NEMZETI KÖZSZOLGÁLATI EGYETEM
Államtudományi és Nemzetközi Tanulmányok Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** ÁKINTM06
2. **A tantárgy megnevezése (magyarul):** Biztonsági technológiák alkalmazása
3. **A tantárgy megnevezése (angolul):** Application of Security Technologies
4. **Kreditérték és képzési karakter:**
   - **4.1.** 4 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. Szádeczky Tamás, 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 biztonsági technológiák alkalmazásának folyamata, technikái, valamint az informatikai rendszerek fenyegetéseinek komplex megismertetése a hallgatókkal. A tantárgyi ismeretek átadása során bemutatásra kerülnek a kibervédelmi folyamatok elméleti alapjai, a megelőzés és a korai figyelmeztetés, az észlelés, a reagálás, valamint a biztonsági események kezelése, a hallgatók megismerik az informatikai rendszerek fenyegetéseit a természeti veszélyforrásoktól a célzott támadásokig, valamint elsajátítják a fizikai és mélyebben a logikai védelmi technológiák előnyeit, hátrányait, felhasználási lehetőségeit és korlátait. Az elsődleges cél, a komplex szemléletmód kialakítása, valamint a gyakorlati ismeretek elsajátítása. Az elsődleges célként megfogalmazott komplex szemléletmód kialakítása mellett célként fogalmazódik meg a gyakorlati ismeretek elsajátítása is annak érdekében, hogy a védelmi szférában létrejöjjön egy olyan szakember gárda, amelyik az elméleti ismereteit képes hatékonyan a gyakorlatba átültetni.

   A tantárgy szakmai tartalma (angolul) (Course description): The course shows the students the application of security technologies, the techniques, and the threats of IT systems. The course introduces students to the theoretical foundations of cyber defense processes, prevention and early warning, detection, response, and security incident management; and more deeply about the advantages, disadvantages, uses and limitations of logical protection technologies. The primary goal is to develop a complex approach to those techniques. In addition to developing a complex approach as the primary objective, the aim is also to acquire practical knowledge in order to establish a team of professionals in the defense sector who can effectively translate their theoretical knowledge into practice.

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

Tudása: Átlátja, hogy milyen védelmi megoldások vannak a kibertámadás ellen.

Képességei: Képes olyan technológiai védelmi intézkedések meghozatalára, amelyek a cyber kill chain egyes elemeihez kapcsolódnak.

Attitűdje: A problémákra a megoldásokat keresi.

Autonómiája és felelőssége: Tudatosan törekszik a kiberbiztonság sajátosságainak megfelelő, korszerű ismeretek hazai és nemzetközi szinten történő gyakorlati alkalmazására.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: Defence solutions against cyber attacks.

Capabilities: Taking technological defensive measures related to elements of the cyber kill chain.

Attitude: Searching for solutions for issues.

Autonomy and responsibility: To implement advanced knowledge characterising cyber security on a national and international level.

11. Előtanulmányi követelmények: -

12. A tantárgy tananyagának leírása, tematika. Description of the subject, curriculum (magyarul, angolul - English):

12.1. Informatikai rendszerek felépítése (Architecture of information systems);

12.2. Informatikai rendszerek, komplexitása, kapcsolatrendszerük (Complexity and interconnection of information systems);

12.3. Fenyegetések a fizikai biztonságra (Threats to physical security);

12.4. Fenyegetések a logikai biztonságra (Threats to logical security);

12.5. Informatikai és hírközlő hálózatok jellemzői, támadások és védelmi intézkedések (Properties of ICT networks, attack and protection);

12.6. Hálózatok sérülékenységei és kihasználásuk. (Computer network vulnerabilities and exploits);

12.7. Fenyegetések az adminisztratív biztonságra (Threats to administrative security);

12.8. Védelmi lehetőségek, intézkedések (Protection measures);

12.9. Munkaállomások biztonsága (Workstation security);

12.10. Mobileszközök és távmunka biztonsága (Mobile device and teleworking security);

12.11. Internet of Things (IoT) jellemzői, biztonsági kihívásaik (Security issues of IoT);

12.12. Ipari vezérlés és ipar 4.0 jellemzői, biztonsági kihívásaik (Security issues of ICS and Industry 4.0);

12.13.

13. A tantárgy meghirdetésének gyakorisága/a tantervben történő félévi elhelyezkedése: 1. félév

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

A tanórákon való 75 %-os részvétel. A hallgató köteles az előadás anyagát beszerezni, abból önállóan felkészülni.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A félév során 2 zh-t kell a hallgatóknak megírni. A zárthelyi dolgozat értékelése ötfokozatú skálán történik az alábbiak szerint: 51 %-tól elégséges, 63 %-tól közepes, 75 %-tól jó, 87 %-tól jeles.

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

16.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele a tanórákon való 75 %-os részvétel és a zárthelyi dolgozatok mindegyikének legalább elégséges osztályzata.

16.2. Az értékelés:

Gyakorlati jegy a két zárthelyi eredményének számtani átlaga alapján.

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. Leitold Ferenc (2014): Biztonsági technológiák alkalmazása. Budapest: NKE, ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel;
2. Muha Lajos, Krasznay Csaba (2014): Az elektronikus információs rendszerek biztonságának menedzselése, Budapest NKE, ÁROP – 2.2.21 Tudásalapú közszolgalati előmenetel ISBN 978-615-5870-27-9;
3. Buttyán Levente, Vajda István (2004): Kriptográfia és alkalmazásai, Typotex Kft., Budapest. ISBN: 978-963-2796-96-3;
4. Berzsenyi Dániel, Dr. Bodó Attila Pál, Kapitány Sándor, Sági Gábor, Sebők Viktória (2018): Incidensmenedzsment. Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában. Dialog Campus, ISBN 978-615-5845-01-7.

17.2. Ajánlott irodalom:

1. Brown, Lawrie, Stalling, William: Computer Security: Principles and Practice, Pearson, 2018. (4. kiadás) ISBN 978-0134794105;
2. CISM Review Manual, ISACA, 2016.; ISBN-13: 978-1604205084
3. NIST Special Publications 800-as sorozat.

Budapest, 2020.04.29.

Dr. Szádeczky Tamás, PhD,
egyetemi docens sk.