Kurs w zakresie bezpieczeństwa systemów sieciowych

PRZEDMIOT (liczba godzin wykładów/ćwiczeń)	**WYMAGANE TREŚCI MERYTORYCZNE ZAJĘĆ**
Zagrożenia w nowoczesnych sieciach komputerowych (2/2)	1. Omówienie zagrożeń występujących we współczesnych sieciach komputerowych 2. Podstawy działania bezpiecznych sieci 3. Organizacje zajmujące się problematyką bezpieczeństwa w sieciach 4. Wirusy, konie trojańskie i robaki komputerowe – wykrywanie i zapobieganie 5. Metody ataków na sieci komputerowe
Zabezpieczenie urządzeń sieciowych (2/7)	1. Zabezpieczanie routerów brzegowych 2. Konfigurowanie bezpiecznego dostępu administracyjnego 3. Prawa administracyjne: poziomy uprzywilejowania i dostęp na podstawie uprawnień 4. Monitorowanie urządzeń sieciowych (syslog, SNMP, NTP) 5. Zabezpieczanie plików na urządzeniach sieciowych. 6. Automatyczne metody zabezpieczania urządzeń.
Uwierzytelnianie, autoryzacja i ewidencjonowanie (2/7)	1. Charakterystyka rozwiązań AAA (Authentication, Authorization, and Accounting) 2. Rozwiązania AAA bazujące na rozwiązaniach serwerowych
Technologie filtrowania ruchu sieciowego (2/7)	1. Listy dostępu ACL 2. Technologie zapór ogniowych (firewalls) 3. Filtrowanie ruchu 4. Firewall bazujący na definicji obszarów
Systemy zapobiegania i wykrywania intruzów (2/7)	1. Omówienie Intrusion Detection Systems (IDS) - systemy wykrywania intruzów 2. Omówienie Intrusion Prevention Systems (IPS) - systemy ochrony przed intruzami 3. Sygnatury IPS 4. Zarządzanie i monitorowanie systemów IPS 5. Implementacja IPS
Zabezpieczenie sieci lokalnych (2/7)	1. Bezpieczeństwo urządzeń końcowych 2. Zagrożenia związane z warstwą drugą ISO OSI 3. Eliminowanie zagrożeń warstwy drugiej 4. Bezpieczeństwa w sieciach bezprzewodowych i sieciach obsługujących
Systemy kryptograficzne (2/7)	1. Zabezpieczanie komunikacji sieciowej 2. Kryptografia, kryptoanaliza, kryptologia 3. Poufność, autentyczność i integralność danych 4. Kryptografia z kluczem publicznym

Wirtualne sieci prywatne (2/7)	1. Podstawy, topologie i rozwiązania sieci prywatnych 2. Protokół IPsec – komponenty i działanie 3. Bezpieczne połączenia Site-to-Site 4. Zdalny bezpieczny dostęp do sieci
Zarządzanie bezpieczną siecią (2/7)	1. Zasady projektowania bezpiecznych sieci komputerowych 2. Testowanie bezpieczeństwa 3. Planowanie ciągłości działania sieci i napraw po awariach 4. Opracowywanie wszechstronnych zasad bezpieczeństwa
Wdrażanie rozwiązań ASA w sieciach komputerowych (2/7)	1. Wprowadzenie do rozwiązań ASA (Adaptive Security Appliance) 2. Konfiguracja zapory ogniowej na urządzeniach ASA 3. Konfigurowanie bezpiecznych tuneli VPN ASA
Podstawy przedsiębiorczości (5/0)	1. Formy organizacyjno-prawne przedsiębiorstwa (działalność gospodarcza, spółka cywilna, spółki prawa handlowego: osobowe i kapitałowe). 2. Procedury i wymagania związane z zakładaniem działalności gospodarczej. 3. Uproszczone formy ewidencyjne (karta podatkowa, ryczałt, PKPiR) 4. Różne formy zatrudnienia pracownika. Podstawowe przepisy Kodeksu Pracy. 5. Źródła finansowania przedsiębiorstw. Finansowanie z wykorzystaniem środków z dotacji. 6. Zarządzanie projektami IT (metodyki brytyjskie, podejście agile, SCRUM).