SYLABUS (KARTA PRZEDMIOTU/MODUŁU)

Nazwa przedmiotu/modułu (zgodna z zatwierdzonym programem studiów na kierunku)	Punkty ECTS	Numer katalogowy
Bezpieczeństwo sieci komputerowych A	**4**	
Nazwa w j. angielskim **Computer networks security A**		

Jednostka(i) realizująca(e) przedmiot/moduł (instytut/katedra)
Instytut Inżynierii Biosystemów
Kierownik przedmiotu/modułu **dr inż. Sebastian Kujawa**

Kierunek studiów	Poziom	Profil	Semestr
Informatyka stosowana	**Studia II stopnia**	**ogólnoakademicki**	**2**
Specjalność -	Specjalizacja magisterska -		

RODZAJE ZAJĘĆ I ICH WYMIAR GODZINOWY
(zajęcia zorganizowane i praca własna studenta)

Forma studiów: stacjonarne		Forma studiów: niestacjonarne	
− wykłady	**15**	− wykłady	**10**
− ćwiczenia laboratoryjne	**30**	− ćwiczenia laboratoryjne	**20**
− inne z udziałem nauczyciela	**15**	− inne z udziałem nauczyciela	**5**
− praca własna studenta	**40**	− praca własna studenta	**65**
Łączna liczba godzin:	**100**	Łączna liczba godzin:	**100**

CEL PRZEDMIOTU/MODUŁU

Celem modułu jest przedstawienie zagrożeń płynących z eksploatacji systemów sieciowych, będących nieodłącznym aspektem współczesnego, efektywnego zarządzania przedsiębiorstwem rolniczym oraz przedstawienie i przećwiczenie metod zabezpieczania sieci komputerowych i przetwarzanych danych przed niepowołanym dostępem i przetwarzaniem.

METODY DYDAKTYCZNE

Wykłady multimedialne z elementami pokazu dynamicznego, ćwiczenia praktyczne w laboratorium komputerowym z wykorzystaniem systemów wirtualnych (projektowanie, wdrażanie, eksploatacja oraz analiza systemów bezpieczeństwa sieciowego).

	EFEKTY KSZTAŁCENIA	Odniesienie do efektów kierunkowych
Wiedza	**E1.** Posiada zaawansowaną wiedzę w zakresie identyfikacji zagrożeń oraz bezpieczeństwa infrastruktury sieciowej.	**IS2A_W11** **IS2A_W13**
Umiejętności	**E2.** Potrafi stosować standardy zabezpieczeń sieci i systemów informatycznych w praktyce. Zna konsekwencje prawne naruszeń bezpieczeństwa w sieciach. **E3.** Potrafi opracować podstawowy projekt sieci komputerowej uwzględniający zabezpieczenia tej sieci na potrzeby przemysłu rolniczego. **E4.** Posiada umiejętność posługiwania się słownictwem z zakresu bezpieczeństwa sieci komputerowych w języku angielskim.	**IS2A_U07** **IS2A_U13** **IS2A_U16** **IS2A_U17**
Kompetencje	**E5.** Rozumie potrzebę ciągłego rozwoju technologii sieciowych, rozwoju metod obrony i ataku i konieczności ciągłego dokształcania się w zakresie bezpieczeństwa i eksploatacji sieci i systemów komputerowych. **E6.** Ma świadomość pozatechnicznych skutków podejmowanych działań, w szczególności skutków społecznych ataków informatycznych. **E7.** Wykazuje kreatywność w zakresie doboru zabezpieczeń do klasy projektowanego rozwiązania sieciowego.	**IS2A_K02** **IS2A_K04** **IS2A_K05**

Metody weryfikacji efektów kształcenia	Numery efektów
Kolokwium w formie testu. Prezentacja multimedialna. Egzamin pisemny.	**E1 - E7**

TREŚCI KSZTAŁCENIA

Wykłady:

