Nazwa zajęć: Bezpieczeństwo systemów informatycznych i kryptografia — Cyber security and cryptography					
Kierunek: Informatyka					***Obowiązuje od roku ak.*** 2019/2020
Poziom: I st. inżynierski		***Profil:*** praktyczny		***Grupa zajęć:*** Kierunkowe	
Semestr: VII	***Forma zaliczenia:*** E - egzamin	***Punkty ECTS:*** 4		***Zajęcia do wyboru:*** Nie	***Język zajęć:*** polski / angielski
Forma zajęć i liczba godzin na studiach stacjonarnych i niestacjonarnych:					
Wykład 30 / 16	***Ćwiczenia*** 30 / 16				***Suma godzin:*** 60 / 32
Specjalność:					
Nazwiska osób odpowiedzialnych za zajęcia: prof. dr hab. inż. Andrzej Giryn, mgr Bogusław Kowalski					

Opis zajęć:

Celem przedmiotu jest zapoznanie studentów z podstawami systemów bezpieczeństwa informacji (SBI) z punktu widzenia zarządzania ryzykami zagrożenia bezpieczeństwa informacji zawartych i przetwarzanych w systemach teleinformatycznych, zwłaszcza - w sieciach komputerowych. Student uzyskuje podstawową wiedzę z zakresu: - obowiązujących w obszarze bezpieczeństwa informacji podstawowych regulacji prawnych; - metod i narzędzi stosowanych w współczesnych SBI. Nabywa także umiejętności w zakresie wyszukiwania w literaturze informacji na temat metod i rozwiązań stosowanych w współczesnych SBI i kierunkach rozwoju tych systemów. W rezultacie uzyskuje podstawowe kompetencje niezbędne w procesach projektowania, wdrażania, testowania i eksploatacji SBI.□

Cele dydaktyczne:

Uzyskanie przez studenta umiejętności zastosowania metod i narzędzi SBI adekwatnych do utrzymania, na akceptowalnym poziomie, ryzyk zagrożenia bezpieczeństwa informacji w systemach IT.□

Uzyskanie przez studenta podstawowej wiedzy z zakresu:- podstawowych regulacji prawnych obowiązujących w obszarze bezpieczeństwa informacji ;- metod i narzędzi stosowanych w współczesnych SBI.□

Uzyskanie umiejętności w zakresie wyszukiwania w literaturze i źródłach elektronicznych informacji na temat metod i rozwiązań stosowanych w współczesnych SBI i kierunkach rozwoju tych systemów.□

Uzyskanie podstawowych kompetencji w procesach projektowania, wdrażania, testowania i eksploatacji SBI □

Metody dydaktyczne:		***Metody oceniania:***	
MP1	wykład informacyjny	MO1	praca pisemna
MP2	praca ze źródłem elektronicznym	MO2	egzamin pisemny
MC1	ćwiczenie praktyczne		
MS1	metoda sytuacyjna		

Wykład

W1	Bezpieczeństwo systemów informatycznych jako proces zarządzania ryzykiem zagrożenia dla bezpieczeństwa informacji zawartych i przetwarzanych w systemach teleinformatycznych - podstawowe aspekty merytoryczne i prawne.
W2	Rodzina norm ISO/IEC 27000
W3	Charaktrystyka "złośliwego oprogramowania" z uwzględnieniem metod jego dystrybucji (systemy: Pegasus; -Stuxnet)
W4	Zarys podstaw kryptografii - podstawowe pojęcia: wybrane: - szyfry symetryczne;- szyfry niesymetryczne;- podpisy cyfrowe;- funkcje skrótu;- uwierzytelnianie
W5	Protokoły kryptograficzne
W6	Sytemy SIEM (Security Information and Event Management)
W7	Problematyka bezpieczeństwa aplikacji internetowych
W8	Instalacja i konfiguracja bezpiecznego serwera WWW
W9	Ataki na aplikacje internetowe
W10	Uwierzytelnianie w serwisach WWW
W11	Przykład kompleksowego systemu bezpieczeństwa i charakterystyka jego istotnych elementów

Ćwiczenia

C1	Exercises in symmetric and asymmetric encryption
C2	Cryptographic protocols
C3	Exercises in Internet application security
C4	Installation and configuration of a secure web server
C5	Attacks on web applications
C6	Authentication in websites

Literatura podstawowa

1. Stallings W. Brown L., Bezpieczeństwo systemów informatycznych. Zasady i praktyka, Helion 2019;
2. Stallings W., Ochrona danych w sieci i intersieci; w teorii i praktyce, WN-T, Warszawa 1997 r.;

