Akademia Nauk Stosowanych

im. Hipolita Cegielskiego w Gnieźnie Uczelnia Państwowa

SYLABUS

Pozycja przedmiotu w planie:		R.III/S.VI - 6
1. **OGÓLNY OPIS PRZEDMIOTU**		
1	Nazwa modułu	Moduł zajęć kierunkowych
2	Nazwa przedmiotu	Bezpieczeństwo systemów informatycznych
3	Kierunek studiów	Informatyka
4	Poziom studiów	pierwszy
5	Forma studiów	stacjonarne
6	Profil studiów	praktyczny
7	Rok studiów	trzeci
8	Semestr przedmiotu	szósty
9	Jednostka prowadząca kierunek studiów	Instytut Nauk Technicznych
10	Liczba punktów ECTS	3
11	Sposób zaliczenia:	wykład: egzamin laboratorium: zaliczenie z oceną
12	Imię i nazwisko nauczyciela (li) akademickiego (ich), stopień lub tytuł naukowy, adres e-mail	dr hab. inż. Piotr Remlein, p.remlein@ans-gniezno.edu.pl; dr inż. Tomasz Łukaszewski, tomasz.lukaszewski@cs.put.poznan.pl
13	Imię i nazwisko koordynatora(ów) przedmiotu, stopień lub tytuł naukowy, adres e-mail	dr hab. Inż. Piotr Remlein, p.remlein@ans-gniezno.edu.pl;
14	Język wykładowy	Polski
15	Tryb prowadzenia zajęć	Mieszany
16	Sposób prowadzenia zajęć	Synchroniczny
17	Narzędzia informatyczne wykorzystywane do prowadzenia zajęć, udostępniania materiałów i komunikacji ze studentami	Platforma Microsoft Teams/Patforma Moodle
15	Przedmioty wprowadzające	Matematyka dyskretna Sieci komputerowe Systemy operacyjne
16	Wymagania wstępne	1. Podstawowe wiadomości z dziedziny systemów operacyjnych i sieci komputerowych 2. Sprawność posługiwania się systemem operacyjnym Unix I Windows oraz programowania 3. Świadomość konieczności poszerzania kompetencji oraz gotowość do podjęcia współpracy w ramach zespołu
17	**Cele przedmiotu:**	
C1	Poznanie podstawowych problemów bezpieczeństwa systemów informatycznych	

C2	Uzyskanie umiejętności posługiwania się mechanizmami kryptograficznymi, kontroli dostępu, filtracji ruchu sieciowego.
C3	Poznanie informacji na temat tuneli wirtualnych oraz zabezpieczeń warstwy aplikacyjnej
18	Forma zajęć, liczba godzin wymagająca bezpośredniego udziału nauczyciela akademickiego, liczba godzin nakładu pracy studenta

Forma zajęć	Liczba godzin
1. Wykłady	30
2. Laboratorium	30
3.	
Suma godzin	60

lp.	**Całkowity nakład pracy studenta**	
1.	Nakład pracy związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela akademickiego wynosi:	**Godzinowe obciążenie studenta**
	Wykład: 30 godz.	62 godzin
	Laboratoria: 30 godz.	
	Konsultacje: 2 godz.	
	Nakład pracy związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela akademickiego wynosi 65 godzin, co odpowiada 2 punktom ECTS.	
2	Bilans nakładu pracy studenta: • Przygotowanie do laboratorium: 10 godzin, • Przygotowanie do egzaminu: 10 godzin, • Przygotowanie do zaliczenia z laboratorium: 5 godzin, Łączny nakład pracy studenta wynosi 25 godzin, co odpowiada 1 punktowi ECTS.	25 godzin
3	**Łączny nakład pracy studenta (pozycja 1+2)**	87 godzin
4	**Punkty ECTS za przedmiot**	3 ECTS
5	Liczba punktów ECTS, którą student musi osiągnąć w ramach zajęć o charakterze praktycznym w tym zajęć laboratoryjnych, warsztatowych, projektowych	2 ECTS

Efekty uczenia – wiedza	K_W15: Zna i rozumie zasady poprawnej i bezpiecznej eksploatacji systemów informatycznych w tym korzystania z narzędzi kryptograficznych, tuneli VPN, zapór sieciowych i systemów IDS. K_W14: Ma podstawową wiedzę niezbędną rozpoznania zagrożeń bezpiecznej eksploatacji systemów operacyjnych, sieci komputerowych i aplikacji użytkowych K_W16: Ma wiedzę niezbędną do właściwego doboru i zastosowania podstawowych mechanizmów uwierzytelniania, ochrony poufności i integralności danych i komunikacji.
Efekty uczenia - umiejętności	K_U10: Potrafi dokonywać konfiguracji systemu operacyjnego i urządzeń sieciowych zmierzającej do podnoszenia bezpieczeństwa ich pracy K_U19: Potrafi posługiwać się zaporami sieciowymi, pakietami kryptograficznymi na poziomie podstawowych usług aplikacyjnych (m.in. SSH, PGP) K_U21: Potrafi budować prawidłowe środowisko komunikacji przy wykorzystaniu tuneli VPN (za pomocą protokołu IPsec) i mechanizmów SSO
Efekty uczenia – kompetencje społeczne	K_K01: Rozumie potrzebę permanentnego kształcenia się i przekazywania w sposób zrozumiały informacji z najbliższym otoczeniem w działalności zawodowej. K_K04: Ma świadomość odpowiedzialności za pracę własną oraz gotowość podporządkowania się zasadom pracy w zespole i ponoszenia odpowiedzialności za wspólnie realizowane zadania; potrafi określić priorytety działania

