

PAŃSTWOWA WYŻSZA SZKOŁA ZAWODOWA W NOWYM SĄCZU

KARTA PRZEDMIOTU

obowiązuje studentów rozpoczynających studia w roku akademickim 2016/2017

Instytut Techniczny

Kierunek studiów: Informatyka

Profil: Praktyczny

Forma studiów: Stacjonarne

Kod kierunku: 11.3

Stopień studiów: I

Specjalności: Informatyka stosowana

1 PRZEDMIOT

NAZWA PRZEDMIOTU	Bezpieczeństwo systemów informatycznych
KOD PRZEDMIOTU	IT 11.3 PIS C5 16/17
KATEGORIA PRZEDMIOTU	Przedmioty specjalnościowe
LICZBA PUNKTÓW ECTS	3
SEMESTRY	4

2 RODZAJ ZAJĘĆ, LICZBA GODZIN W PLANIE STUDIÓW

SEMESTR	WYKŁAD	ĆWICZENIA	LABORATORIUM	PROJEKT	SEMINARIUM
4	15			30	

3 CELE PRZEDMIOTU

Cel 1 Przedmiot ma na celu zapoznanie studentów z podstawowymi zasadami i mechanizmami bezpieczeństwa systemów informatycznych.

Cel 2 Student potrafi oceniać i zarządzać bezpieczeństwem systemów informatycznych, potrafi wraz z zespołem zaprojektować, a następnie stworzyć politykę bezpieczeństwa informacji, zasady metodologii rozwoju, tworzenia, wdrażania i skuteczności wykorzystania.



4 WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

a Sieci komputerowe Systemy operacyjne Programowanie na C, C++, PHP

5 EFEKTY KSZTAŁCENIA

- EK1** Wiedza: Posiada wiedzę dotyczącą projektowania i obsługi sieci informatycznych oraz tworzenia aplikacji internetowych, zna zagadnienia związane z bezpieczeństwem tych aplikacji oraz metody stosowane w ich projektowaniu i obsłudze sieci.
- EK2** Wiedza: Posiada wiadomości dotyczące stanu obecnego rozwoju informatyki oraz kierunków jej rozwoju.
- EK3** Umiejętności: Potrafi ocenić przydatność i sposób funkcjonowania, istniejące rozwiązania elementów informatycznych, możliwość ich zastosowania dla konkretnego systemu lub sieci informatycznej.
- EK4** Umiejętności: Potrafi dokonać analizy krytycznej wyników funkcjonalnego i strukturalnego testowania systemu informatycznego.
- EK5** Umiejętności: Potrafi zaprojektować sieć komputerową oraz tworzyć bezpieczne aplikacje internetowe i zabezpieczyć je przed typowymi atakami.
- EK6** Umiejętności: Potrafi określić parametry, cechy pożądane elementów informatycznych i opracować etapy budowy prostego systemu informatycznego.
- EK7** Kompetencje społeczne: Ma świadomość ważności zachowania w sposób profesjonalny, przestrzegania zasad etyki zawodowej, bezpieczeństwa i higieny pracy, ochrony własności intelektualnej oraz poszanowania różnorodności poglądów i kultur.
- EK8** Kompetencje społeczne: Ma świadomość dotyczącą swojej roli wykształconego inżyniera informatyka w lokalnym społeczeństwie, w szczególności dotyczącą propagacji nowoczesnych rozwiązań informatycznych, ich wpływu na polepszenie jakości życia mieszkańców regionu oraz jakości i konkurencyjności ich pracy; potrafi zdobytą wiedzę, informacje i opinie sformułować i przekazać w sposób zrozumiały dla przeciętnego obywatela

