Załącznik nr 9
do Zarządzenia Rektora PŚk Nr 35/19
w brzmieniu ustalonym Zarządzeniem Nr 12/22

KARTA PRZEDMIOTU

Kod przedmiotu	studia stacjonarne:	E-I2C-2002-s1
	studia niestacjonarne:	E-1IZ2C-1003-s1
Nazwa przedmiotu	**Audyt Bezpieczeństwa**	
Nazwa przedmiotu w języku angielskim	**Security Audit**	
Obowiązuje od roku akademickiego	**2022/23**	

USYTUOWANIE PRZEDMIOTU W SYSTEMIE STUDIÓW

Kierunek studiów	**Informatyka**
Poziom kształcenia	**II stopień**
Profil studiów	**Ogólnoakademicki**
Forma i tryb prowadzenia studiów	**Studia stacjonarne i niestacjonarne**
Zakres	**Cyberbezpieczeństwo**
Jednostka prowadząca przedmiot	**Katedra Elektrotechniki Przemysłowej i Automatyki**
Koordynator przedmiotu	**Dr hab. inż. Sebastian Różowicz, prof. PŚk**
Zatwierdził	**Dziekan Wydziału Elektrotechniki, Automatyki i Informatyki** **dr hab. inż. Roman Deniziak, prof. PŚk**

OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

Przynależność do grupy/bloku przedmiotów		**Przedmiot specjalnościowy**
Status przedmiotu		**Obowiązkowy**
Język prowadzenia zajęć		**Polski**
Usytuowanie w planie studiów - semestr	studia stacjonarne	**Semestr I**
	studia niestacjonarne	**Semestr I**
Wymagania wstępne		**Podstawy programowania,** **Wstęp do informatyki**
Egzamin (TAK/NIE)		**NIE**
Liczba punktów ECTS		**4**

Forma prowadzenia zajęć		**wykład**	**ćwiczenia**	**laboratorium**	**projekt**	**inne**
Liczba godzin w semestrze	studia stacjonarne:	**30**		**15**	**15**	
	studia niestacjonarne:	**18**		**9**	**9**	

EFEKTY UCZENIA SIĘ

Kategoria	Symbol efektu	Efekty uczenia się	Odniesienie do efektów kierunkowych
Wiedza	W01	Student ma szczegółową i podbudowaną teoretycznie wiedzę w zakresie bezpieczeństwa informacji i bezpieczeństwa systemów informatycznych służącą do formułowania i rozwiązywania prostych zadań inżynierskich o charakterze praktycznym, typowych dla inżynierii bezpieczeństwa	INF2_W07
	W02	Student ma podstawową wiedzę o cyklu życia urządzeń, obiektów i systemów technicznych, typowych dla inżynierii bezpieczeństwa	INF2_W08
	W03	Student ma podstawową wiedzę niezbędną do rozumienia społecznych, ekonomicznych, prawnych i innych pozatechnicznych uwarunkowań działalności inżynierskiej Zna i rozumie zasady, metody oraz narzędzia pozwalające tworzyć oprogramowanie spełniające wymogi bezpieczeństwa.	INF2_W07
Umiejętności	U01	Student potrafi opracować dokumentację dotyczącą realizacji zadania inżynierskiego i przygotować tekst zawierający omówienie wyników realizacji tego zadania	INF2 _U01, INF2 _U03, INF2_U05, INF2_U06
	U02	Student potrafi, przy współpracy z innymi specjalistami, określić politykę bezpieczeństwa i zastosować rozwiązania informatyczne pozwalające ją zaimplementować. Ponadto potrafi, przy użyciu odpowiednich metod i narzędzi, monitorować, wykrywać, usuwać i zapobiegać zagrożeniom, a także zabezpieczać dowody ich wystąpienia na potrzeby dalszej analizy i czynności śledczych.	INF2 _U02, INF2 _U11
	U03	Student potrafi, stosując odpowiednie metody i narzędzia, tworzyć oprogramowanie spełniające wymagania bezpieczeństwa, a także zapewnić bezpieczeństwo procesu samego procesy wytwórczego.	INF2 _U09
Kompetencje społeczne	K01	Student potrafi wykorzystać wybrane metody, techniki i narzędzia do formułowania i rozwiązywania zadań inżynierskich dotyczących systemów informacyjnych w dziedzinie bezpieczeństwa i higieny pracy	INF2_K03, INF2_K04

