NEMZETI KÖZSZOLGÁLATI EGYETEM
Államtudományi és Nemzetközi Tanulmányok Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** ÁKINTM09
2. **A tantárgy megnevezése (magyarul):** Kockázatértékelés, kockázatmenedzsment
3. **A tantárgy megnevezése (angolul):** Risk assessment and risk management
4. **Kreditérték és képzési karakter:**
   - **4.1.** 5 kredit
   - **4.2.** a tantárgy elméleti vagy gyakorlati jellegének mértéke: 100% gyakorlat, 0% elmélet
5. **A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):** kiberbiztonsági MA
6. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** Államtudományi és Nemzetközi Tanulmányok Kar, Közszervezési és Infotechnológiai Tanszék
7. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Krasznay Csaba, PhD, egyetemi docens
8. **A tanórák száma és típusa**
   - **8.1.** össz óraszám/félév:
   - 8.1.1. nappali munkarend: 42 (0 EA + 42 GY)
   - 8.1.2. levelező munkarend: 12 (0 EA + 12 GY)
   - **8.2.** heti óraszám - nappali munkarend: 3 (0 EA + 3 GY)
   - **8.3.** Az ismeret átadásában alkalmazandó további sajátos módok, jellemzők: -
9. **A tantárgy szakmai tartalma (magyarul):** A tantárgy célja az információbiztonsági kockázatelemzés és kockázatkezelés bemutatása. Ennek kapcsán a hallgató megismeri a szabványokban használatos fogalmi eszköztárat, részletesen az ISO 31000 és 27005 szabványt, azaz általános és információbiztonsági kockázatkezelési szabványokat. Elsajátítja a kockázatbecslés kvantitatív, kvalitatív és szemikvantitatív megoldásait. Áttekintésre kerülnek a kockázatértékelési opciók és algoritmusok. Az előadás bemutatja az olyan kockázatkezelési keretrendszereket, mint a COBIT5 - RiskIT, ITILv3, Octave, ISO 73, ISO/IEC 31000, ISO 13335, NIST 800-53, illetve részletesen elemzésre kerül a 2013. évi L. tv. és a CISM alapú kockázatmenedzsment is. A gyakorlat során kockázatértékelési esettanulmányok kerülnek kidolgozásra, kockázati forgatókönyveket állítanak össze a hallgatók, valamint kockázatkezelési terveket készítenek el, beleértve ebbe a vagyonleltárakat és a sebezhetőség vizsgálatokat is.

   A tantárgy szakmai tartalma (angolul) (Course description): The goal of the course is to introduce information security risk analysis and risk management. In this context, the student will become familiar with the conceptual toolkit used in the standards, in particular ISO 31000 and 27005, which are general and information security risk management standards. Students will acquire quantitative, qualitative and semi-quantitative solutions to risk assessment. The risk assessment options and algorithms are reviewed. The lecture introduces risk management frameworks such as COBIT5 - RiskIT, ITILv3, Octave, ISO 73, ISO / IEC 31000, ISO 13335, NIST 800-53 and detailed analysis of the Act L of 2013 and CISM-based risk management. As practice, risk assessment case studies are developed, students prepare risk scenarios and prepare risk management plans, including asset inventories and vulnerability analysis.

10. **Elérendő kompetenciák (magyarul):**
    Tudása: Ismeri azokat a fontosabb előírásokat a szabályozásokból, melyek a mindennapi munkáját befolyásolják. Átlátja a munkáltatók által meghatározott belső szabályzatok megalkotásának szükségességét az információs rendszerekben tárolt adatok sértetlensége és a rendelkezésre állás

tekintetében. Megérti a szervezeti feladatokat a kibervédelemben. Ismeri azokat a fontosabb előírásokat a szabályozásokból, melyek meghatározzák a szervezeti kockázatkezelés követelményeit. Átlátja azon kockázatokat, melyek az információs rendszerekben tárolt adatok bizalmassága, sértetlensége és a rendelkezésre állás tekintetében előfordulhatnak. Átlátja, hogy milyen kockázatkezelési megoldások léteznek.

