# ZOI - ZS 2011/12 – osnova požadavků ke zkoušce

1/ Význam el. informací pro obchodní společnost, důvody ochrany el. informací.

2/ Pojem zabezpečení el. informací (zajištění důvěrnosti, integrity, dostupnosti) – vysvětlení pojmů. Základní pojmy z oblasti zabezpečení informačního systému (informační technologie, data, informace, uživatel, správce).

3/ Postup realizace zabezpečení informací obchodní společnosti; oblasti realizace bezpečnostních opatření.

4/ Analýza rizik – základní pojmy (aktivum, hrozba, riziko, zranitelnost, míra rizika), možné přístupy provedení analýzy rizik, postup realizace analýzy rizik. Metoda CRAMM, IPAK a FRAP.

5/ Bezpečnostní politika IS, systémové bezpečnostní politiky, bezpečnostní dokumentace.

6/ Klasifikace informací, vlastníci informací.

7/ Organizace řízení bezpečnosti.

8/ Úvod do kryptografie, šifrování x kódování, systémy s proudovým a blokovým šifrováním, symetrická šifra, asymetrická šifra, základní pojmy.

9/ Historie vývoje šifer.

10/ Jednorázová (Vernamova) šifra.

11/ Metoda DES, Triple DES.

12/ Metoda RSA.

13/ Užití symetrických a asymetrických šifrových systémů.

13/ Jednosměrná funkce, hašovací funkce, využití hašovacích funkcí, funkce MD5, SHA.

15/ Digitální podpis – princip, význam.

16/ Certifikát veřejného klíče, povinné a volitelné položky certifikátu a CRL dle normy X.509.

17/ Certifikační autorita – základní poslání, činnosti CA, registrační autorita.

18/ Elektronický podpis, zaručený elektronický podpis, akreditovaný poskytovatel certifikačních služeb. Vztah mezi digitálním podpisem a elektronickým podpisem.



19/ Legislativa ve vztahu k zabezpečení el. informací (obchodní tajemství, zákon o ochraně osobních údajů, zákon o utajovaných skutečnostech, zákon o elektronickém podpisu, směrnice 1999/93/ES, směrnice 2001/115/ES).

20/ Monitorování aktivit uživatelů informačního systému, audit informačního systému, penetrační testy.

doc. RNDr. Jaroslav Mlýnek, CSc.

V Liberci dne 21. 12. 2011