6 TREŚCI PROGRAMOWE

WYKŁAD

LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
W1	Wstęp. Streszczenie 1. Co to jest bezpieczeństwo systemów informatycznych 2. Badania w zakresie bezpieczeństwa systemów informatycznych 3. Wybrane pojęcia 4. Dokumenty standaryzujące 5. Metody przeciwdziałania zagrożeniom i klasyfikacja metod ochrony Zadania Polityka bezpieczeństwa Streszczenie 1. Co to jest polityka bezpieczeństwa? 2. Zadania zespołu d/s bezpieczeństwa 3. Procedura tworzenia polityki bezpieczeństwa	1
W2	Testy penetracyjne - techniki skanowania Streszczenie 1. Idea testów penetracyjnych 2. Metody i techniki rekonesansu 3. Techniki skanowania Zadania	1
W3	Zdalne rozpoznawanie systemów operacyjnych i sniffing Streszczenie 1. Zdalna identyfikacja systemu operacyjnego 2. Zjawisko sniffingu 3. Techniki wykrywania sniferów Zadania	1
W4	Techniki enumeracji Streszczenie 1. Co to jest enumeracja? 2. Enumeracja Windows 3. Enumeracja systemu Linux Zadania	1
W5	Ataki - spoofing Streszczenie 1. Co to jest spoofing? 2. Spoofing ARP 3. Spoofing usługi routingu 4. Spoofing DNS 5. Porywanie sesji (hijacking) Zadania	1
W6	Ataki odmowy usługi (Denial of Service) Streszczenie 1. Wprowadzenie 2. Wykorzystanie fragmentacji pakietów 3. Ataki poprzez zalew pakietów 4. Rozproszone ataki DoS Zadania	1



WYKŁAD

LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
W7	Kryptograficzne metody ochrony informacji Streszczenie 1. Wstęp 2. Algorytmy z kluczem tajnym 3. Algorytmy z kluczem publicznym 4. Algorytmy skrótu 5. Podpis cyfrowy 6. Dystrybucja kluczy kryptograficznych 7. Infrastruktura klucza publicznego Zadania	2
W8	Systemy uwierzytelniania Streszczenie 1. Klasyfikacja metod uwierzytelniania 2. Słowniki haseł 3. Ochrona haseł 4. Systemy haseł jednorazowych 5. System Kerberos Zadania	1
W9	Kontrola dostępu Streszczenie 1. Macierz dostępu 2. Etykiety poziomów zaufania 3. Inne modele ochrony 4. Funkcjonowanie kontroli dostępu 5. Kanały ukryte	1
W10	Bezpieczne protokoły sieciowe Streszczenie 1. IPSec 2. L2TP i PPTP 3. SSL i TLS Zadania	2
W11	Zapory sieciowe Streszczenie 1. Co to jest firewall? 2. Filtrowanie pakietów 3. Translacja adresów 4. Usługi proxy 5. Etapy budowy zapory Zadania	1
W12	Wykrywanie intruzów Streszczenie 1. Koncepcja systemów wykrywania intruzów 2. Klasyfikacja IDS według źródeł informacji 3. Klasyfikacja IDS według metod analizy 4. Klasyfikacja IDS według typów odpowiedzi 5. Typowe symptomy działania intruzów 6. Pułapki internetowe Zadania	1
W13	Bezpieczeństwo poczty elektronicznej Streszczenie 1. Atrybuty bezpiecznego systemu pocztowego 2. Zagrożenia dla bezpieczeństwa systemu przekazywania poczty 3. Zagrożenia bezpieczeństwa na zewnątrz 4. Protokoły pocztowe a bezpieczeństwo 5. Rozwiązania zwiększające bezpieczeństwo systemu pocztowego Zadania	1
	RAZEM	15