Képességei: Képes értelmezni a jogszabályokból eredő követelményeket. Képes felmérni a belső munkavállalók jelentette kiberbiztonsági kockázatokat. Képes olyan szabályzatok alkotására, amelyek a belső munkavállalók jelentette fenyegetések kezelésére vonatkoznak. Képes felmérni a szervezet adatvagyonát, ezekre fenyegetéseket, sebezhetőségeket meghatározni. Képes az egyes sebezhetőségek kockázatait több módszerrel is felmérni. Képes olyan védelmi intézkedések meghozatalára, melyek segítik a kockázatok csökkentését. Képes olyan szabályzatok alkotására, melyek biztosítják a szervezet kockázat alapú információbiztonsági folyamatának működtetését.

Attitűdje: Munkája során figyelembe veszi és alkalmazza a kiberbiztonsággal kapcsolatos jogszabályokat. Hatékony lépéseket tesz a kibertámadások megelőzése érdekében, így csökkentve a szervezete kitettségét. Szükség esetén támogatja a külső feleket a szervezeténél keletkezett információk megosztásával.

Autonómiája és felelőssége: Önállóan dolgozza fel az új és összetett információkat, problémákat, illetve jelenségeket rendszerszerű és kritikus módon. Felelősséget vállal a kiberbiztonság összefüggő ismeretének és a meghatározó jogi, szabályozási és gazdasági összefüggések ismeretének alapján a szakmai javaslatok kidolgozásában. Vállalja a kiberbiztonsági fenyegetések kezelésének felelősségét.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: He/she is familiar with specifications of regulations that have an immediate impact on his/her daily work. He/she is familiar with the need for introducing internal regulations defined by employers in order to maintain integrity and availability of the data stored in information systems. He/she is familiar with organisational tasks in cyber security. He/she is familiar with the key requirements of the regulations that determine the requirements of organizational risk management. He/she is familiar with the risks that can arise in terms of confidentiality, integrity and availability of data stored in information systems. He/she is familiar with existing risk management solutions.

Capabilities: He/she is capable of interpreting legal requirements. He/she is capable of assessing cyber security risk posed by internal employees. He/she is capable of creating regulations to handle threats posed by internal employees. He/she is capable of assessing the organization's data assets, identify threats, vulnerabilities. He/she is capable of assessing the risks of each vulnerability on multiple ways. He/she is capable of taking protective measures that help reduce risks. He/she is capable of establishing policies that ensure the operation of an organization's risk-based information security process.

Attitude: His/Her personal attitude is characterized by an attention to and application of laws of cyber security in his/her work. His/Her personal attitude is characterized by an effort to design the cyber security management system in its own complexity. His/Her personal attitude is characterized by an effort to take effective measures in order to prevent cyber attacks, by this means reducing the exposure of his/her organisation. His/Her personal attitude is characterized by an ability to treat internal employees as high risk and plans information security processes accordingly.

Autonomy and responsibility: Autonomy and responsibility is to process new and complex information, problems and phenomena in a systematic and critical way. Autonomy and responsibility to take responsibility for making professional proposals based on comprehensive knowledge of cyber security and dominant legal, regulatory and economical processes. Autonomy and responsibility is to handle cyber security threats.

11. Előtanulmányi követelmények: -

12. A tantárgy tananyagának leírása, tematika. Description of the subject, curriculum

(magyarul, angolul - English):

12.1. Bevezetés: a 2013. évi L. tv. és a CISM alapú kockázatmenedzsment (Introduction: risk assessment based on the Act L of 2103 and CISM);

12.2. Alapfogalmak „ISO-s" alapokon (Definitions based on ISO);

12.3. Egy kis kitérő: ISO alapú szabványosítás (ISO based standardisation);

12.4. Az ISO 27000-es szabványcsalád és a kockázatelemzés szabványa (ISO 27005) (ISO 27000 standard family and its risk assessment standard (ISO 27005));

12.5. Kockázatkezelési opciók ISO 27005 alapon (Risk management options based on ISO 27005);

12.6. Kockázatértékelés és ISO 27001:2013 (Risk assessment and ISO 27001:2013);

12.7. A kockázatértékelés áttekintő algoritmusa (Review algorithm of risk assessment);

12.8. Kockázatértékelési esettanulmányok (Risk assessment case studies);

12.9. Szabályozott kockázatmenedzsment (Áttekintés: COBIT2019 - RiskIT, ITILv4, Octave, ISO 73, ISO/IEC 31000, ISO 13335, NIST 800) (Regulated risk management (Review: COBIT2019 - RiskIT, ITILv4, Octave, ISO 73, ISO/IEC 31000, ISO 13335, NIST 800);

