przedmioty wprowadzające oraz wymagania wstępne: Wymogi wstępne dotyczą wiedzy pobranej przez studentów na przedmiotach: „Systemy operacyjne”, oraz „Sieci komputerowe i internet”, oraz „Zarządzanie sieciowymi systemami operacyjnymi I”.	
16. Cel przedmiotu: Celem przedmiotu jest przekazanie studentom wiedzy na temat funkcjonowania nowoczesnych metod służących do ochrony prywatności danych, autentyfikacji użytkowników systemów komputerowych, zabezpieczania przed nieuprawnionymi modyfikacjami danych i innymi tego typu zastosowaniami opartymi na technikach kryptograficznych.	

17. Efekty kształcenia

Student który zaliczy przedmiot:

Nr	Opis efektu kształcenia	Metoda sprawdzenia efektu kształcenia	Forma prowadzenia zajęć	Odniesienie do efektów dla kierunku studiów
1	… ma szczegółową i podbudowaną teoretycznie wiedzę w zakresie metod szyfrowania danych stosowanych w sieciach komputerowych, ze szczególnym uwzględnieniem Infrastruktury Klucza Publicznego	spr, egz	wykład, laboratorium	K1A_W06, T1A_W04, T1A_U01, T1A_K01

2	… ma szczegółową i podbudowaną teoretycznie wiedzę w zakresie metod i mechanizmów szyfrowania danych na nośnikach danych	spr, egz	wykład, laboratorium	K1A_W06, T1A_W04, T1A_U01, T1A_K01
3	… ma szczegółową i podbudowaną teoretycznie wiedzę w zakresie zarządzania urzędem certyfikującym	spr, egz	wykład, laboratorium	K1A_W06, T1A_W04, T1A_U01, T1A_K01
4	… posiada szczegółową i podbudowaną teoretycznie wiedzę związaną z instalacją, konfiguracją i zarządzaniem usługą sieciową VPN	spr, egz	wykład, laboratorium	K1A_W06, T1A_W04, T1A_U01, T1A_K01
5	… posiada szczegółową i podbudowaną teoretycznie wiedzę związaną z planowaniem oraz wdrażaniem mechanizmów wysokiej dostępności usług sieciowych w systemie MS Windows Server	spr, egz	wykład, laboratorium	K1A_W06, T1A_W04, T1A_U01, T1A_K01
6	… rozumie cele stosowania oraz zasady działania, i potrafi wdrożyć zarządzanie aplikacjami w systemach MS Windows	spr, egz	wykład, laboratorium	K1A_W06, T1A_W04, T1A_U01, T1A_K01

19. Treści kształcenia:

Wykład:

1. Zagrożenia dla bezpieczeństwa informacji i sposoby przeciwdziałania tym zagrożeniom.
2. Jednokierunkowe funkcje skrótu. Typy ataków na funkcje jednokierunkowe.
3. Szyfrowanie symetryczne.
4. Szyfrowanie asymetryczne.
5. Zagadnienia dotyczące infrastruktury klucza publicznego oraz podpisu elektronicznego.
6. Zasady działania protokołu SSL/TLS.
7. Zarządzanie urzędem certyfikującym. Lista CRL oraz protokół OCSP.
8. Metody uwierzytelniania użytkowników stosowane w systemach teleinformatycznych (PAP, CHAP, MS-CHAP, LM, NTLM, Kerberos).
9. Szyfrowanie systemów plików.
10. Dostęp zdalny przy użyciu połączenia VPN
11. Mechanizmy wysokiej dostępności usług sieciowych i aplikacji
12. Planowanie wykorzystania zaawansowanych usług serwera plików w systemie MS Windows Server
13. Zarządzanie aktualizacjami i aplikacjami w systemie MS Windows Server

Laboratorium:

1. Szyfrowanie danych z wykorzystaniem GnuPG
2. Instalacja i konfiguracja roli Active Directory Certificate Services w systemie Windows Server,
3. Zarządzanie certyfikatami w ramach urzędu certyfikacyjnego zintegrowanego z usługą Active Directory w systemie Windows Server, obsługa listy CRL oraz wykorzystanie protokołu OCSP
4. Wdrażanie usługi szyfrowania danych EFS z wykorzystaniem infrastruktury klucza publicznego
5. Wykorzystanie mechanizmu Bitlocker/Bitlocker To Go
6. Dostęp zdalny do zasobów sieciowych firmy z wykorzystaniem usługi VPN w systemie Windows Server oraz GNU/Linux
7. Mechanizmy wysokiej dostępności w systemie Windows Server (DNS Round Robin, Network Load Balancing, Failover Clustering)
8. Zarządzanie aktualizacjami w systemach MS Windows z wykorzystaniem Windows Server Update Service (WSUS),
9. Zarządzanie aplikacjami w systemach MS Windows (AppLocker, Software Restrictions Policies),

20. Egzamin: tak

21. Literatura podstawowa:

1. B.Schneier: Kryptografia dla praktyków. WNT, Warszawa 2002
2. N. Ferguson, B. Schneier: Kryptografia w praktyce. Helion 2004
3. W. Stallings: Ochrona danych w sieci i intersieci w teorii i praktyce. WNT, Warszawa 1997
4. Dillard K.: Egzamin 70-412. Konfigurowanie zaawansowanych usług Windows Server 2012 R2. Wyd. Microsoft Press 2014
5. Stanek W. R.: Vademecum Administratora Windows Server 2012, Helion, Gliwice 2014

22. Literatura uzupełniająca:

1. K. Mitnick: Sztuka podstępu. Łamanie ludzi, nie haseł. Helion 2003
2. J. Stokłosa, T. Bliski, T. Pankowski: Bezpieczeństwo danych w systemach informatycznych. PWN 2001
3. M. Kutyłowski, W. Strothmann: Kryptografia, Lupus, 1998
4. J.C. Mackin, Tony Northrup: Training Kit 70-642 Konfigurowanie infrastruktury sieciowej Windows Server 2008 Egzamin MCTS 70-642, Wyd. PROMISE, 2009

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	30/60
4	Projekt	-/-
5	Seminarium	-/-
6	Inne:	-/-
	Suma godzin	60/90

24.

Suma wszystkich godzin	150

25.

Liczba punktów ECTS	5

26.

Liczba punktów ECTS uzyskanych na zajęciach z bezpośrednim udziałem nauczyciela akademickiego	5

27.

Liczba punktów ECTS uzyskanych na zajęciach o charakterze praktycznym (laboratoria, projekty)	3

28. Uwagi:

Brak

Zatwierdzono:

…….
(data i podpis prowadzącego)

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