NEMZETI KÖZSZOLGÁLATI EGYETEM
Hadtudományi és Honvédtisztképző Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** HKKNBM03
2. **A tantárgy megnevezése (magyarul):** A hazai és nemzetközi szervezetek feladatai a kibervédelemmel összefüggésben
3. **A tantárgy megnevezése (angolul):** Tasks of national and international organizations in the context of cybersecurity
4. **Kreditérték és képzési karakter:**
   - **4.1.** 3 kredit
   - **4.2.** a tantárgy elméleti vagy gyakorlati jellegének mértéke: 0% gyakorlat, 100% elmélet
5. **A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):** kiberbiztonsági MA
6. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** Hadtudományi és Honvédtisztképző Kar, Katonai Nemzetbiztonsági Tanszék
7. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Magyar Sándor, PhD, adjunktus
8. **A tanórák száma és típusa**
   - **8.1.** össz óraszám/félév:
   - 8.1.1. nappali munkarend: 28 (28 EA + 0 GY)
   - 8.1.2. levelező munkarend: 8 (8 EA + 0 GY)
   - **8.2.** heti óraszám - nappali munkarend: 2 (2 EA + 0 GY)
   - **8.3.** Az ismeret átadásában alkalmazandó további sajátos módok, jellemzők: -
9. **A tantárgy szakmai tartalma (magyarul):** A képzésben résztvevő hallgatók átfogó módon ismerkedhetnek meg a kiberbűnözéssel és a kiberbiztonsággal folalkozó hazai és a nemzetközi szervezetekkel, valamint feladataikkal. Az elméleti ismeretek elsajátítása előadások keretében, ám interaktív jellegű foglalkozásokon keresztül valósul meg. Az előadások alkalmával megbeszélendő jogszabályok és szervezetek különösen az elmúlt időszak változásai, az egyetemes (európai) és magyar kiberbiztonsági és a kiberbűnözés elleni harc lehetséges kapcsolódási pontjaira is rámutatnak.

   A tantárgy szakmai tartalma (angolul) (Course description): The students participating in the course will get a comprehensive introduction to national and international organizations dealing with cybercrime and cyber security and their tasks. Theoretical knowledge is acquired through interactive lectures. The discussion about relevant legislation and tasks of organizations, especially recent changes and developments also highlight possible links between global (but primary European) and Hungarian cybersecurity and the fight against cybercrime.

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

Tudása: Ismeri a nemzetközi jog alkalmazhatóságát a kibertérben. 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.

Képességei: Képes olyan technológiai védelmi intézkedések meghozatalára, amelyek a cyber kill chain egyes elemeihez kapcsolódnak. Képes támogatni szervezetét a kibervédelmi képességek kialakításában.

Attitűdje: Hatékony lépéseket tesz a kibertámadások megelőzése érdekében, így csökkentve a

szervezete kitettségét.

Autonómiája és felelőssége: Vállalja a szakterület, a szakmai praxis módszertanának fejlesztéséhez szükséges elméleti, tudományos kutatási és gyakorlati információk beszerzésének, értékelésének és hasznosításának végrehajtását.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: The applicability of international law in cyberspace. The need for introducing internal regulations defined by employers in order to maintain integrity and availability of the data stored in information systems. Organisational tasks in cyber security.

Capabilities: Is capable of supporting his/her organisation in developing cyber security skills. Is capable of taking technological defensive measures related to elements of the cyber kill chain.

Attitude: An effort to take effective measures in order to prevent cyber attacks, by this means reducing the exposure of his/her organisation.

Autonomy and responsibility: To obtain, evaluate and utilize theoretical, scientific and practical information necessary for the improvement of the field and the methodology of professional practice.

