(pieczęć wydziału)

KARTA PRZEDMIOTU

1. Nazwa przedmiotu: Bezpieczeństwo systemów informatycznych	**2. Kod przedmiotu:** BSI
3. Karta przedmiotu ważna od roku akademickiego: 2019/20	
4. Forma kształcenia: studia pierwszego stopnia	
5. Forma studiów: studia stacjonarne	
6. Kierunek studiów: INFORMATYKA (SYMBOL WYDZIAŁU) **RMS**	
7. Profil studiów: ogólnoakademicki	
9. Semestr: 6	
10. Jednostka prowadząca przedmiot: Instytut Matematyki	
11. Prowadzący przedmiot: dr inż. Jarosław Karcewicz	
12. Przynależność do grupy przedmiotów: przedmioty swobodnego wyboru (przedmiot obieralny)	
13. Status przedmiotu: obieralny	
14. Język prowadzenia zajęć: polski	
15. Cel przedmiotu: Celem przedmiotu jest przekazanie studentom wiedzy na temat funkcjonowania mechanizmów szyfrowania danych, w tym w szczególności infrastruktury klucza publicznego, jak również mechanizmów zarządzania tożsamością i kontroli dostępu, których znajomość jest nieoceniona podczas procesu tworzenia oprogramowania.	

16. 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, kol	wykład, laboratorium	K1P_W09 K1P_W11 K1P_U23 K1P_U33
2	… ma szczegółową i podbudowaną teoretycznie wiedzę w zakresie mechanizmów uwierzytelniania i autoryzacji użytkowników stosowane w systemach teleinformatycznych	spr, kol	wykład, laboratorium	K1P_W09 K1P_W11 K1P_U23 K1P_U33
3	… ma szczegółową i podbudowaną teoretycznie wiedzę w zakresie metod i mechanizmów szyfrowania danych na nośnikach danych	spr, kol	wykład, laboratorium	K1P_W09 K1P_W11 K1P_U23 K1P_U33

4	… ma szczegółową i podbudowaną teoretycznie wiedzę w zakresie zarządzania urzędem certyfikującym	spr, kol	wykład, laboratorium	K1P_W09 K1P_W11 K1P_U23 K1P_U33
5	… posiada podstawową i podbudowaną teoretycznie wiedzę związaną z instalacją, konfiguracją i zarządzaniem usługą sieciową VPN na potrzeby zabezpieczenia transmisji między aplikacją kliencką i serwerową wykorzystywanymi w celach biznesowych	spr, kol	wykład, laboratorium	K1P_W09 K1P_W11 K1P_U23 K1P_U33

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

Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
30	-	30	-	-

18. Treści kształcenia:

Wykład:

1. Problematyka zarządzania tożsamością i kontroli dostępu, tj. uwierzytelniania i autoryzacji użytkowników, m.in. w ramach oprogramowania tworzonego w architekturze klient-serwer
2. Mechanizmy szyfrowania danych
3. Zasady działania infrastruktury klucza publicznego i urzędu certyfikacji, oraz protokołów SSL/TLS i IPsec
4. Analiza narzędzia PGP/GPG jako przykład wykorzystania klucza asymetrycznego i podpisu cyfrowego w ramach tworzonego oprogramowania
5. Analiza usługi EFS na potrzeby szyfrowania danych jako przykład wykorzystania infrastruktury klucza publicznego w ramach tworzonego oprogramowania
6. Analiza mechanizmu szyfrowania danych Bitlocker/Bitlocker To Go jako przykład szyfrowania danych w ramach tworzonego oprogramowania
7. Analiza realizacji dostępu zdalnego do zasobów informatycznych firmy z wykorzystaniem usługi VPN jako przykład wykorzystania infrastruktury klucza publicznego, oraz protokołu SSL/TLS i IPsec w ramach tworzonego oprogramowania
8. Analiza wykorzystania mechanizmów uwierzytelniana poprzez sieć komputerową w ramach oprogramowania tworzonego w architekturze klient-serwer (Kerberos, LM, NTLM, PAP, CHAP, MS-CHAP, EAP/PEAP)

Laboratorium:

1. Zarządzanie tożsamością i kontrolą dostępu, tj. uwierzytelniania i autoryzacji użytkowników w systemie operacyjnym na przykładzie MS Windows
2. Zarządzanie dostępem do zasobu sieciowego w systemie MS Windows jako m.in. przykład potrzeb wykorzystania usługi Active Directory w ramach oprogramowania tworzonego na potrzeby biznesowe
3. Podstawy zarządzania usługą Active Directory jako systemu scentralizowanego uwierzytelniania dla wielu różnych aplikacji wykorzystywanych w zastosowaniach biznesowych
4. Zarządzanie urzędem certyfikującym, obsługującym wydawanie certyfikatów dla aplikacji
5. Analiza narzędzia PGP/GPG jako przykład wykorzystania klucza asymetrycznego i podpisu cyfrowego w ramach tworzonego oprogramowania
6. Analiza mechanizmu szyfrowania danych Bitlocker/Bitlocker To Go oraz EFS jako przykład szyfrowania danych w ramach tworzonego oprogramowania
7. Analiza realizacji dostępu zdalnego do zasobów informatycznych firmy z wykorzystaniem usługi VPN jako przykład wykorzystania infrastruktury klucza publicznego oraz protokołu SSL/TLS i IPsec w ramach tworzonego oprogramowania

20. Egzamin: nie

21. Literatura podstawowa:

1. M. Karbowski: Podstawy kryptografii. Wydanie III. Wyd. Helion 2014
2. Jean-Philippe Aumasson: Nowoczesna kryptografia. Praktyczne wprowadzenie do szyfrowania. Wyd. Naukowe PWN 2018
3. B. Schneier: Kryptografia dla praktyków. WNT, Warszawa 2002
4. N. Ferguson, B. Schneier: Kryptografia w praktyce. Helion 2004
5. Andrew James Warren: Egzamin 70-742: Tożsamość w Windows Server 2016, Wyd. Promise 2017
6. Szeląg A.: Windows Server 2008. Infrastruktura klucza publicznego (PKI). Wyd. Helion 2008

22. Literatura uzupełniająca:

1. Dillard K.: Egzamin 70-412. Konfigurowanie zaawansowanych usług Windows Server 2012 R2. Wyd. Microsoft Press 2014
2. J. Stokłosa, T. Bliski, T. Pankowski: Bezpieczeństwo danych w systemach informatycznych. PWN 2001
3. M. Kutyłowski, W. Strothmann: Kryptografia, Lupus, 1998
4. W. Stallings: Ochrona danych w sieci i intersieci w teorii i praktyce. WNT, Warszawa 1997

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	4

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)*