

DESCRIPTION DU COURS

Université: Univerzita Komenského v Bratislave	
Faculté: Faculté de Management	
Identifiant du cours: FM.KIS/337B/18	Titre du cours: Cybercriminalité pour les managers
Activités éducatives: Type d'activités: séminaire Nombre d'heures: par semaine: 2 par niveau/semestre: 28 Forme du cours: présentielle	
Nombre de crédits: 3	
Semestre recommandé: 1., 3.	
Degré d'études: I., II.	
Conditions préalables:	
Conditions pour pouvoir suivre le cours: Examen - pour obtenir l'évaluation A, il faut obtenir au moins 91 points, pour obtenir l'évaluation A, il faut obtenir au moins 81 points, pour obtenir l'évaluation C il faut obtenir au moins 73 points, pour obtenir l'évaluation D il faut obtenir au moins 66 points et pour obtenir l'évaluation E, il faut obtenir au moins 60 points.	
Résultats attendus du cours: L'objectif du cours est de familiariser les étudiants avec des risques et des menaces liées à la cybercriminalité avec lesquels ils pourraient être confrontés directement ou indirectement dans leur futur travail de gestionnaire. Au cours des conférences on leur présentera les plus courants types d'attaques informatiques sur les infrastructures informatiques et de réseau avec les techniques et les outils utilisés, ainsi que les implications juridiques pour chaque domaine pertinent. En même temps, ils leur seront présentés des mesures appropriées et des mécanismes de sécurité pertinents pour augmenter le pourcentage de protection contre les différents types de cybercriminalité. Les étudiants, dans le cadre de ce cours, doivent préparer la présentation des nouveautés et des spécificités intéressantes proposées par eux-mêmes sur chaque sujet des conférences et doivent les présenter à l'auditoire de leurs collègues. Cela stimule leur capacité de présenter leur propre rhétorique et leur savoir-faire dans le domaine de la présentation devant un large public, qui sont demandés comme une obligation et nécessité lorsqu'on travaille au poste d'un manager. Pendant les séminaires, seront discutés des cas des attaques concrets dans les domaines présentés pendant les conférences et les étudiants sont encouragés de suggérer des mesures de protection ou des conceptions d'outils matériels et logiciels par l'intermédiaire desquels on pourrait éviter au moins partiellement les attaques identiques ou similaires. Pendant les exercices sont aussi discutés les symptômes de diverses attaques, pour que les futurs managers seront capables de reconnaître dans la pratique les menaces potentielles pendant l'utilisation des systèmes d'information et de communication.	
Programme du cours: • Malware – virus informatiques, vers, chevaux de Troie, keylogger, spyware, adware, • Spamming, • Hacking, • Phishing,	

- Pharming,
- Cracking,
- Ingénierie sociale,
- Warezing,
- Sniffing,
- Spoofing,
- Phreaking,

et la présentation des autres types de cybercriminalité avec les exemples pratiques.

Littérature recommandée:

1. E. Kostrecová, M. Jókay, M. Kostrec: Počítačová kriminalita. Vysokoškolské skriptum. Slovenská technická univerzita v Bratislave, 2010, 128 s., ISBN: 978-80-227-3410-3
2. V. Jirovský: Kybernetická kriminalita - nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Grada Publishing, a. s., Praha, 2007, 288 s., ISBN: 978-80-247-1561-2.
3. M. Matějka: Počítačová kriminalita. Computer Press Praha, 2002, 120 s., ISBN: 80-7226-419-2.
4. A. Bowker: THE CYBERCRIME HANDBOOK FOR COMMUNITY CORRECTIONS: Managing Offender Risk in the 21st Century, Charles C. Thomas publisher LTD, Springfield, USA, 2012, 276 s., ISBN: 978-0-398-08729-6
5. M. Quémener, J.-P. Pinte: Cybersécurité des acteurs économiques : Risques, réponses stratégiques et juridiques. Hermes Science Publications, coll. « Cyberconflits et cybercriminalité », Middlesex, 2012, 274 p., ISBN: 978-2746239159

Langues nécessaires pour terminer le cours:

langue française

Remarques:

Evaluation du cours

Nombre total d'étudiants évalués: 17

A	ABS	B	C	D	E	FX	M
100,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0

Chargé(e) de cours: RNDr. Eva Kostrecová, PhD.

Dernier changement: 02.05.2025

Approuvé par: prof. Mgr. Anna Lašáková, PhD., prof. JUDr. Daniela Nováčková, PhD., prof. Ing. Ján Papula, PhD.