Kolegium Jagiellońskie
Toruńska Szkoła Wyższa

SYLABUS PRZEDMIOTU	
Usytuowanie przedmiotu w programie studiów	
Nazwa przedmiotu	Bezpieczeństwo systemów komputerowych
Kierunek	MBA-*Master of Business Administration*
Profil kształcenia	praktyczny
Poziom kształcenia	studia podyplomowe
Rok studiów	I
Forma studiów	niestacjonarne
Forma realizacji zajęć	wykład/ ćwiczenia
Liczba godzin	Razem 10 godzin ,5h-wykład, 5h-
Liczba punktów ECTS	razem 3 ECTS
Status przedmiotu	kierunkowy
Forma zaliczenia	zaliczenie/ egzamin
Przewidywany termin egzaminu/ zaliczenia	marzec 2021 roku
Język wykładowy	polski
Prowadzący	mgr Arkadiusz Kozub
Doświadczenie praktyczne prowadzącego w zakresie przedmiotu	tak Wykształcenie kierunkowe, praca w charakterze wykładowcy oraz nauczyciela (15 lat), praca administratora sieci komputerowych (3 lata), certyfikat egzaminatora ECDL
E-mail prowadzącego	arkkoz13@wp.pl
Konsultacje	15 min. przed zajęciami i 15 min. po zajęciach

Cele przedmiotu

C1- student ma wiedzę na temat zagrożeń występujących w systemach oraz sieciach komputerowych, przeciwdziała nim wykorzystując administracyjne narzędzia systemowe
C2-student umie zabezpieczyć system oraz sieć komputerową przez nieuprawnioną inwigilacją
C3- wyposażenie absolwentów w umiejętności samodzielnego uzupełniania i doskonalenia wiedzy oraz wykorzystania zdobytej wiedzy do analizy i pracy w systemach oraz sieciach komputerowych

Wymagania wstępne (prerekwizyty)

Student powinien znać zasady nawigacji w systemach oraz sieciach komputerowych

Treści merytoryczne przedmiotu

Wykład oraz ćwiczenia

- **systemu komputerowego i sieci komputerowej.** Architektura harwardzka. Architektura von Neumanna. Pojęcie rozkazu. Wykonanie programu komputerowego. Cykl rozkazowy procesora. Podstawy systemów operacyjnych. Pojęcie procesu i jądra systemu operacyjnego. Systemy z podziałem czasu. Architektury sieci komputerowych. Sprzęt i oprogramowanie sieciowe. Model odniesienia OSI oraz TCP/IP. Komunikacja w sieci Internet. Adresowanie w sieci Internet.

- **Wstęp do bezpieczeństwa komputerowego.** Koncepcja bezpieczeństwa komputerowego. Podstawowe pojęcia. **Przestępczość komputerowa**. Przestępstwa ujawnione i nieujawnione. Obiekty, typy i sprawcy przestępstw komputerowych. Ataki bierne i czynne na systemy komputerowe. Atak Man In the Middle.
Inżynieria społeczna (socjotechnika). Phising oraz pharming. Oszustwo nigeryjskie. Inne metody ataków: terroryzm sieciowy, przestępstwa bankowe, przechwyt elektromagnetyczny, sabotaż komputerowy, szpiegostwo, piractwo komputerowe, wywiad gospodarczy. Inżynieria odwrotna.

- **Zagrożenia w systemach informatycznych.** Specyfika systemów informatycznych. Klasyfikacja zagrożeń. Przyczyny zagrożeń systemów informatycznych. Zagrożenia w sieci Internet. Zagrożenia związane z DNS. Skanowanie komputerów. Sieci botnet. Szkodliwe oprogramowanie – charakterystyka i rodzaje.
  Przeciwdziałanie szkodliwemu oprogramowaniu.

- **Klasyczne techniki szyfrowania.** Dziedzina kryptografii i podstawowe pojęcia. Podstawowe techniki szyfrowania: technika podstawieniowa, szyfr Cezara, szyfry mono i polialfabetyczne, szyfr Playfaira, szyfr Vigenère'a. Techniki przestawieniowe, szyfr zygzakowy, maszyny wirnikowe. Kryptoanaliza. Szyfrowanie symetryczne i asymetryczne. **Szyfry strumieniowe i blokowe.** Struktura Feistela. Standard DES. Struktura AES.

- **Podpis cyfrowy.** Idea podpisu cyfrowego. Wymagania stawiane podpisom cyfrowym. Mechanizm uwierzytelniania komunikatów. Kody uwierzytelnienia komunikatów MAC. Kryptograficzne funkcje haszujące. Algorytm SHA. Paradoks urodzin.