11. Előtanulmányi követelmények: -

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

12.1. A kiberbűncselekményekkel és kibervédelemmel foglalkozó hazai szervezetek (Domestic organizations dealing with cybercrime and cyber defence);

12.2. A kiberbűncselekmények nyomozásával foglalkozó hazai szervezetek és feladataik (Domestic organizations dealing with cybercrime investigations and their tasks);

12.3. A kibervédelemmel foglalkozó hazai szervezetek és feladataik (Domestic cyber defense organizations and their responsibilities);

12.4. A kiberbűncselekmények nyomozásával foglalkozó és kibervédelemmel foglalkozó szervezetek együttműködése (Cooperation between cybercrime investigation and cyber defense organizations);

12.5. A kiberbűncselekményekkel és kibervédelemmel foglalkozó nemzetközi szervezetek és feladataik (International organizations dealing with cybercrime and cyber defense and their tasks);

12.6. A kiberbűncselekményekkel foglalkozó európai uniós és más nemzetközi szervezetek és feladataik (The European Union and other international organizations dealing with cybercrime and their tasks);

12.7. A kibervédelemmel foglalkozó európai uniós és más nemzetközi szervezetek és feladataik (The European Union and other international organizations organizations dealing with cyber defence and their tasks);

12.8. Jogok és kötelezettségek a bűnüldöző szervezetek és a magánszektor között a kiberbűncselekmények elleni harcban (Rights and obligations between law enforcement agencies and the private sector in the fight against cybercrime);

12.9. Együttműködési kötelezettségek (Obligations of cooperation);

12.10. Adatkérésekkel kapcsolatos szabályozás (Regulation of data requests);

12.11. A szervezetek közötti együttműködésre vonatkozó jogszabályi háttér (Legal background for cooperation between organizations).

13. A tantárgy meghirdetésének gyakorisága/a tantervben történő félévi elhelyezkedése: 3. félév

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

A hallgató köteles az előadások legalább 80%-án részt venni. Rövid/tartós távolmaradás indokolt esetben (orvosi, szolgálati) pótolható, amely pótlás egyéni megbeszélés szerint történik.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A tanulmányi munka alapja az előadások rendszeres látogatása (a Foglalkozásokon való részvétel feltételei pont szerint). Az elméleti anyagából egy évközi ZH sikeres, legalább elégséges (kettes) érdemjegyre történő megírása. A zárthelyi dolgozat értékelése: ötfokozatú értékelés – (a helyes válaszok aránya 0-60% elégtelen; 61-70% elégséges; 71-80% közepes; 81-90% jó; 91-100% jeles osztályzat). Eredménytelen zárthelyi dolgozat kétszer javítható.

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

16.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele a Foglalkozásokon való részvétel pontban meghatározott arányú részvétel a foglalkozásokon és a Félévközi feladatok, ismeretek ellenőrzésének rendje pontban meghatározott félévközi feladatok legalább elégséges teljesítése.

16.2. Az értékelés:

A félév értékelése kollokvium – írásbeli vizsga. A Tanszék beszámoló felkészülési kérdéseket ad ki. A vizsga tartalmát az előadáson elhangzottak és az alább felsorolt kötelező és ajánlott irodalmak anyagai képezik. A vizsgadolgozat értékelése szummatív: 0-50% - elégtelen, 51-70% - elégséges, 71-80% - közepe, 81-90% - jó, 91-100% - jeles.

16.3. A kreditek megszerzésének feltételei:

A kreditek megszerzésének feltétele az aláírás megszerzése és legalább elégséges kollokvium (K).

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. Dr. Nagy Zoltán András: Számítástechnikai környezetben elkövetett bűncselekmények (megjelenés alatt);
2. Gyaraki Réka: A nyomozóhatóság és a katasztrófavédelem feladata a kiberbűncselekmények vonatkozásában, In. Szakmai Szemle, 2017/1.szám, pp. 113-127.;
3. Sorbán Kinga: Az informatikai bűncselekmények elleni fellépés nemzetközi dimenziói, In. Themis: Az ELTE ÁLLAM-és Jogtudományi Doktori Iskola lektorált elektronikus folyóirata, 2015., pp. 344-375.