PROJEKT

LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
P1	Testy penetracyjne - techniki skanowania Instalacja systemu Kali Linux 1. Metody i techniki rekonesansu 2. Techniki skanowania 2.1. Cele skanowania 2.2. Skanowanie ICMP 2.3. Skanowanie TCP 2.4. Skanowanie UDP 2.5. Inne techniki skanowania 2.6. Ukrywanie skanowania	4
P2	Zdalne rozpoznawanie systemów operacyjnych i sniffing 1. Zdalna identyfikacja systemu operacyjnego 2. Zjawisko sniffingu 3. Techniki wykrywania sniferów	2
P3	Techniki enumeracji 1. Co to jest enumeracja? 2. Enumeracja Windows 2.1. NetBIOS 2.2. SNMP 2.3. DNS 2.4. SID 2.5. Przechwytywanie etykiet 3. Enumeracja systemu Linux 3.1. Programy finger, rwho, rusers, w, nc 3.2. SMTP 3.3. SNMP 3.4. NFS 3.5. NIS 3.6. RPC 3.7. Przechwytywanie etykiet	4
P4	Ataki - spoofing 1. Spoofing ARP 2. Spoofing usługi routingu 3. Spoofing DNS 4. Porywanie sesji (hijacking)	2
P5	Ataki odmowy usługi (Denial of Service) 1. Wykorzystanie fragmentacji pakietów 2. Ataki poprzez zalew pakietów 3. Rozproszone ataki DoS	2
P6	Kryptograficzne metody ochrony informacji 1. Algorytmy z kluczem tajnym 2. Algorytmy z kluczem publicznym 3. Algorytmy skrótu 4. Podpis cyfrowy 5. Dystrybucja kluczy kryptograficznych	4
P7	Systemy uwierzytelniania 1. Klasyfikacja metod uwierzytelniania 2. Słowniki haseł 3. Ochrona haseł 4. Systemy haseł jednorazowych 5. System Kerberos	2
P8	Kontrola dostępu 1. Macierz dostępu 2. Etykiety poziomów zaufania 3. Funkcjonowanie kontroli dostępu 4. Kanały ukryte	2
P9	Bezpieczne protokoły sieciowe 1. IPSec 2. L2TP i PPTP 3. SSL i TLS	2
P10	Zapory sieciowe 1. Filtrowanie pakietów 2. Translacja adresów 3. Usługi proxy 4. Etapy budowy zapory	2



PROJEKT

LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
P11	Wykrywanie intruzów 1. Klasyfikacja IDS według źródeł informacji, według metod analizy, według typów odpowiedzi 2. Typowe symptomy działania intruzów 3. Pułapki internetowe	2
P12	Bezpieczeństwo poczty elektronicznej 1. Atrybuty bezpiecznego systemu pocztowego 2. Zagrożenia dla bezpieczeństwa systemu przekazywania poczty 3. Zagrożenia bezpieczeństwa na zewnątrz 4. Protokoły pocztowe a bezpieczeństwo 5. Rozwiązania zwiększające bezpieczeństwo systemu pocztowego	2
	RAZEM	30

7 METODY DYDAKTYCZNE

M1 Ćwiczenia projektowe

M2 Prezentacje multimedialne

M3 Symulacja laboratoryjna

M4 Wykłady

M5 Filmy edukacyjne

M6 Słowne objaśnienie

8 OBCIĄŻENIE PRACĄ STUDENTA

FORMA AKTYWNOŚCI	ŚREDNIA LICZBA GODZIN NA ZREALIZOWANIE AKTYWNOŚCI
Godziny kontaktowe z nauczycielem akademickim, w tym:	
Godziny wynikające z planu studiów	45
Konsultacje przedmiotowe	2
Egzaminy i zaliczenia w sesji	2
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	6
Opracowanie wyników	5
Przygotowanie raportu, projektu, prezentacji, dyskusji	15
SUMARYCZNA LICZBA GODZIN DLA PRZEDMIOTU WYNIKAJĄCA Z CAŁEGO NAKŁADU PRACY STUDENTA	75
SUMARYCZNA LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU	3