- **Uwierzytelnianie.** Pojęcie uwierzytelniania. Uwierzytelnianie za pomocą hasła. Strategie wyboru haseł. Inne metody uwierzytelniania. Protokoły uwierzytelniania: protokół challenge and response. Dowód z wiedzą zerową. Uwierzytelnianie dwuskładnikowe. Hasło jednorazowe. Generowanie haseł jednorazowych – protokół S/KEY.

- **Bezpieczeństwo sieci komputerowych.** Protokoły komunikacyjne. Struktura nagłówków protokołów TCP/IP. Ataki na warstwę sieci. Fałszowanie pakietów IP. Fragmentacja pakietów IP. Atak smerfów. Atak DDoS. Ataki na warstwę transportową. Atak SYN Flood. Skanowanie portów.

- **Zapory sieciowe (firewalle).** Model ogólny zapory sieciowej. Charakterystyka firewalli. Ograniczenia firewalli. Firewall filtrujący pakiety. Firewall filtrujący pakiety z badaniem stanu pakietu. Brama aplikacyjna, brama transmisyjna. Implementacja firewalla.

Metody dydaktyczne

Słowne: wykłady konwencjonalny, wykład problemowy, ćwiczenia praktyczne
Oglądowe: prezentacja multimedialna , aktywność w grupach
Praktyczne: dyskusja, analiza zagadnień z dyskusją, metoda problemowa, praca przy komputerze

Praktyczne czynności zawodowe wykonywane przez studentów podczas zajęć (dotyczy ćwiczeń)

Personalizacja zabezpieczeń systemów oraz sieci komputerowych.

Literatura

Podstawowa:

- J. Stokłosa, T. Bilski, T. Pankowski, *Bezpieczeństwo danych w systemach informatycznych*, PWN, 2001
- S. Garfinkel, G. Spafford, *Bezpieczeństwo w Unixie i Internecie*, Wydawnictwo RM, 1997
- W. R. Cheswick, *Firewalle i bezpieczeństwo w sieci*, Helion, 2003

Uzupełniająca:

- W. Stallings, *Ochrona danych w sieci i intersieciach. W teorii i praktyce*, WNT, 1997

EFEKTY KSZAŁCENIA W POWIĄZANIU Z EFEKTAMI KIERUNKOWYMI I SPECJALNOŚCIOWYMI

Nr efektu kształcenia	Opis efektu kształcenia	Odniesienie do kierunkowych i specjalnościowych efektów kształcenia
	Wiedza	
W1	Ma podstawową wiedzę z zakresu bezpieczeństwa systemów oraz sieci informatycznych	**K_W04**
W2	Zna techniki związane z atakami na systemy informatyczne i potrafi je opisać	**K_W07**
W3	Student zna w sposób pogłębiony właściwe dla dyscypliny naukowej ekonomia wybrane metody i narzędzia opisu rynków finansowych (kapitałowych).	**K_W03**

	Umiejętności	
U1	Potrafi sprawnie wyszukiwać w literaturze informacje związane z bezpieczeństwem systemów informatycznych, potrafi wyszukać informacje na temat nowych podatności wykrytych w systemach komputerowych	**K_U03**
U2	Student posiada umiejętność samodzielnego proponowania rozwiązań konkretnego problemu z zakresu systemów i sieci komputerowych	**K_U02**
U3	Student posiada umiejętność rozumienia i samodzielnego analizowania zjawisk i procesów informatycznych w skorelowaniu z obszarem ekonomicznym	**K_U03**
	Kompetencje społeczne	
K1	Rozumie potrzebę systematycznego aktualizowania swojej wiedzy na temat bezpieczeństwa systemów informatycznych oraz sieci komputerowych	**K_K01**
K2	Student potrafi odpowiednio określać priorytety i planować oraz organizować zadania związane z ich realizacją, a także monitorować i oceniać postępy, prawidłowo identyfikuje, diagnozuje i rozstrzyga dylematy oraz różne warianty rozwiązań problemu	**K_K02**

Metody i sposoby weryfikacji efektów kształcenia							
Efekt kształcenia	**Forma weryfikacji**						
	Egzamin pisemny	Praca w grupie	Prezentacja aktualnego problemu	Aktywny udział w zajęciach	Zaliczenie prezentacji multimedialnej	Selekcja i wybór źródeł	Praktyczne czynności zawodowe
W1	x		x	x	x		
W2	x	x	x	x	x		
W3	x	x	x	x	x		
U1	x	x		x			x
U2	x	x		x			x
U3	x	x	x	x	x		x
K1	x	x	x	x	x	x	x
K2	x	x	x	x	x		x

Formy i warunki zaliczenia przedmiotu
(F – ocena formująca, P – ocena podsumowująca)

