NEMZETI KÖZSZOLGÁLATI EGYETEM
Államtudományi és Nemzetközi Tanulmányok Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** ÁKINTV12
2. **A tantárgy megnevezése (magyarul):** Információbiztonsági tudatosság
3. **A tantárgy megnevezése (angolul):** Information security awareness
4. **Kreditérték és képzési karakter:**
   - **4.1.** 2 kredit
   - **4.2.** a tantárgy elméleti vagy gyakorlati jellegének mértéke: 100% gyakorlat, 0% elmélet
5. **A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):** ÁNTK BA szintű szabadon választható tárgy
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. Bányász Péter, PhD, tanársegéd
8. **A tanórák száma és típusa**
   - **8.1.** össz óraszám/félév:
   - 8.1.1. nappali munkarend: 28 (0 EA + 28 GY)
   - 8.1.2. levelező munkarend: 8 (0 EA + 8 GY)
   - **8.2.** heti óraszám - nappali munkarend: 2 (0 EA + 2 GY)
   - **8.3.** Az ismeret átadásában alkalmazandó további sajátos módok, jellemzők: -
9. **A tantárgy szakmai tartalma (magyarul):** A tantárgy keretein belül az adott tematika mentén a hallgatók megismerhetik a leggyakoribb és legújabb támadási technikákat, ezek észlelésének és megelőzésének lehetőségeit. A tananyag összeállítása kifejezetten azon témakörökön alapszik, melyek az emberi tényező biztonságtudatosságát teszik próbára, és elsősorban az ismeretek hiányára, vagy a figyelmetlenségre, naivitásra építenek.

   A tantárgy szakmai tartalma (angolul) (Course description): Within the subject, students will be familiar with the most common and latest attack techniques along with the possibilities of detecting and preventing them. The compilation of the curriculum is based on topics that are conducive to the security awareness of the human factor and primarily build on the lack of knowledge, or on ignorance and naivety.

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

Tudása: Megérti a szervezeti feladatokat a kiberbiztonságban.

Képességei: A tananyag elsajátításával a hallgatók képesek lesznek felismerni és azonosítani az esetlegesen ellenük irányuló támadásokat, valamint megelőzni, hogy ilyen jellegű támadások célpontjává váljanak. Képes olyan védelmi intézkedések meghozatalára, amelyek segítik a humán fenyegetettségből eredő kockázatok csökkentését.

Attitűdje: Az órákon elhangzottak segítségével a résztvevők gondoskodni tudnak saját eszközeik, alkalmazásaik biztonságos beállításáról, megfelelő védelméről.

Partner abban, hogy se a szervezete, se ő maga ne váljon kibertámadás áldozatává.

Autonómiája és felelőssége: Gyakorlatába beépíti és alkalmazza az e szakterületen folyó kutatások eredményeit.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: Understands organizational responsibilities in cybersecurity.

Capabilities: By acquiring the curriculum, students will be able to recognise and identify possible attacks against them and prevent them from becoming targets of such attacks. Taking defensive measures that ensure the reduction of risk resulting from threat against humans.

Attitude: With the help of the lessons, participants can take care of their own devices, secure configuration and proper protection of their applications. Cooperation in preventing his/her organisation and him/herself from becoming a victim of a cyber attack.

Autonomy and responsibility: He/She integrates and applies the results of research in this field into practice.

11. **Előtanulmányi követelmények:** -

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

12.1. Bevezetés az információbiztonsági tudatosságba (Introduction to the information security awareness);

12.2. Social Engineering I.- Humán alapú támadások (Social Engineering I.- Human-based attacks);

12.3. Social Engineering II.- IT alapú támadások (Social Engineering II.- IT-based attacks);

12.4. Kiberfenyegetettségek I. Kiberbűnözés (Cyber threats I.- Cyber crime);

12.5. Kiberfenyegetettségek II. Kiberterrorizmus és hacktivizmus (Cyber threats II.- Cyber terrorism and hacktivism);

12.6. Kiberfenyegetettségek III. Kiberkémkedés (Cyber threats III.- Cyber espionage);

12.7. Kiberfenyegetettségek IV. Kiberhadviselés (Cyber threats IV.- Cyber warfare);

12.8. Lélektani műveletek (Psychological operations);

12.9. A közösségi média kockázatai (The risks of social media);

12.10. Internetes zaklatás (Cyberbulling);

12.11. Okos mobil eszközök biztonsága (The safety of smart mobile devices)

12.12.Jó gyakorlatok az információbiztonságban (Best practices in building information security awareness);

12.13. Prezentációk (Presentations);

12.14.Összefoglalás (Conclusion).

13. **A tantárgy meghirdetésének gyakorisága/a tantervben történő félévi elhelyezkedése:** őszi 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 témakörben beadandó dolgozat készítése szükséges. A hallgató köteles az előadás

anyagát beszerezni, abból önállóan felkészülni.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A tanulmányi munka alapja az órai aktivitás és a tantárgyi tematika 12. pontjában meghatározott alkalommal kiselőadás tartása a hallgató által tantárgyi programból választott témából. A prezentáció értékelése ötfokozatú skálán történik. Amennyiben a hallgató nem tudja megtartani a kis előadást, úgy az oktató által meghatározott terjedelemben beadandó dolgozatot köteles készíteni a szemeszter végéig.

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

16.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele 75%-os részvétel a foglalkozásokon, illetve a tantárgyi tematika 15. pontjában meghatározott feltételek teljesítése.

16.2. Az értékelés:

Részvétel a szemináriumi foglalkozások legalább 75 %-án, valamint a szemeszter végén kiselőadás megtartása.

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. Kevin D. Mitnick - William L. Simon: A legendás hacker - A megtévesztés művészete, Perfact-Pro Kft., Budapest, 2003., ISBN: 9789632065557;
2. Kevin D. Mitnick - William L. Simon: A legendás hacker 2. - A behatolás művészete, Perfact-Pro Kft., Budapest, 2006., ISBN: 9638647256.

17.2. Ajánlott irodalom:

1. David Willson – Henry Dalziel: Cyber Security Awareness for Lawyers, Syngress, 2015. ISBN 978-0128047200
2. P. W. Singer – Allan Friedman: Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford University Press, 2014. ISBN 978-0199918119
3. Bruce Schneier: Click Here to Kill Everybody: Security and Survival in a Hyper-connected World, W. W. Norton & Company, 2018. ISBN 978-0393608885

Budapest, 2020.04.09.

Dr. Bányász Péter, PhD,
tanársegéd sk.