17.2. Ajánlott irodalom:

1. Kovács László (2018): A kibertér védelme. Dialóg Campus, Budapest, 2018., ISBN 978-615-5889-63-9 (nyomtatott)ISBN 978-615-5889-64-6 (elektronikus);
2. Kovács László (2018): Kiberbiztonság és-stratégia. Dialóg Campus, Budapest, 2018., ISBN 978-615-5920-92-9 (nyomtatott)ISBN 978-615-5920-93-6 (elektronikus);
3. Alexander Klimburg (Ed.) (2012): National Cyber Security Framework Manual. NATO Cooperative Cyber Defence Centre of Excellence, ISBN 978-9949-9211-1-9.

Budapest, 2021.01.05.

Dr. Magyar Sándor, PhD,
adjunktus sk.

NEMZETI KÖZSZOLGÁLATI EGYETEM
Rendészettudományi Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** NPNBM24
2. **A tantárgy megnevezése (magyarul):** A kiberbiztonság humán tényezői
3. **A tantárgy megnevezése (angolul):** Human factors of cybersecurity
4. **Kreditérték és képzési karakter:**
   - **4.1.** 3 kredit
   - **4.2.** a tantárgy elméleti vagy gyakorlati jellegének mértéke: 0% gyakorlat, 100% elmélet
5. **A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):** kiberbiztonsági MA
6. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** Rendészettudományi Kar, Polgári Nemzetbiztonsági Tanszék
7. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Dobák Imre, PhD, egyetemi docens
8. **A tanórák száma és típusa**
   - **8.1.** össz óraszám/félév:
     - 8.1.1. nappali munkarend: 28 (28 EA + 0 GY)
     - 8.1.2. levelező munkarend: 8 (8 EA + 0 GY)
   - **8.2.** heti óraszám - nappali munkarend: 2 (2 EA + 0 GY)
   - **8.3.** Az ismeret átadásában alkalmazandó további sajátos módok, jellemzők: -
9. **A tantárgy szakmai tartalma (magyarul):** A tárgy az emberi tényező oldaláról vizsgálja a kiberbiztonság jelentőségét, és ismerteti meg a hallgatókat a „humán alapú” sebezhetőség témakörével. A „social engineering”, az emberi tényező kihasználására épülő támadási formák témakörében vizsgálja a humán kockázatok jelentőségét, a támadások humán alapú módszereit, technikáit, céljait, a védekezés lehetőségeit. Az információbiztoság emberi tényezői témakörében esettanulmányokkal, példákkal mélyíti a biztonságtudatos szakmai gondolkodás fejlődését.

   A tantárgy szakmai tartalma (angolul) (Course description): The subject examines the importance of cybersecurity from the side of human factor and introduces the topic of "human-based" vulnerability. Social engineering, forms of attack based on the use of the human factor, examines the significance of human risks, the human-based methods, techniques, objectives, and defense capabilities of attacks. Deepens the development of security-conscious professional thinking in the field of human factors of information security with case studies and examples.

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

Tudása: Tisztában van az emberi tényező szerepével a kibertámadások kivitelezése során.

Képességei: Képes olyan védelmi intézkedések meghozatalára, amelyek segítik a humán fenyegetettségből eredő kockázatok csökkentését.

Attitűdje: Kiemelt kockázatként kezeli a belső munkavállalókat, és ennek megfelelően tervezi meg az információbiztonsági folyamatokat.

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

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: The role of human factors in the execution of cyber attacks.

Capabilities: Taking defensive measures that ensure the reduction of risk resulting from threat against humans.

Attitude: An ability to treat internal employees as high risk and plans information security processes accordingly.

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. A kiberbiztonság humán oldala, az emberi tényező szerepe (The human side of cybersecurity, the role of human factor) (N/4, L/2 tanóra):

12.2. - A humán kockázatok, a humán alapú sebezhetőség a kibertérben;

12.3. - Infokommunikációs trendek és hatásaik az ICT eszközök felhasználóira;

12.4. - A biztonságtudatosság jelentősége.

