CEMI
CENTRAL EUROPEAN MANAGEMENT INSTITUTE

Bezpečnost informací, dat a informačních systémů

Ing. Jiří Urbanec, Ph.D.

CO ZÍSKÁTE STUDIEM A ABSOLVOVÁNÍM TOHOTO PŘEDMĚTU

Studiem předmětu Bezpečnost informací, dat a informačních systémů se naučíte aplikovat postupy, které napomáhají správnému nastavení procesů kybernetické bezpečnosti v organizacích. Naučíte se chápat bezpečnost informací a IS jako součást běžné praxe, rozlišovat základní a podstatné pojmy a vazby mezi nimi, znát základní postupy při zajištění bezpečnosti v rámci projektové činnosti, při kooperaci v různých rolích (manažerských či konzultantských) v týmech zaměřených na bezpečnostní analýzu a audit informačních systémů.

Díky studiu tohoto předmětu dokážete vysvětlit základní pojmy v bezpečnosti informací a IS, vyjmenovat kritické charakteristiky a vysvětlit jejich význam, včetně konceptuálního modelu bezpečnosti informací, identifikovat základní zdroje rizik pro informace a data v ICT, formulovat cíle informační bezpečnosti a prostředky dosažení těchto cílů, vyjmenovat standardy a principy hodnocení bezpečnosti IS včetně penetračních testů. Absolvování předmětu napomáhá k rozvoji manažerského rozhodování, rozvoje schopnosti reagovat na měnící se bezpečnostní podmínky pro práci s daty a informacemi. Toto studium vám pomůže rozvinout schopnost reagovat na měnící se bezpečnostní podmínky po práci s daty a informacemi, a zvýší vaši konkurenceschopnost na pozicích IT manažera, projektového manažera nebo manažera bezpečnosti informačních systémů, případně v top managementu podniků a organizací.

Studiem tohoto předmětu dále získáte především možnost průběžně **konzultovat reálné problémy, případy a situace z vaší praxe** s lektorem – **expertem na danou problematiku**, a v rámci těchto konzultací pod jeho odborným vedením **zpracovat jejich řešení formou prakticky orientované případové studie** (seminární práce). Díky tomu, že konzultace neprobíhají skupinově, ale pouze přímo mezi vámi a lektorem, **můžete konzultovat i konkrétní firemní záležitosti**, včetně konkrétních dat atd., bez obav ze sdílení těchto údajů s dalšími studenty.

PŘÍKLADY OBLASTÍ A TÉMAT, V NICHŽ MŮŽETE S LEKTOREM/LEKTORKOU KONZULTOVAT

- Definice pojmů a základní principy: Data, informace, bezpečnost dat a informací, informační a kybernetická bezpečnost, ochrana, systém, požadavky na informace, vlastnosti informace, kritické charakteristiky informací a dat, kvalitativní charakteristiky informací, informační proces, riziko a nejistota, zdroje rizik, útočníci.
- Základní principy: Konceptuální modely bezpečnosti informace, metody reakce na riziko, modelové přístupy k řízení informační bezpečnosti v podniku.
- Metody zabezpečení podnikových IS a standardy řízení bezpečnosti IS: ISMS Information Security Management System, Cobit, ITIL, NIST, rodina standardů ISO 27000, bezpečnostní politika podniku a jeho bezpečnostní cíle, úvod do postupů zajištění bezpečnosti IT a principů hodnocení bezpečnosti IS, hrozby na Internetu, intranetu.
- Metody a principy pro realizaci bezpečnostních opatření: základní principy kryptografie, elektronického podpisu, čas. razítka, autentizace, autorizace, IDP, DLP, Public Key Infrastructure a elektronické certifikáty a jejich aplikace.
- Legislativní prostředí, zákony: přehled legislativního prostředí v České republice, jednotná identita občana, elektronický podpis.

ZPŮSOB ABSOLVOVÁNÍ PŘEDMĚTU

Předmět je zakončen zpracováním **seminární práce**, v níž student **řeší konkrétní téma ze své praxe**, týkající se daného předmětu, případně **některé z modelových témat připravených lektorem** (viz níže). Seminární práce je zpracovávána v rozsahu **7-10 stran formátu A4**, z toho se musí jednat alespoň o **8 normostran textu**. Seminární práce je lektorem ohodnocena procentuálně, přičemž **50 % a více** znamená **úspěšné absolvování daného předmětu**.

MODELOVÁ TÉMATA SEMINÁRNÍ PRÁCE

1. Identifikace rizik pro kritické charakteristiky bezpečnosti informací v IS v dané organizaci a stanovení jejich významu pro danou organizaci.
2. Identifikace základních zdrojů rizik pro informace a data v ICT v dané organizaci.
3. Formulace cílů informační bezpečnosti a prostředky dosažení těchto cílů ve vybrané organizaci.
4. Nastavení hodnocení bezpečnosti IS v dané organizaci.
5. Nastavení bezpečnostních testů v ICT.

STUDIJNÍ LITERATURA A DALŠÍ ZDROJE

Podpůrné studijní materiály zpracované lektorem (k dispozici online ve studijním systému)

Elektronické knihy z online knihovny Bookport od nakladatelství Grada:

Jan Kolouch a kol. *CyberSecurity,* Edice CZ.NIC, 8.01.2019 ISBN 978-80-88168-31-7(Online ZDE)

Smejkal Vladimír, Rais Karel, *Řízení rizik ve firmách a jiných organizacích,* 4., aktualizované a rozšířené vydání, Grada, ISBN 2013 978-80-247-4644-9 (Online ZDE)

Pour Jan, Gála Libor, Šedivá Zuzana, *Podniková informatika,* 2., přepracované a aktualizované vydání, Grada, 2009, ISBN 978-80-247-2615-1 (Online ZDE)

Vrana Ivan, Richta Karel, *Zásady a postupy zavádění podnikových informačních systémů, Praktická příručka pro podnikové manažery,* Grada 2004, ISBN 80-247-1103-6, (Online ZDE)

Basl Josef, Blažíček Roman, *Podnikové informační systémy, Podnik v informační společnosti - 3., aktualizované a doplněné vydání,* Grada, 2012, ISNB 978-80-247-4307-3 (Online ZDE)

Ostatní studijní literatura (Autoři: Název, Vydavatelství, Rok vydání, ISBN):
DOUCEK, P., NOVÁK, L., NEDOMOVÁ, L., SVATÁ, V. Řízení bezpečnosti informací. 2. vydání. Praha: Professional publishings, 2011. ISBN 978-80-7431-050-8.
SMEJKAL, V. Kybernetická kriminalita. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk s.r.o, 2015. ISBN 978-80-7380-501-2.
Jindřich Kodl Tomáš Sokol Vladimír Smejkal. Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti. Vydavatelství: Čeněk Aleš, 2019, ISBN: 978-80-7380-765-8
Sedlák, V., Vaník, P. Kybernetická (ne)bezpečnost. Problematika bezpečnosti v kyberprostoru. CERM, 2022, str. 440, ISBN: 9788076230682.
WHITMAN, M., MATTORD, H. Management of Information Security. USA: Course Technology, Cengag Learning, 2010. ISBN 0-8400-3160-2.
Ostatní užitečné zdroje (videomateriály, online profesní skupiny, blogy, diskuse atd.):