

CZ.1.07/2.2.00/28.0138

Modularizace manažerského a psychologického vzdělávání na Univerzitě Palackého v Olomouci cestou inovace a propojení ekonomických a psychologických studijních programů

| <b>Charakteristika studijního předmětu dle nařízení vedení FF UP</b>  |   |                      |          |                                    |                           |
|---|---|----------------------|----------|------------------------------------|---------------------------|
| <b>Název studijního předmětu</b>  | <i>Management - bezpečnost a rizika</i> |                      |          |                                    |                           |
| <b>Typ předmětu</b>   | <i>povinný</i>                          |                      |          | <b>doporučený ročník / semestr</b> | <i>2./Z</i>               |
| <b>Rozsah studijního předmětu (kolik hodin přednášek, seminářů, cvičení)</b>  | <i>1+1+0</i>                            | <b>hod. za týden</b> | <i>2</i> | <b>kreditů</b>                     | <i>4</i>                  |
| <b>Jiný způsob vyjádření rozsahu</b>  |   |                      |          |                                    |                           |
| <b>Způsob zakončení</b>   | <i>Zkouška</i>                          |                      |          | <b>Forma výuky</b>                 | <i>přednášky/ seminář</i> |
| <b>Cíle předmětu (česky/anglicky)</b>   |   |                      |          |                                    |                           |
| <p>Cílem předmětu je analýza stavu informační bezpečnosti v českých firmách. Pochopení a aplikace bezpečnosti a rizik v oblastech fyzické, organizační, personální, softwarové, hardwarové, informačních systémech a komunikačních cest a dále bezpečnost z hlediska práva. Studenti si vyzkoušejí praktickou ukázkou analýzy rizik a získají přehled v oblastech jako je digitální podpis, zálohování, plány obnovy, plány kontinuity atd.</p> <p>Target of subject is obtaining background knowledge and basic concepts in the area security management and risk analysis. Students will be able to do risk analysis in area physical, organization, personal, software, hardware, information systems and communication network. There will be practical cases from risk analysis. Student is able to describe area like electronic signature, backup, plan renewal, plan continuity, law etc.</p> |   |                      |          |                                    |                           |
| <b>Předpoklady (např. splnění jiného předmětu) (česky/anglicky)</b>   |   |                      |          |                                    |                           |
| Je doporučeno absolvování kurzů KAE/ Management<br>KAE/Management completion is recommended.  |   |                      |          |                                    |                           |
| <b>Obsah (česky/anglicky)</b>   |   |                      |          |                                    |                           |
| <ol style="list-style-type: none"> <li>1. Úvod do problematiky, základní pojmy</li> <li>2. Aktuální stav bezpečnosti v českých firmách.</li> <li>3. Příčiny a důvody úniků, ztrát.</li> <li>4. Budování systému managementu bezpečnosti</li> <li>5. Fyzická (technická) bezpečnost.</li> <li>6. Režimová ochrana, personální ochrana.</li> <li>7. HW ochrana, SW ochrana.</li> <li>8. Bezpečnost počítačových sítí. Kryptografie. Kryptografické algoritmy. Symetrická a nesymetrická kryptografie. Elektronický podpis.</li> <li>9. Bezpečnostní prvky v počítačových sítích: bezpečnostní brány, bezpečnostní protokoly,</li> <li>10. Bezpečnost systému: zálohování, ochrana zdrojů, kontrola integrity, monitorování, antivirová ochrana.</li> </ol>  |   |                      |          |                                    |                           |

CZ.1.07/2.2.00/28.0138

Modularizace manažerského a psychologického vzdělávání na Univerzitě Palackého v Olomouci cestou inovace a propojení ekonomických a psychologických studijních programů

11. Postup při napadení: odhalení průniku, úklid po útočnickovi, obnovení provozu, opatření proti opakování.

12. Systém managementu bezpečnost informací z pohledu práva, legislativní normy.

Tento předmět je inovován o zařazení nejnovějších poznatků z aktuálního průzkumu stavu informační bezpečnosti. Tyto poznatky vychází z průzkumu, který provádí renomované společnosti jako PricewaterhouseCoopers, Národní bezpečnostní úřad a časopis DSM - data security management. Předmět je inovován o případové studie, jejichž rozbor vytvoří významnou součást vzdělávacího procesu.

Inovace předmětu vznikla v rámci projektu CZ.1.07/2.2.00/28.0138 „Modularizace manažerského a psychologického vzdělávání na Univerzitě Palackého v Olomouci cestou inovace a propojení ekonomických a psychologických studijních programů“.

