(pieczęć wydziału)

KARTA PRZEDMIOTU

1. Nazwa przedmiotu: Bezpieczeństwo systemów informatycznych	**2. Kod przedmiotu:**
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: 5 lub 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	
16. 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 niezbędna podczas procesu tworzenia oprogramowania.	

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

Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
30h		30h		

19. Treści kształcenia:

1. Mechanizmy szyfrowania danych (funkcja skrótu, klucz symetryczny, klucz asymetryczny)
2. Zasady działania infrastruktury klucza publicznego i urzędu certyfikacji, oraz protokołów SSL/TLS i IPsec
3. Problematyka zarządzania tożsamością i kontroli dostępu, tj. uwierzytelniania i autoryzacji użytkowników, m.in. w ramach oprogramowania tworzonego w architekturze klient-serwer
4. Analiza narzędzia PGP/GPG jako przykład wykorzystania klucza asymetrycznego i podpisu cyfrowego w ramach tworzonego oprogramowania
5. Analiza oprogramowania EFS (Encrypted File System) 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)