NEMZETI KÖZSZOLGÁLATI EGYETEM
Államtudományi és Nemzetközi Tanulmányok Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** ÁKINTM12
2. **A tantárgy megnevezése (magyarul):** Incidensmenedzsment
3. **A tantárgy megnevezése (angolul):** Incident management
4. **Kreditérték és képzési karakter:**
   - **4.1.** 4 kredit
   - **4.2.** a tantárgy elméleti vagy gyakorlati jellegének mértéke: 67% gyakorlat, 33% 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 (14 EA + 28 GY)
   - 8.1.2. levelező munkarend: 12 (4 EA + 8 GY)
   - **8.2.** heti óraszám - nappali munkarend: 3 (1 EA + 2 GY)
   - **8.3.** Az ismeret átadásában alkalmazandó további sajátos módok, jellemzők: -
9. **A tantárgy szakmai tartalma (magyarul):** A tantárgy célja a hallgatók megismertetése az incidensmenedzsment alapjaival és eljárásrendjével. Ezen belül tárgyalásra kerül az incidensek osztályozási rendszere, az incidens válasz terv egyes komponensei, az incidensek kezeléséért felelős szervezet felépítése és feladatköre. Bemutatásra kerül a hazai és nemzetközi CERT/CSIRT hálózat. Kitér továbbá az üzletmenetfolytonosság tervezési kérdéseire is. Az előadás tárgyalja az incidensekkel kapcsolatos információk megosztásának módját hivatalos és iparági szereplőkkel. A gyakorlati foglalkozások során bemutatásra kerülnek az incidensmenedzsment folyamat technikai eszközei, melyeknek segítségével a hallgatók esettanulmányokat oldanak meg.

   A tantárgy szakmai tartalma (angolul) (Course description): The goal of this course is to introduce the basics and procedures of incident management for the students. In details, it discusses the qualification of incidents, components of incident response, the setup and role of the organization responsible for incident management. It introduces the national and international CERT/CSIRT network. It also includes the design questions of business continuity. The lecture highlights incident information sharing with official and private actors. On the practice lessons, technical tools of incident management are presented, that are used by the students to solve case studies.

10. **Elérendő kompetenciák (magyarul):**

Tudása: Ismeri azokat a fontosabb előírásokat a szabályozásokból, melyek a mindennapi munkáját befolyásolják. Átlátja, hogy milyen védelmi megoldások vannak a kibertámadás ellen. Ismeri a kibertámadás esetén alkalmazandó eljárásokat. Tisztában van az információmegosztás folyamatával bűncselekmény felmerülése esetén. Tisztában van az állami kibervédelmi rendszerrel. Megérti a szervezeti feladatokat a kibervédelemben. Ismeri az incidensmenedzsmenthez kapcsolódó fontosabb előírásokat a szabályozásokból. Átlátja, hogy az egyes műszaki megoldások hogyan támogatják az incidenskezelési eljárásokat. Ismeri az incidensek kezelése esetén alkalmazandó eljárásokat.

Képességei: Képes átlátni a kibertér aktuális fenyegetéseit. Képes támogatni szervezetét a kibervédelmi képességek kialakításában. Képes megfelelően támogatni szervezetét és a külső feleket egy kibertámadás kezelésében. Képes értelmezni a jogszabályokból eredő, incidenskezelésre és jelentésre vonatkozó követelményeket. Képes olyan védelmi intézkedések meghozatalára, melyek az incidensek elemzése alapján támogatják a kockázatok csökkentését. Képes olyan technológiai védelmi intézkedések meghozatalára, melyek fejlesztik az incidensmenedzsment folyamatot.

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 kkeletkezett információk megosztásával.

Autonómiája és felelőssége: Vállalja a kiberbiztonsági fenyegetések kezelésének felelősségét.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: He/she is familiar with the specifications of regulations that have an immediate impact on his/her daily work. He/she is familiar with defence solutions against cyber attacks. He/she is familiar with procedures applicable in case of a cyber attack. He/she is familiar with the procedure of information sharing in case of a crime. He/she is familiar with the cyber security system of the state. He/she is familiar with the organisational tasks in cyber security. He/she is familiar with the most important incident management regulations. He/she is familiar with how each technical solution supports incident management procedures. He/she is familiar with procedures for handling incidents. He/she is familiar with the cyber security system of the state. He/she is familiar with the organisational tasks in cyber security.

Capabilities: He/she is capable of understanding the current threats of cyber space. He/she is capable of supporting his/her organisation in developing cyber security skills. He/she iscapable of supporting his/her organisation and external parties in handling a cyber attack. He/she is capable of interpreting the legal requirements of incident management and reporting. He/she is capable of taking protective measures that, based on incident analysis, support risk reduction. He/she is capable of taking technological protection measures that improve the incident management 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 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 effort to support external parties by sharing information produced by his/her organisation if required.

Autonomy and responsibility: 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. Az incidenskezelés elmélete (Theory of incident management);

12.2. Az incidenskezelés jogi háttere (Legal background of incident management);

12.3. Az incidenskezelés szervezeti háttere Magyarországon és a nemzetközi térben, CERT/CSIRT szervezetek (Organizational background of incident management in Hungary and internationally, CERT/CSIRT);

12.4. A Biztonsági Műveleti Központok (Security Operation Centers);

12.5. Az incidenskezelés műszaki eszköztára (Technical tools of incident management);

12.6. Incidenssel kapcsolatos információk megosztása (Incident information sharing);

12.7. Üzletmenet-folytonosság tervezése (Business continuity planning);

12.8. Esemény, probléma, incidens fogalmának meghatározása, gyakorlati példák bemutatása

(Definition of security event, problem and incident, practical examples);

12.9. Incidens esettanulmányok (Incident related case studies);

12.10. Incidenskezelő csapat létrehozása (Setup of an incident management team);

12.11. Az incidenskezelés folyamata a gyakorlatban (Incident management in practice).

13. A tantárgy meghirdetésének gyakorisága/a tantervben történő félévi elhelyezkedése: 4. 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 hallgató értékelése a szorgalmi időszak végéig, a 12. pontban meghatározott témakörökhöz köthető, 5000 leütés terjedelmű beadandó dolgozat alapján történik. Emellett 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, a félévközi feladat legalább elégséges teljesítése és a ZH eredményes megírása.

16.2. Az értékelés:

Gyakorlati jegy, ötfokozatú értékelés. A gyakorlati jegy a félévközi feladat és a ZH értékelésének számtani átlagával (50-50%-os arányban) egyezik 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. Berzsenyi et al. (2018): Incidensmenedzsment. Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára 2017. Budapest: Dialóg Campus, ISBN 978-615-5764-99-8;
2. Berzsenyi et al. (2018): Incidensmenedzsment. Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára 2017. Budapest: Dialóg Campus, ISBN 978-963-498-090-2.

17.2. Ajánlott irodalom:

1. Luttgens, Jason T., Pepe, Matthew, Mandia, Kevin (2014): Incident Response & Computer Forensics, Third Edition. McGraw-Hill Education, ISBN 978-0071798686;
2. Thomas, Arun E. (2018): Security Operations Center - SIEM Use Cases and Cyber Threat Intelligence. CreateSpace Independent Publishing Platform, ISBN 978-1986862011.

Budapest, 2020.04.29.

Dr. Krasznay Csaba, PhD,
egyetemi docens sk.