1. Introduction into problems, basic terms.

2. Current situation of information security in Czech Republic.

3. Reason and motive escape and loss.

4. Implementation information security management system.

5. Physical (technical) security.

6. Regime protection, personal protection.

7. HW protection, SW protection.

8. Security of network. Encryption. Encryption algorithm. Symmetrical and asymmetrical encryption. Electronic signature.

9. Security elements in network: security gates, security protocols.

10. Security system: back up, protection source, check integrity, monitoring, antivirus protection.

11. Process during attack: unveiling penetration, renew system.

12. Information security management system and law, legislative norm.

This subject is innovated by the latest knowledge in the field of current research situation information security. These findings are taken from recent studies published by recognized firms such as PricewaterhouseCoopers, NBU - National Security Authority and journal DSM - Data Security Management. Subject is innovated about the case studies used in the course are consistently upgraded and are used for analyses. The analyses and discussions are an important part of the educational process.

The innovation of the subject was established within a project CZ.1.07/2.2.00/28.0138 "Modularization of Managerial and Psychological Education at Palacky University in Olomouc through Innovating and Linking Economic and Psychological Study Programs."

**Požadavky (podmínky splnění kurzu) (česky - podrobně/anglicky - stručně)**

*Docházka (2 absence povoleny)*

*Samostatné zpracování vybraného tématu včetně prezentace.*

*Účast na modelových situacích během seminářů.*

CZ.1.07/2.2.00/28.0138

Modularizace manažerského a psychologického vzdělávání na Univerzitě Palackého v Olomouci cestou inovace a propojení ekonomických a psychologických studijních programů

*Attendance (2 absences allowed)*

*Elaboration of a case study and its defence in the lessons.*

*Participation in model situations during seminars.*

### **Literatura (Základní, Rozšiřující, Doporučená)**

#### **Základní:**

Český normalizační institut 2006. " ČSN ISO/IEC 27001 - Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky.

LÁTAL, I., ŠTANTEJSKÝ, M. *Bezpečnostní zásady ochrany podniku (Prevence a řešení krizových situací)*. Praha: Prospektrum, 2001. 119 str. ISBN 80-7175-091-3.

STEINER, F.; TUPA, J. *Management rizik v systémech řízení bezpečnosti informací*. In MOPP 2007. V Plzni: Západočeská univerzita, 2007. s. 183. ISBN 978-80-7043-535-9..

#### **Rozšiřující:**

ŠEBESTA, V.; ŠTVERKA, V.; ŠEBESTOVÁ, M.; SEDLÁČEK, M. *Systémy řízení bezpečnosti informací, Část 3: Směrnice pro management rizik bezpečnosti informací podle BS 7799-3:2005 s komentářem k managementu rizik v ISMS*. Praha: Český normalizační institut. Praha: 2007. 50 str..

ŠEBESTA, V., ŠTVERKA, V., STEINER, F., ŠEBESTOVÁ, M. *Praktické zkušenosti z implementace systému managementu bezpečnosti informací podle ČSN BS 7799-2:2004 a komentované vydání ISO/IEC 27001:2005*, Český normalizační institut. Praha: 2006. 50str. ISBN 80-7283-204-2.

#### **Doporučená:**

PSIB ČR 09Ernst & Young, NBÚ, DSM - data security management, ISBN 978-80-86813-19-6.

### **Časová náročnost jednotlivých aktivit**

Položky:

Účast na výuce: 28 h

Domácí příprava na výuku: 22 h

Semestrální práce 25 h (*zpracování vybraného téma včetně prezentace*)

Samostudiu: 25 h

### **Získané způsobilosti (česky/anglicky)**

- *Definuje disciplínu bezpečnostní management.*
- *Popíše aktuální stav bezpečnosti informací v ČR.*
- *Vysvětlí hlavní části, ze kterých se skládá bezpečnost v podnicích.*
- *Definuje pojmy bezpečnostní incident, rizika, klasifikace informací.*
- *Provádí analýzu rizik v podniku.*
- *Předvídá příčiny lidského selhání.*
- *Definuje a analyzuje rizika.*
  
- *Student is able to define discipline security management.*
- *Student is able to describe current situation information security in Czech Republic.*



evropský  
sociální  
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,  
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání  
pro konkurenceschopnost



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

CZ.1.07/2.2.00/28.0138

Modularizace manažerského a psychologického vzdělávání na Univerzitě Palackého v Olomouci cestou inovace a propojení ekonomických a psychologických studijních programů

- *Student is able to explain main parts of security management*
- *Student is able to define term as information security incident, risk, classification of information*
- *Student is able to do risk analysis*
- *Student is able to anticipate reason of people failure*

#### **Vyučovací metody**

*Přednášení*

*Prezentace*

*Demonstrace*

#### **Hodnotící metody**

*Absolvování testu bezpečnosti a rizik v podniku*

*Znalostní test problematiky*

*Zpracování a prezentace vybraných témat předmětu*

*Analýza výkonů studenta*

*Systematické pozorování studenta*