9 SPOSOBY OCENY

OCENA FORMUJĄCA

F1 Sprawozdanie z ćwiczenia laboratoryjnego

F2 Aktywność na zajęciach

F3 Kolokwium

**OCENA AKTYWNOŚCI BEZ UDZIAŁU NAUCZYCIELA AKADEMICKIEGO**

1 Ćwiczenie praktyczne

2 Projekt indywidualny

KRYTERIA OCENY

EFEKT KSZTAŁCENIA 1		MIEJSCE WERYFIKACJI	OPIS WERYFIKACJI EK 1
NA OCENĘ 3	Ma elementarną wiedzę dotyczącą projektowania i obsługi sieci informatycznych oraz tworzenia aplikacji internetowych, zna zagadnienia związane z bezpieczeństwem tych aplikacji oraz metody stosowane w ich projektowaniu i obsłudze sieci. Robi dużo błędów.	wykład, projekt	prezentacja sprawozdania
NA OCENĘ 4	Ma elementarną wiedzę dotyczącą projektowania i obsługi sieci informatycznych oraz tworzenia aplikacji internetowych, zna zagadnienia związane z bezpieczeństwem tych aplikacji oraz metody stosowane w ich projektowaniu i obsłudze sieci. Nie robi poważnych błędów.		
NA OCENĘ 5	Ma elementarną wiedzę dotyczącą projektowania i obsługi sieci informatycznych oraz tworzenia aplikacji internetowych, zna zagadnienia związane z bezpieczeństwem tych aplikacji oraz metody stosowane w ich projektowaniu i obsłudze sieci. Nie robi wcale błędów.		
EFEKT KSZTAŁCENIA 2		MIEJSCE WERYFIKACJI	OPIS WERYFIKACJI EK 2
NA OCENĘ 3	Posiada wiadomości dotyczące stanu obecnego rozwoju informatyki oraz kierunków jej rozwoju. Robi dużo błędów.	wykład	Aktywność na zajęciach. Kolokwium.
NA OCENĘ 4	Posiada wiadomości dotyczące stanu obecnego rozwoju informatyki oraz kierunków jej rozwoju. Nie robi poważnych błędów.		
NA OCENĘ 5	Posiada wiadomości dotyczące stanu obecnego rozwoju informatyki oraz kierunków jej rozwoju. Nie robi wcale błędów.		
EFEKT KSZTAŁCENIA 3		MIEJSCE WERYFIKACJI	OPIS WERYFIKACJI EK 3
NA OCENĘ 3	Potrafi ocenić przydatność i sposób funkcjonowania, istniejące rozwiązania elementów informatycznych, możliwość ich zastosowania dla konkretnego systemu lub sieci informatycznej. Robi dużo błędów.	projekt	prezentacja sprawozdania projektu.



NA OCENĘ 4	Potrafi ocenić przydatność i sposób funkcjonowania, istniejące rozwiązania elementów informatycznych, możliwość ich zastosowania dla konkretnego systemu lub sieci informatycznej. Nie robi poważnych błędów.		
NA OCENĘ 5	Potrafi ocenić przydatność i sposób funkcjonowania, istniejące rozwiązania elementów informatycznych, możliwość ich zastosowania dla konkretnego systemu lub sieci informatycznej. Nie robi wcale błędów.		
EFEKT KSZTAŁCENIA 4		MIEJSCE WERYFIKACJI	OPIS WERYFIKACJI EK 4
NA OCENĘ 3	Potrafi dokonać analizy krytycznej wyników funkcjonalnego i strukturalnego testowania systemu informatycznego. Robi dużo błędów.	wykład, projekt	prezentacja sprawozdania projektu. Aktywność na zajęciach. Kolokwium.
NA OCENĘ 4	Potrafi dokonać analizy krytycznej wyników funkcjonalnego i strukturalnego testowania systemu informatycznego. Nie robi poważnych błędów.		
NA OCENĘ 5	Potrafi dokonać analizy krytycznej wyników funkcjonalnego i strukturalnego testowania systemu informatycznego. Nie robi wcale błędów.		
EFEKT KSZTAŁCENIA 5		MIEJSCE WERYFIKACJI	OPIS WERYFIKACJI EK 5
NA OCENĘ 3	Potrafi zaprojektować sieć komputerową oraz tworzyć bezpieczne aplikacje internetowe i zabezpieczyć je przed typowymi atakami. Robi dużo błędów.	wykład, projekt	prezentacja sprawozdania projektu. Kolokwium.
NA OCENĘ 4	Potrafi zaprojektować sieć komputerową oraz tworzyć bezpieczne aplikacje internetowe i zabezpieczyć je przed typowymi atakami. Nie robi poważnych błędów.		
NA OCENĘ 5	Potrafi zaprojektować sieć komputerową oraz tworzyć bezpieczne aplikacje internetowe i zabezpieczyć je przed typowymi atakami. Nie robi wcale błędów.		
EFEKT KSZTAŁCENIA 6		MIEJSCE WERYFIKACJI	OPIS WERYFIKACJI EK 6
NA OCENĘ 3	Potrafi określić parametry, cechy pożądane elementów informatycznych i opracować etapy budowy prostego systemu informatycznego. Robi dużo błędów.	wykład, projekt	prezentacja sprawozdania projektu. Kolokwium.
NA OCENĘ 4	Potrafi określić parametry, cechy pożądane elementów informatycznych i opracować etapy budowy prostego systemu informatycznego. Nie robi poważnych błędów.		



