(pieczęć wydziału)

KARTA PRZEDMIOTU

1. Nazwa przedmiotu: Bezpieczeństwo sieciowych systemów operacyjnych	**2. Kod przedmiotu:**
3. Karta przedmiotu ważna od roku akademickiego: 2020/201	
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	
16. Cel przedmiotu: Celem przedmiotu jest przekazanie studentom wiedzy na temat różnego rodzaju aspektów bezpieczeństwa działania samego systemu operacyjnego MS Windows Server oraz GNU/Linux, jak również aspektów bezpieczeństwa związanych z wykorzystaniem podstawowych ról, usług sieciowych jaką mogą pełnić te w/w systemy operacyjne w ramach lokalnej sieci komputerowej w zastosowaniach biznesowych.	

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

Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
30h		30h		

19. Treści kształcenia:

1. Wybrane zagadnienia monitorowania i hardeningu systemu MS Windows Server oraz GNU/Linux
2. Planowanie i wdrażanie mechanizmów zarządzania aplikacjami oraz aktualizacjami w systemie MS Windows
3. Planowanie i wdrażanie zaawansowanych usług serwera plików w systemie MS Windows Server (DFS, FSRM, BranchCache, Work Folders, Dynamic Access Control)
4. Zabezpieczanie usługi DNS (m.in. DNSsec, mechanizm TSIG, rekord DANE SSHFP, rekord DANE TLSA, rekord CAA)
5. Zabezpieczanie usługi HTTP (na przykładzie Apache2: HTTPS, HSTS, ModSecurity, ModEvasive, itp.)
6. Instalacja oraz konfiguracja usługi VPN typu „Remote-Access" oraz „Site-to-Site" w systemach Windows Server oraz GNU/Linux (OpenVPN, StrongSwan, PPTP, L2TP/IPsec, SSTP)
7. Planowanie i wdrażanie mechanizmów wysokiej dostępności usług sieciowych (NLB, klaster pracy awaryjnej)
8. Uwierzytelnianie klientów sieci Wi-Fi oraz sieci przewodowej do Active Directory