2. **TREŚCI PROGRAMOWE ODNIESIONE DO EFEKTÓW UCZENIA SIĘ**		
	Treści programowe	**liczba godzin**
Forma: wykład		
W1	Elementy kryptografii: podstawy matematyczne szyfrowania, szyfrowanie symetryczne i asymetryczne, algorytmy szyfrowania, podpis elektroniczny, infrastruktura klucza publicznego, zastosowania kryptografii (EFS, PGP, S/MIME).	4
W2	Zagrożenia systemów informatycznych w kontekście poufności, integralności i dostępności informacji	4
W3	Bezpieczeństwo protokołów komunikacyjnych.	2
W4	Mechanizm NAT/PAT. Filtrowanie ruchu sieciowego – listy kontroli dostępu (ACL).	4
W5	Zabezpieczenia protokołów routingu. Konfiguracja protokołu SSH. Działanie i wykorzystanie RADIUS i TACACS+.	4
W6	Bezpieczeństwo aplikacji i usług komunikacyjnych, m.in. www, poczty elektronicznej oraz komunikatorów internetowych. Problematyka bezpiecznego programowania –budowa aplikacji sieciowych.	4
W7	Zapory sieciowe (firewall), strefy zdemilitaryzowane. Wirtualne sieci prywatne (VPN).	4
W8	Projektowanie i wdrażanie polityki bezpieczeństwa systemu informatycznego, zarządzanie bezpieczeństwem, narzędzia analizy zabezpieczeń i monitoringu.	4
Forma: laboratoria		
L1	Bezpieczeństwo protokołów komunikacyjnych.	4
L2	Poznanie podstawowych problemów bezpieczeństwa systemów informatycznych.	4
L3	Uzyskanie umiejętności posługiwania się mechanizmami kryptograficznymi.	4
L4	Uzyskanie umiejętności posługiwania się mechanizmami kontroli dostępu.	4
L5	Uzyskanie umiejętności posługiwania się mechanizmami filtracji ruchu sieciowego, tuneli wirtualnych, sieci VPN.	6
L6	Realizacja zabezpieczeń warstwy aplikacyjnej.	4
L7	Poznanie sposobów konfiguracji zabezpieczeń na urządzeniach sieciowych.	4

3. **Literatura**	
Literatura podstawowa	1. K. Liderman, „Bezpieczeństwo informacyjne”, Warszawa: Wydawnictwo Naukowe PWN , 2020. 2. Janusz Stokłosa, Tomasz Bliski, Tadeusz Pankowski, „Ochrona danych w systemach teleinformatycznych”, Poznań : Wydawnictwo Politechniki Poznańskiej , 2005 3. W. Stallings, L. Brown, „Ochrona danych w sieci i intersieci”, Warszawa: Wydawnictwa Naukowo-Techniczne, 1997
Literatura uzupełniająca	1. W. Stallings, L. Brown, Bezpieczeństwo systemów informatycznych. Zasady i praktyka. Wydanie IV. 2. William R. Cheswick, „Firewalle i bezpieczeństwo w sieci”, Helion, 2003. 3. Jie Wang, “Computer Network Security Theory and Practice”, Higher Education Press, 2009. 4. Niels Ferguson, Bruce Schneier, „Kryptografia w praktyce”, Helion, 2004 5. A. Józefiok, Security CCNA 210-260. Zostań administratorem sieci komputerowych Cisco, Helion 2016. 6. William Stallings, “Network Security Principles and Practices”, IV ed., Prentice Hall, 2005 7. David Salomon, “Elements of Computer Security”, Springer-Verlag, 2010..

4. **Metody dydaktyczne**	
Forma	**Metody dydaktyczne**
Wykład	Wykład: wykład informacyjny i częściowo konwersatoryjny, prezentacja multimedialna przygotowana przez prowadzącego zajęcia, ilustrowana przykładami

Laboratoria	Wykonanie zadań podanych przez prowadzącego. Ćwiczenia praktyczne z wykorzystaniem dostępnego w laboratorium oprogramowania. Laboratoria mogą być uzupełnianie poprzez prezentacje multimedialne i podawane przykłady.

5, Metody i kryteria oceniania

Forma zajęć: wykład	**Forma zaliczenia: egzamin**

Uzyskane punkty są przeliczane na oceny według następującej skali:

Procent punktów:	***Ocena:***
91-100%	Bardzo dobry
85-90%	Dobry plus
76-84%	Dobry
66-75%	Dostateczny plus
51-65%	Dostateczny
0-50%	Niedostateczny

Opis: Egzamin w formie testu na platformie Moodle lub egzamin pisemny złożony z kilkunastu zagadnień dotyczących omawianych problemów .

Forma zajęć: laboratoria	**Forma zaliczenia: zaliczenie z oceną**

Uzyskane punkty są przeliczane na oceny według następującej skali:

Procent punktów:	***Ocena:***
91-100%	Bardzo dobry
85-90%	Dobry plus
76-84%	Dobry
66-75%	Dostateczny plus
51-65%	Dostateczny
0-50%	Niedostateczny

Opis: Zaliczenie w laboratorium – zadania ze znajomości omawianych zagadnień.

Warunkiem zaliczenia przedmiotu jest uzyskanie oceny pozytywnej ze wszystkich form zajęć.

	Zatwierdzenie karty opisu zajęć	
	Stanowisko Tytuł/stopień naukowy, imię nazwisko	**Podpis**
Opracował	Dr hab. inż. Piotr Remlein	
Zatwierdził	Dyrektor Instytutu Nauk Technicznych	