NA OCENĘ 5	Potrafi określić parametry, cechy pożądane elementów informatycznych i opracować etapy budowy prostego systemu informatycznego. Nie robi wcale błędów.		
EFEKT KSZTAŁCENIA 7		MIEJSCE WERYFIKACJI	OPIS WERYFIKACJI EK 7
NA OCENĘ 3	Ma świadomość ważności zachowania w sposób profesjonalny, przestrzegania zasad etyki zawodowej, bezpieczeństwa i higieny pracy, ochrony własności intelektualnej oraz poszanowania różnorodności poglądów i kultur. Robi dużo błędów.	wykład, projekt	Aktywność na zajęciach. Prezentacja sprawozdania projektu. Kolokwium.
NA OCENĘ 4	Ma świadomość ważności zachowania w sposób profesjonalny, przestrzegania zasad etyki zawodowej, bezpieczeństwa i higieny pracy, ochrony własności intelektualnej oraz poszanowania różnorodności poglądów i kultur. Nie robi poważnych błędów.		
NA OCENĘ 5	Ma świadomość ważności zachowania w sposób profesjonalny, przestrzegania zasad etyki zawodowej, bezpieczeństwa i higieny pracy, ochrony własności intelektualnej oraz poszanowania różnorodności poglądów i kultur. Nie robi wcale błędów.		
EFEKT KSZTAŁCENIA 8		MIEJSCE WERYFIKACJI	OPIS WERYFIKACJI EK 8
NA OCENĘ 3	Potrafi określić parametry, cechy pożądane elementów informatycznych i opracować etapy budowy prostego systemu informatycznego. Robi dużo błędów.	wykład, projekt	Aktywność na zajęciach. Prezentacja sprawozdania projektu. Kolokwium.
NA OCENĘ 4	Potrafi określić parametry, cechy pożądane elementów informatycznych i opracować etapy budowy prostego systemu informatycznego. Nie robi poważnych błędów.		
NA OCENĘ 5	Potrafi określić parametry, cechy pożądane elementów informatycznych i opracować etapy budowy prostego systemu informatycznego. Nie robi wcale błędów.		

OCENA DO INDEKSU (OCENA PODSUMOWUJĄCA)

Ocena końcowa wystawiana jako średnia z oceny kolokwium teorii oraz ocen z projektów.

WARUNKI ZALICZENIA PRZEDMIOTU

- a Ocena kolokwium teorii.
- b Oceny z prezentacji sprawozdań projektów.