F1- aktywny udział w zajęciach,
F2- przygotowanie i prezentacja podczas zajęć na forum grupy aktualnego problemu informatycznego i próba jego oceny,
F3- interpretacja i analiza środowiska pracy,
P1- przygotowanie prezentacji multimedialnej na wybrany temat z zakresu zabezpieczeń systemów i sieci komputerowych
P2 egzamin w formie pisemnej (pytania otwarte) - 8 pytań,
Kryteria oceny:
- odpowiedz na 4 pełne pytania – ocena 3,
- odpowiedz na 5 pełnych pytań. – ocena 3+
- odpowiedz na 6 pełnych pytań - ocena 4
- odpowiedz na 7 pełnych pytań - ocena 4+
- odpowiedz na 8 pełnych pytań - ocena 5

Oceny z egzaminu:
2 –student nie osiągnął wymaganych efektów kształcenia (poniżej 50 %),
3 – student osiągnął efekty kształcenia w stopniu dostatecznym (51 do 60 %),
3+ –student osiągnął efekty kształcenia w stopniu dostatecznym plus (61 do 70%),
4 –student osiągnął efekty kształcenia w stopniu dobrym (71 do 80 %),
4+ –student osiągnął efekty kształcenia w stopniu dobrym plus (81 do 90 %),
5 –student osiągnął efekty kształcenia w stopniu bardzo dobrym (91do 100%).

Kryteria oceny	Na ocenę dostateczną (minimalny poziom osiągnięcia efektów kształcenia)	Na ocenę bardzo dobrą (pełna realizacja efektów kształcenia)
	Wiedza - dysponuje podstawową i uporządkowaną wiedzą z zakresu systemów i sieci komputerowych - zna podstawową terminologię dotyczącą problematyki systemów i sieci komputerowych, - dysponuje podstawową i uporządkowaną wiedzą z zakresu funkcjonowania systemów informatycznych, **Umiejętności:** - umie wykorzystać podstawową wiedzę teoretyczną z praktycznym rozwiązaniu problemu w trakcie pracy przy komputerze, - potrafi zidentyfikować wybrane rodzaje ryzyk oraz problemów technicznych z zakresu obsługi systemów i sieci komputerowych, - umie wykorzystywać wiedzę do podejmowania nowych wyzwań, rozstrzygania dylematów pojawiających się	**Wiedza:** - wykazuje się wiedzą wykraczającą poza zakres właściwy dla dyscypliny naukowej informatyka w skorelowaniu z ekonomią, - zna zasady funkcjonowania systemów komputerowych i sieci informatycznych, -potrafi krytycznie ocenić zachodzące w nich zjawiska, -wykazuje się wiedzą wykraczającą poza zakres problemowy zajęć z zakresu uwarunkowań informatycznych związanych z efektywnym funkcjonowaniem w środowisku informatycznym, - ma poszerzoną wiedzę na temat regulacji prawnych z zakresu licencji systemów komputerowych **Umiejętności:**

	w pracy zawodowej, - potrafi prawidłowo interpretować zjawiska zachodzące w systemach i sieciach komputerowych, **Kompetencje społeczne:** - rozumie potrzebę uczenia się przez cale życie, - potrafi samodzielnie uzupełniać i doskonalić nabytą wiedzę i umiejętności z zakresu informatyki, jest otwarty na nowe pomysły i techniki, ma skłonność do nauki każdą metodą oraz skłonność do interakcji z innymi uczestnikami procesu uczenia się, - prawidłowo identyfikuje i rozstrzyga dylematy związane z pracą przy komputerze oraz sieci informatycznej, - posiada umiejętność rozumienia i samodzielnego analizowania zjawisk i procesów informatycznych w korelacji z obszarem gospodarczym.	- bezbłędnie identyfikuje wybrane rodzaje ryzyk oraz błędów związanych z funkcjonowaniem w środowisku systemów i sieci komputerowych, - potrafi ponad przeciętnie dokonywać obserwacji i analiz p odstawowych procesów informatycznych w korelacji w procesami gospodarczymi oraz ekonomicznymi, potrafi interpretować niezbędne w tym zakresie dane ilościowo – jakościowe, **Kompetencje społeczne:** - zna ograniczenia własnej wiedzy oraz umiejętności w zakresie obsługi systemów komputerowych oraz sieci informatycznych, - potrafi myśleć w sposób innowacyjny .

Punkty ECTS i ich rozkład z uwzględnieniem pracy studenta

Rodzaj pracy studenta	Obciążenie studenta
Udział w zajęciach określonych w planie studiów	1
Samodzielne przygotowanie do zajęć (zadania domowe – lektura przygotowująca do zajęć, praktyczne czynności zawodowe do wykonania w domu, inne)	1
~~Przygotowanie do egzaminu/zaliczenia i egzamin/zaliczenie~~	~~1~~
Łącznie punktów ECTS za przedmiot	**3**

Arkadiusz Kozub
podpis wykładowy