TREŚCI PROGRAMOWE

Forma zajęć	Treści programowe
wykład	1. **Przechowywanie informacji, audyt bezpieczeństwa i regulacje prawne** (audyt bezpieczeństwa informacji umożliwia na łatwe zweryfikowanie sprawności działania norm i zabezpieczeń funkcjonujących w danej firmie. Wszystkie prace związane z niezależną oceną danej organizacji, zakończone są stworzeniem obszernego raportu, pozwalającego na sprawdzenie podatności na działania cyberprzestępców sieci IT oraz infrastruktury) 2. **Zabezpieczenia fizyczne**. (bezpieczne zarządzanie systemami i sieciami komputerowymi oraz kontrola dostępu do systemu). 3. **Audyt informacji i procesy biznesowe** (zagrożenia i podatności systemu informatycznego i wykrywanie włamań i reakcja na atak). 4. **Wykorzystanie narzędzi informatycznych do przeprowadzenia audytu systemów informatycznych oraz do wykrywania oszustw i nadużyć komputerowych** (bezpieczeństwo przeglądarek, stron www, poczty elektronicznej, DNS i bezpieczeństwo serwerów). 5. **Protokoły sieciowe i bezpieczeństwo sieci bezprzewodowych** (może składać się z kilku komponentów, zależnie od indywidualnych lub firmowych potrzeb zabezpieczeń. Dostęp do małych systemów – takich jak routery klasy SOHO (Small Office/Home Office) dla małych, a nawet wręcz domowych biur, czy osobiste sieci bezprzewodowe LAN - zwykle ograniczany jest za pomocą haseł). 6. **Audyt legalności oprogramowania** (ocena systemu znajdującego się w posiadaniu firmy, w jaki sposób został on nabyty oraz zaimplementowany na firmowych stacjach roboczych i serwerach). 7. **Procedury realizacji audytów wewnętrznych** (aspekty prawne w obszarze IT) 8. **Zagadnienia wymagane do egzaminu CISA**

laboratorium	W ramach laboratorium, studenci realizować będą zadania z zakresu: 1. Wprowadzenie do problematyki zarządzania bezpieczeństwem w sieci. 2. Charakterystyka zagrożeń. 3. Utrata danych oraz sposoby ich odzyskiwania. 4. Tworzenie baz danych oraz wytyczne ich ochrony. 5. Współpraca z instytucjami zewnętrznymi, administrowanie danych oraz ograniczanie dostępu do informacji. 6. Zarządzanie ryzykiem, analiza ryzyka systemu informatycznego. 7. Polityka bezpieczeństwa – określanie wymagań. 8. Ataki na system informatyczny.
projekt	W ramach projektu, studenci realizować będą zadania z zakresu planowania i realizacja audytu systemu bezpieczeństwa informacyjnego przedsiębiorstwa, zgodnie z międzynarodowymi standardami, oraz infrastruktury teleinformatycznej, techniki zarządzania usługami i projektami informatycznymi, szacowania ryzyka w oparciu o normy międzynarodowe, opracowywania procedur ochrony informacji, a także identyfikowania oraz szacowania ryzyk, towarzyszących wykorzystaniu techniki informacyjnej w przedsiębiorstwie. Prace będą wykonywane w zespołach liczących nie więcej niż trzy osoby.
inne	

METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ

Symbol efektu	Metody sprawdzania efektów uczenia się					
	Egzamin ustny	Egzamin pisemny	Kolokwium	Projekt	Sprawozdanie	Inne
W01			x			
W02			x			
W03			x			
U01				x		
U02				x	x	
U03					x	
K01				x	x	

FORMA I WARUNKI ZALICZENIA

Forma zajęć	Forma zaliczenia	Warunki zaliczenia
wykład	zaliczenie z oceną	Uzyskanie co najmniej 50% punktów z kolokwium
laboratorium	zaliczenie z oceną	Uzyskanie co najmniej 50% punktów z kolokwium
projekt	zaliczenie z oceną	Uzyskanie co najmniej 50% punktów z projektu wraz ze sprawoadaniem

NAKŁAD PRACY STUDENTA

Bilans punktów ECTS													
Lp.	Rodzaj aktywności	Obciążenie studenta										Jednostka
		studia stacjonarne					studia niestacjonarne					
1.	Udział w zajęciach zgodnie z planem studiów	W	C	L	P	S	W	C	L	P	S	h
		30		**15**	**15**		**18**		**9**	**9**		
2.	Inne (konsultacje, egzamin)	**2**		**2**	**2**		**2**		**2**	**2**		h
3.	**Razem przy bezpośrednim udziale nauczyciela akademickiego**	**66**					**42**					h

4.	**Liczba punktów ECTS, którą student uzyskuje przy bezpośrednim udziale nauczyciela akademickiego**	**2,64**	**1,68**	ECTS
5.	**Liczba godzin samodzielnej pracy studenta**	**34**	**58**	h
6.	**Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy**	**1,36**	**2,32**	ECTS
7.	**Nakład pracy związany z zajęciami o charakterze praktycznym**	**30**	**18**	h
8.	**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym**	**1,20**	**0,72**	ECTS
9.	**Sumaryczne obciążenie pracą studenta**	**100**	**100**	h
10.	**Punkty ECTS za moduł** *1 punkt ECTS=25 godzin obciążenia studenta*	**4**		ECTS

LITERATURA

1. Rozporządzenie Ministra Finansów w sprawie trybu sporządzania oraz wzoru sprawozdania z wykonania planu audytu za rok poprzedni (Dz. U. z 2008 r., Nr 61, poz. 378)
2. Rozporządzenie Ministra Finansów w sprawie szczegółowego sposobu i trybu przeprowadzania audytu wewnętrznego (Dz. U. z 2008 r., Nr 66, poz. 406)
3. Polaczek Tomasz, *Audyt bezpieczeństwa informacji w praktyce,* Gliwice 2006, Wyd. Helion, 2006.
4. Cole Eric, Krutz Roland L.,Conley James, *Bezpieczeństwo sieci,* Gliwice 2005, Wyd. Helion, 2005.
5. Fry Chris, Nystrom Martin, *Monitoring i bezpieczeństwo sieci,* Gliwice 2010, wyd. Helion, 2010.
6. McNab Chris, *Ocena bezpieczeństwa sieci,* Warszawa 2017, wyd. APN PROMISE SA, 2017.
7. Liderman Krzysztof, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Warszawa 2009, wyd. PWN, 2009.
8. Jonathan Reuvid, *E-biznes bez ryzyka. Zarządzanie bezpieczeństwem w sieci,* Gliwice, Wyd. Helion, 2007.
9. Rafał Krzemien, Kazimiera Winiarska, *Audyt wewnetrzny w pytaniach i odpowiedziach*, 2004 r.
10. Leszek Kępa, *Dane osobowe w firmie. Praktyczny poradnik przedsiębiorcy*, Warszawa, Difin, 2012.
11. Kevin Lam, David LeBlanc, Ben Smith, *Ocena bezpieczeństwa sieciowego*, Warszawa, Promise, 2005.
12. PN-ISO/IEC 27001:2007- Technika informatyczna- Techniki bezpieczeństwa- Systemy zarządzania bezpieczeństwem informacji- Wymagania.
13. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2002.101.926 ze zm.)