- Bezpieczeństwo komputerowe – pojęcia kluczowe. Triada wymogów bezpieczeństwa: poufność, integralność i dostępność. Zagrożenia i ataki, klasyfikacja ataków – ataki bierne i czynne.
- Bezpieczeństwo haseł w Linux: skróty haseł, moduły PAM.
- Kryptologia, kryptografia i kryptoanaliza. Algorytmy i protokoły kryptograficzne – klasyfikacja, algorytmy szyfrowania symetrycznego i asymetrycznego, funkcje skrótu, podpisy cyfrowe.
- Narzędzia PGP i GnuPG – szyfrowanie symetryczne, asymetryczne i podpisywanie danych, zarządzanie kluczami, wykorzystanie serwerów kluczy.
- Wykorzystanie mechanizmów kryptograficznych (szyfrowanie, podpisy cyfrowe) w ramach poczty elektronicznej. Szyfrowanie zasobów w systemie Linux.
- Protokoły SSH – uwierzytelnianie z użyciem kluczy, generowanie i dystrybucja kluczy, montowanie zdalnych zasobów, tunelowanie połączeń.
- Narzędzia i biblioteki OpenSSL. Certyfikaty X.509 – urzędy certyfikacji (CA), ścieżka certyfikacji, procedura tworzenia certyfikatów (klucz prywatny, żądanie certyfikatu, podpisywanie żądania certyfikatu).
- Osadzanie certyfikatów na serwerach szyfrowanych usług sieciowych.
- Wirtualne sieci prywatne (VPN) i IPsec. OpenVPN – konfiguracja klientów i serwerów, tryby pracy (routing, bridging), uwierzytelnianie, protokoły transportowe.

Ćwiczenia:

- Instalacja i konfiguracja środowiska roboczego w postaci maszyn wirtualnych. Zarządzanie maszynami wirtualnymi.
- Bezpieczeństwo systemu Linux (algorytmy wyznaczania skrótów haseł, polityka haseł, PAM-Linux).
- GnuPG – szyfrowanie symetryczne i asymetryczne, importowanie i eksportowanie kluczy publicznych i prywatnych, unieważnianie kluczy, podpisy cyfrowe.
- Szyfrowanie zasobów z użyciem narzędzia eCryptfs.
- SSH – uwierzytelnianie z użyciem kluczy, montowanie zdalnych katalogów, tunelowanie połączeń, dodatkowe narzędzia: ssh-agent, keychain, sshfs.
- Certyfikaty X.509 – instalacja OpenSSL, tworzenie certyfikatów w OpenSSL (klucze prywatne, żądania certyfikatu). Tworzenie własnego urzędu certyfikacji (CA) i podpisywanie żądań certyfikatu.
- Certyfikaty X.509 – konfiguracja bezpiecznych (szyfrowanych) usług sieciowych.
- Tworzenie wirtualnych sieci prywatnych z wykorzystaniem OpenVPN.
- Konfiguracja ściany ogniowej z wykorzystaniem narzędzia iptables.
- Zabezpieczanie sieci bezprzewodowych.

Formy i kryteria zaliczenia przedmiotu/modułu	Procentowy udział w końcowej ocenie
Kolokwium w formie testu	70% oceny z ćwiczeń
Prezentacja multimedialna	30% oceny z ćwiczeń
Egzamin pisemny	100% oceny z egzaminu

WYKAZ LITERATURY

- Nemeth E., Snyder G., Hein T.R., Whaley B. (2011): Unix i Linux. Przewodnik administratora systemów. Wydanie IV. Helion, Gliwice.
- Stallings W. (2011): Kryptografia i bezpieczeństwo sieci komputerowych. Matematyka szyfrów i techniki kryptologii. Helion, Gliwice.
- Stallings W. (2012): Kryptografia i bezpieczeństwo sieci komputerowych. Koncepcje i metody bezpiecznej komunikacji, Helion, Gliwice.