12.10. Kockázatmenedzsment a 2013. évi L. törvényben és a 41/2015 BM rendeletben (Risk assessment in the Act L of 2013 and Decree 41/2015);

12.11. A kockázatértékelési folyamat (azonosítás, elemzés, kiértékelés) (Risk assessment process (identification, analysis, evaluation);

12.12. Kockázati forgatókönyv (Risk scenario);

12.13. Általánosítható következtetések (Generalizable conclusions);

12.14. Kockázatmenedzsment ISO 27005:2018 mentén (Risk management according to ISO 27005:2018);

12.15. Általános kockázatmenedzsment – ISO 31000:2018 (General risk management – ISO 31000:2018);

12.16. Kockázatmenedzsment – kockázatkezelési terv (Risk management plan);

12.17. Lehetséges intézkedések meghatározása és értékelése (Identification and evaluation of potential countermeasures);

12.18. Az információvédelmi intézkedések területei (Areas of countermeasures in information security);

12.19. A kockázatértékelés karbantartása (megismétlése) (Review (repeat) of risk assessment);

12.20. Vagyonleltár és sebezhetőség vizsgálat (Asset and vulnerability assessment);

12.21. Kockázatbecslés (kvantitatív, kvalitatív, szemikvantitatív) (Risk estimation (quantitative, qualitative, semi-quantitative).

13. A tantárgy meghirdetésének gyakorisága/a tantervben történő félévi elhelyezkedése: 2. félév

14. A tanórákon való részvétel követelményei, az elfogadható hiányzások mértéke, a távolmaradás pótlásának lehetősége:

A követelmény a tanórákon történő részvétel. Az elfogadható hiányzások mértéke 25%, az efeletti távolmaradás esetén a tantárgy oktatója által meghatározott feladatot szükséges teljesíteni, mely a témához kapcsolódó házidolgozat elkészítését jelenti.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A félév folyamán egy, a félév elején kiadott gyakorlati feladatot kell kidolgozni, mely ötfokozatú skálán kerül értékelésre. Nappali munkarendben a félév utolsó előtti, levelező munkarendben az

utolsó előadásán kerül sor ZH dolgozat megírására, melynek értékelése ötfokozatú skálán történik. A nem megfelelt értékelésű ZH-t egy alkalommal lehet javítani, nappali munkarendben az utolsó előadáson, levelező munkarendben egyeztetett időpontban. A ZH során egy elképzelt kiberbiztonsági incidens különböző szempontú megoldására kell javaslatot tennie a vizsgázónak, felhasználva az elméleti és gyakorlati foglalkozásokon elsajátított ismereteket.

16. Az értékelés, az aláírás és a kreditek megszerzésének pontos feltételei:

16.1. Az aláírás megszerzésének feltételei:

A tanórákon részvétel a 14. pontban meghatározottak szerint, valamint a félévi feladat és a ZH eredményes megírása.

16.2. Az értékelés:

Gyakorlati jegy, ötfokozatú értékelés. A gyakorlati jegyet a félévi feladat és a ZH eredményének számtani átlaga adja meg.

16.3. A kreditek megszerzésének feltételei:

A kreditek megszerzésének feltétele az aláírás megszerzése és legalább elégséges gyakorlati jegy (GYJ).

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. László Gábor (2014): Kockázatértékelés, kockázatmenedzsment. Budapest: NKE, ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel;
2. Som Zoltán (2014): Kockázatmenedzsment gyakorlat. Budapest: NKE, ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel.

17.2. Ajánlott irodalom:

1. Wheeler, Evan (2011): Security Risk Management: Building an Information Security Risk Management Program from the Ground Up, Syngress, ISBN 978-1597496155;
2. Talabis, Mark (2012): Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis, Syngress, ISBN 978-1597497350978-1986862011.

Budapest, 2020.04.29.

Dr. Krasznay Csaba, PhD,
egyetemi docens sk.