



C E M I

CENTRAL EUROPEAN MANAGEMENT INSTITUTE

Kybernetická bezpečnost v organizacích

Ing. Jiří Urbanec, Ph.D.

CO ZÍSKÁTE STUDIEM A ABSOLVOVÁNÍM TOHOTO PŘEDMĚTU

Studiem tohoto předmětu pochopíte principy vzniku bezpečnostních rizik pro data a informace v informačních technologiích, jejich ošetření a řízení. Naučíte se chápat principy bezpečnosti, pochopíte smysl bezpečnostních opatření v rozsáhlých informačních systémech v organizacích. Osvojíte si principy řešení nových postupů, které povedou k návrhu, instalaci, provozu a údržbě bezpečných informačních systémů. Absolvování předmětu napomáhá k rozvoji manažerského rozhodování, rozvoje schopnosti reagovat na měnící se bezpečnostní prostředí pro práci s daty a informacemi. Absolvent předmětu zvýší svou konkurenceschopnost v oblasti informatiky na pozicích IT manažer, projektový nebo delivery manažer, manažer 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.

Výstupem po absolvování tohoto předmětu je tedy cenný dokument dále použitelný ve vaší organizaci či zaměstnání, s vysokou přidanou hodnotou díky one-to-one konzultacím s odborníkem.

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

- Definice pojmů a základní principy: Data, informace, 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, identita, identifikace, autentizace, autorizace.
- Základní prvky zabezpečené organizace
- Základní součásti IS a jejich bezpečnostní vlastnosti.
- Principy zabezpečení dat při přenosu, při zpracování, při uložení.
- Fyzická bezpečnost.
- Principy auditování bezpečnosti IT

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 informačních rizik v dané organizaci a určit jejich váhu.
2. Navrhnout opatření a řízení informačních rizik v dané organizaci.



C E M I

CENTRAL EUROPEAN MANAGEMENT INSTITUTE

3. Návrh nastavení a údržby bezpečnostních prvků organizace a informačních systémů.
4. Nastavení personálního zabezpečení pro zabezpečení kyberbezpečnosti organizace
5. Nastavení auditu IT v organizaci.
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. <i>CyberSecurity</i> , Edice CZ.NIC, 8.01.2019 ISBN 978-80-88168-31-7(Online ZDE)
Smejkal Vladimír, Rais Karel, <i>Řízení rizik ve firmách a jiných organizacích</i> , 4., aktualizované a rozšířené vydání, Grada, ISBN 2013 978-80-247-4644-9 (Online ZDE)
Pour Jan, Gála Libor, Šedivá Zuzana, <i>Podniková informatika</i> , 2., přepracované a aktualizované vydání, Grada, 2009, ISBN 978-80-247-2615-1 (Online ZDE)
Vrana Ivan, Richta Karel, <i>Zásady a postupy zavádění podnikových informačních systémů, Praktická příručka pro podnikové manažery</i> , Grada 2004, ISBN 80-247-1103-6, (Online ZDE)
Basl Josef, Blažiček Roman, <i>Podnikové informační systémy, Podnik v informační společnosti - 3., aktualizované a doplněné vydání</i> , Grada, 2012, ISBN 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, Cengage Learning, 2010. ISBN 0-8400-3160-2.
Ostatní užitečné zdroje (videomateriály, online profesní skupiny, blogy, diskuse atd.):