Popis předmětu

Pracoviště / Zkratka	KIT / IBIS			**Akademický rok**	2023/2024
Název	Bezpečnost informačních systémů			**Způsob zakončení**	Zkouška
Akreditováno/Kredity	Ano, 4 Kred.			**Forma zakončení**	Kombinovaná
Rozsah hodin	Přednáška 2 [HOD/TYD] Cvičení 2 [HOD/TYD]				
Obs/max	Statut A	Statut B	Statut C	**Zápočet před zkouškou**	ANO
Letní semestr	0 / -	0 / 0	0 / 0	**Počítán do průměru**	ANO
Zimní semestr	0 / -	0 / -	0 / -	**Min. (B+C) studentů**	nestanoveno
Rozvrh	Ano			**Opakovaný zápis**	NE
Vyučovací jazyk	Čeština			**Vyučovaný semestr**	Letní semestr
Volně zapisovatelný předmět	Ano			**Počet dnů praxe**	0
Hodnotící stupnice	A|B|C|D|E|F			**Hodn. stup. zp. před zk.**	S|N
Počet hodin kontaktní / **Automat. uzn. záp. před zk.**	Ne				
Periodicita	K				
Nahrazovaný předmět	Žádný				
Vyloučené předměty	Nejsou definovány				
Podmiňující předměty	Nejsou definovány				
Předměty informativně doporučené	Nejsou definovány				
Předměty,které předmět podmiňuje	Nejsou definovány				

Cíle předmětu (anotace):

Seznámit studenty s návrhem bezpečného informačního systému a systémem řízení bezpečnosti informací ve firmě.

Požadavky na studenta

Aktivní povinná účast na přednáškách a cvičeních, kde budou procvičovány a plněny zadané úkoly a požadavky.
Úspěšné dokončení všech zadaných úkolů.

Obsah

Informační systém, definice a druhy IS.
Základní pojmy bezpečnosti, hrozba, riziko, útok a zranitelné místo.
Analýza rizik.
Bezpečnostní opatření a bezpečnostní politika.
Kritéria pro hodnocení bezpečnosti informačních systémů TCSEC, CTCPEC, ITSEC a CC.
Metody monitorování systému, typy IDS.
Bezpečnostní funkce zvyšující bezpečnost IS.
Reakce na incidenty a forenzní analýza.
Audit/penetrační test.
Bezpečnost operačních systémů, databází a aplikací.
Význam čipových karet v oblasti bezpečnosti.
Počítačová kriminalita, hrozby ICT a bezpečnost.
Metody zabezpečení klientského počítače.
Bezpečnost informací při přenosu dat.
Cloud computing a bezpečnost informačních aktiv.
Kryptografické bezpečnostní mechanismy.
Symetrické a asymetrické šifrovací algoritmy.
Elektronický podpis, klíče a certifikace.
Systém řízení bezpečnosti informací (Information Security Management System - ISMS).

Certifikace - zavádění systému řízení bezpečnosti informací.
Přínosy zavedení a certifikace ISMS.
Využití norem ČSN BS7799-2:2004, ČSN ISO/IEC 17799:2005 a ČSN ISO/IEC 27001 při zavádění systému řízení bezpečnosti informací.
Zvýšení bezpečnosti informačního systému zavedením a udržováním subsystémů zvyšujících bezpečnost informací v organizaci.
Subsystém řízení aktiv, řízení rizik, bezpečnostní politiky, řízení informační bezpečnosti, personální bezpečnosti, fyzické bezpečnosti, řízení komunikace a provozu ICT.
Subsystém pravidel přístupu k systémům, bezpečnostních pravidel ve fázi pořízení, vývoje a údržby, řešení bezpečnostních incidentů a nedostatků, řízení správy kontinuity činnosti organizace a zajištění souladu se standardy a právními normami.
Legislativní rámec informační bezpečnosti v České republice.

Předpoklady - další informace k podmíněnosti studia předmětu

Základní znalost práce s PC (Windows 7, 8, 10 or Linux OS).
Notebook s OS Windows.

Získané způsobilosti

Studenti získají znalosti v oblasti bezpečnosti informačních systémů a řízení informační bezpečnosti.

Studijní opory

V případě mimořádných opatření bude výuka probíhat vzdáleně s využitím programu MS Teams v době dle rozvrhu. Účast na schůzkách skupiny v MS Teams je ekvivalentní účasti na přednáškách a cvičeních.

Garanti a vyučující

- **Garanti:** Ing. Martin Pozdílek, Ph.D.
- **Přednášející:** Ing. Martin Pozdílek, Ph.D. (100%)
- **Cvičící:** Ing. Martin Pozdílek, Ph.D. (100%)

Literatura

- **Základní:** HANÁČEK, P; STAUDEK, J. *Bezpečnost informačních systémů. Praha: Úřad pro státní informační systém, 2000. ISBN: 80-23854-00-3. S: 127.*.
- **Základní:** KOLOUCH, Jan. *CyberCrime. 1. vydání, Praha: CZ.NIC, z.s.p.o. , 2016. ISBN 978-80-88168-18-8. S: 528. Dostupný z WWW: http://www.nic.cz>.*.
- **Základní:** BUDIŠ, Petr. *Elektronický podpis a jeho aplikace v praxi. Praha: Nakladatelství ANAG, 2008. ISBN 978-80-7263-465-1. S:162.*.
- **Základní:** ČSN ISO/IEC 27001. *Informační technologie-Bezpečnostní techniky-Systémy managementu bezpečnosti informací - Požadavky. Praha: Český normalizační institut, 2006. 36s.*.
- **Doporučená:** PATTINSON, F. *Certifying Information Security Management Systems. CISSP, CSDP, Atsec information security corporation. Dostupný z WWW: http://www.atsec.com>.*.
- **Doporučená:** MACHÁČEK, Miloslav. *Cloud Computing and Security of Information Assets. Annual International Interdisciplinary Conference, AIIC 2014. University of the Azores, Ponta Delgada, 8-12 July 2014, Azores Islands, Portugal. p. 428. ISBN 978-608-4642-26-8.*.
- **Doporučená:** JOINT TASK FORCE TRANSFORMATION INITIATIVE. *Information security. Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology. Gaithersburg 2011, MD 20899-8930. March 2011. Dostupný z WWW: http://csrc.nist.gov>.*.

Vyučovací metody

Monologická (výklad, přednáška, instruktáž)
Dialogická (diskuze, rozhovor, brainstorming)
Metody samostatných akcí
Nácvik dovedností

Hodnotící metody

Písemná zkouška
Posouzení zadané práce
Rozhovor
Obhajoba vlastního projektu

Prezentace

Předmět je zařazen do studijních programů:

Studijní program	Typ stud.	Forma stud.	Obor	Etapa V.st.pl.	Rok	Blok	Statut	D.roč.	D.sem.
Informační technologie	Bakalářský	Prezenční	Informační technologie	1 2019	2023	Povinné 3. ročník	A	3	LS