10 MACIERZ REALIZACJI PRZEDMIOTU

EFEKTY KSZTAŁCENIA DLA PRZEDMIOTU	ODNIESIENIE DO EFEKTÓW KIERUNKOWYCH	CELE PRZEDMIOTU	TREŚCI PROGRAMOWE	METODY DYDAKTYCZNE
EK1	INFP_W13, INFP_UB01, INFP_W08	Cel1	W1, W2, W3, P1, P2, P4, P9, P10	M1, M2, M3, M4, M5, M6
EK2	INFP_W13, INFP_UB04, INFP_UB01, INFP_W08	Cel1, Cel2	W2, W4, W5, W8, W9, P1, P2, P5, P6, P9, P11	M1, M2, M4, M6
EK3	INFP_UB04, INFP_UB07, INFP_UB09	Cel1, Cel2	W4, W5, W6, W9, W10, W13, P1, P3, P7, P9, P12	M1, M4, M5, M6
EK4	INFP_K07, INFP_UB07, INFP_W08	Cel1, Cel2	W6, W7, W8, W11, W12, P3, P5, P6, P7, P11	M1, M2, M4, M5, M6
EK5	INFP_K07, INFP_UB01, INFP_K05, INFP_W08	Cel1, Cel2	W3, W5, W8, W9, W10, W13, P1, P2, P10	M2, M4, M5
EK6	INFP_K07, INFP_UB07, INFP_W08, INFP_UB09	Cel1, Cel2	W4, W6, W7, W10, W12, P1, P3, P6, P7, P11, P12	M3, M4, M6
EK7	INFP_W13, INFP_K07, INFP_UB07, INFP_W08	Cel2	W4, W6, W8, W9, W10, W11, P2, P3, P8, P9, P10, P12	M2, M3, M5, M6
EK8	INFP_K07, INFP_K05, INFP_W08, INFP_UB09	Cel1, Cel2	W4, W6, W8, W10, W13, P3, P4, P6, P7, P9, P11, P12	M2, M3, M5

11 WYKAZ LITERATURY

LITERATURA PODSTAWOWA:

- [1] **Peter Kim** — *Podręcznik pentestera. Bezpieczeństwo systemów informatycznych.*, Warszawa, 2015, Helion
- [2] **Leszek Kępa, Paweł Tomasik, Sebastian Dobrzyński** — *Bezpieczeństwo Systemu E-commerce*, Gliwice, 2012, Helion
- [3] **Paco Hope, Ben Walther** — *Testowanie bezpieczeństwa aplikacji internetowych*, Gliwice, 2010, Helion
- [4] **Marek Serafin** — *Sieci VPN. Zdalna praca i bezpieczeństwo danych*, Gliwice, 2009, Helion
- [5] **D. R. Ahmad** — *Hack Proofing Your Network*, Rockland, 2001, Syngress Publ
- [6] **J. Scambray, S. Mc Clure, G. Kurtz** — *Hacking Exposed: Network Security Secrets & Solutions*, Osborne, 2000, McGraw-Hill
- [7] **M. Strebe, Ch. Perkins** — *Firewalls*, USA, 2000, Sybex Inc.



LITERATURA UZUPEŁNIAJĄCA:

- [1] M. Schiffman — *Hacker's Challenge*, Osborne, 2001, McGraw-Hill
- [2] Dhanjani N., Clarke J. — *Bezpieczeństwo sieci. Narzędzia*, Gliwice, 2008, Helion
- [3] Szmit M., Gusta M., Tomaszewski M. — *101 zabezpieczeń przed atakami w sieci komputerowej*, Gliwice, 2005, Helion
- [4] C. P. Pfleeger — *Security in Computing*, USA, 1997, Prentice Hall International
- [5] L. Klander — *Hacker Proof*, New York, 1997, Jamsa Press

12 INFORMACJE O NAUCZYCIELACH AKADEMICKICH

OSOBA ODPOWIEDZIALNA ZA KARTĘ

prof. dr hab. inż. Oleksandr Petrov (kontakt: asp1951@gmail.com)

OSOBY PROWADZĄCE PRZEDMIOT

prof. dr hab. inż. Oleksandr Petrov (kontakt: asp1951@gmail.com)

13 ZATWIERDZENIE KARTY PRZEDMIOTU DO REALIZACJI

(miejscowość, data)	(odpowiedzialny za przedmiot)	(kierownik zakładu)	(dyrektor instytutu)
---------------------	-------------------------------	---------------------	----------------------

PRZYJMUJĘ DO REALIZACJI (data i podpisy osób prowadzących przedmiot)

.....