Literatura uzupełniająca

1. Kim D., Fundamentals of Information Systems Security, 3rd Edition, O'Reailly 2016
2. Stokłosa J., Bilski T., Pańkowski T., Bezpieczeństwo danych w systemach informatycznych, Wydawnictwo Naukowe PWN Warszawa-Poznań 2001;
3. Wawrzyniak D., Zarządzanie bezpieczeństwem systemów informatycznych w bankowości", Oficyna Wydawnicza „Zarządzanie i Finanse, Warszawa 2002
4. Metodologia TISM firmy European Network Security Institute (ENSI); http://www.ensi.net;
5. Kutyłowski M., Strothmann B., „Kryptografia; teoria i praktyka zabezpieczenia systemów komputerowych", Oficyna Wydawnicza Read Me, Warszawa 1999 r.;
6. Vademecum podpisu elektronicznego", Centrum Promocji Informatyki, Warszawa 2002;
7. Schneier B., Kryptografia dla praktyków – WNT, Warszawa 2002,
8. Laurie B, Laurie P., Apache. Przewodnik encyklopedyczny, HELION, Gliwice 2003.
9. Stallings W., Ochrona danych w sieci i intersieci; w teorii i praktyce, WN-T, Warszawa 1997 r.;

Źródła dodatkowe

1. https://pl.khanacademy.org/computing/computer-science/cryptography
2. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. nr. 133. poz. 883);
3. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. nr. 133. poz. 883);
4. Rodzina norm ISO/IEC 27000

Warunki zaliczenia

Co najmniej 60% porawnych odpowiedzi na egzaminie i wykonanie ćwiczeń.

Przykłady pytań zaliczeniowych

Scharakteryzuj „typowe" fazy ataku typu APT (Advanced Persistent Threats), np. - "Stuxnet"
Scharakteryzuj podstawowe różnice pomiędzy szyfrowaniem symetrycznym a niesymetrycznym

Scharakteryzuj podstawowe elementy kryptosystemu PKI.
Jakie są zasadnicze różnice pomiędzy: - "zwykłym" podpisem elektronicznym;- bezpiecznym (kwalifikowanym) podpisem elektronicznym;- profilem zaufanym.
Wymień tryby w jakich mogą pracować szyfrowe algorytmy blokowe (np. na przykładzie DES).
Wymień podstawowe typy protokółów kryptograficznych.
Czy w protokóle SSL serwer uwierzytelnia sie przed klientem, czy odwrotnie, a może obaj uwierzytelniają sie nawzajem.

Obciążenie pracą studenta

Studia stacjonarne/niestacjonarne

Forma pracy studenta	Wykład		Ćwiczenia				Suma	
Zajęcia z bezpośrednim udziałem nauczyciela	30 g	16 g	30 g	16 g			60 g	32 g
Zapoznanie się z literaturą przedmiotu	10 g	13 g					10 g	13 g
Przygotowanie się do zajęć	5 g	5 g					5 g	5 g
Przygotowanie się do kolokwiów								
Realizacja zadanych ćwiczeń i zadań			10 g	20 g			10 g	20 g
Przygotowanie sprawozdania z ćwiczeń								
Przygotowanie projektu / pracy								
Przygotowanie się i udział w egzaminie	15 g	30 g					15 g	30 g
	60 g	64 g	40 g	36 g			100 g	100 g

Efekty uczenia się	KEK	Treści kształcenia	Metody dydaktyczne	M. oceniania
posiadł umiejętności zastosowania metod i narzędzi SBI adekwatnych do utrzymania, na akceptowalnym poziomie, ryzyk zagrożenia bezpieczeństwa informacji.	K_W03	W1-W11	MP1	MO1,MO2
posiadł podtawową wiedzę z zakresu:- podstawowych regulacji prawnych;- metod i narzędzi stosowanych w współczesnych SBI	K_W04	W1-W11	MP1	MO1,MO2
has the ability to search the literature and electronic sources for information on the methods and solutions used in contemporary ISS and the directions of development of these systems.	K_U01	C1-C6	MC1, MS1	MO1,MO2
can participate in the processes of designing, implementing, testing and operating "simple" ISS's.	K_U06	C1-C6	MC1, MS1	MO1,MO2
is ready to think and act in an entrepreneurial way in the field of security of ISS.	K_K04	C1-C6	MC1, MS1	MO1,MO2