12.5. A kibertér szereplői és támadói (Players and attackers in the cyberspace) (N/6, L/2 tanóra):

12.6. - A kibertér támadói és mögöttes szándékaik;

12.7. - A támadók kategorizálása motivációjuk alapján.

12.8. Az emberi tényező kihasználására épülő támadási technikák és formák (Attacking techniques and forms based on human factors) (N/6, L/2 tanóra):

12.9. - A támadásokhoz felhasznált információk forrásai;

12.10. - Az emberi tényező kihasználására épülő támadási technikák;

12.11. - A támadások megelőzésének lehetőségei.

12.12. Hírszerzés, kémkedés a kibertérben (Intelligence, espionage in the cyberspace) (N/6, L/1 tanóra):

12.13. - Nemzetközi kitekintés, műveletek a kibertérben;

12.14. - A kibertér humán alapú információgyűjtő lehetőségének várható tendenciái;

12.15. - Adataink az OSINT tükrében.

12.16. A közösségi oldalak veszélyei (Threats of social networking sites) (N/8, L/2 tanóra):

12.17. - A közösségi média szerepe a befolyásolás szempontjából;

12.18. - A közösségi média szerepe vs. kapcsolattartás veszélyei (személyiségprofil);

12.19. - Bűnügyi-, nemzetbiztonsági megközelítés;

12.20. - A közösségi média szerepe a bűnmegelőzés szempontjából.

12.21. A biztonságtudatosítás jelentősége, az oktatás szerepe (Importance of awareness, role of education) (N/4, L/1 tanóra):

12.22. - Biztonságtudatosság magatartás kialakításának jelentősége, lehetőségei;

12.23. - Biztonságtudatosságot fejlesztő oktatási módszerek.

12.24. Esettanulmányok feldolgozása, gyakorlatok (Processing of case studies) (N/8, L/4 tanóra).

13. A tantárgy meghirdetésének gyakorisága/a tantervben történő félévi elhelyezkedése: 3. félév

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

A hallgató köteles a tanórák min. 70 %-án részt venni. Amennyiben a hallgató az elfogadható hiányzások mértékét túllépi, köteles az elmaradt órai tananyag beszerzéséről gondoskodni, a részvétel a tanárral való egyeztetés alapján meghatározott házi dolgozat készítésével pótolható.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A félév során félévközi feladatként nappali képzésben két zárthelyi dolgozat megírására kerül sor egy a 3. és egy a 6. témakör zárását követően. (Levelező képzésben egy zárthelyi a 6. témakör zárását követően). A zárthelyi legalább elégséges eredménnyel történő teljesítése az aláírás feltétele. A zárthelyi ötfokozatú kerül értékelésre (60 %-tól elégséges, 70 %-tól közepes, 80-tól % jó, 90 %-tól jeles). Sikertelen zárthelyi dolgozat a szorgalmi időszak végéig pótolható.

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

16.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele a meghatározott arányú részvétel a foglalkozásokon és a meghatározott félévközi feladat legalább elégséges teljesítése.

16.2. Az értékelés:

A vizsga típusa: Kollokvium (írásbeli vagy szóbeli) A kollokviumra a 12. pontban tárgyalt témakörökből a tanszék által felkészülési kérdéssor kerl kiadásra. A kollokvium ötfokozatú értékelésű. Írásbeli kollokvium esetén annak értékelése szummatív: 0-50% - elégtelen, 51-70% - elégséges, 71-80% - közepes, 81-90% - jó, 91-100% - jeles.

16.3. A kreditek megszerzésének feltételei:

A kreditek megszerzésének feltétele az aláírás megszerzése és legalább elégséges kollokvium (K).

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. Kovács László: A kibertér védelme, Dialóg Campus Kiadó, Budapest, 2018., ISBN 978-615-5889-63-9 (nyomtatott)ISBN 978-615-5889-64-6 (elektronikus);
2. Mitnick, Kevin D. -Simon, William L.: A legendás hacker - A megtévesztés művészete. Perfact-Pro Kiadó, 2003., ISBN 963-206-555-7;
3. Bányász Péter: Social engineering és közösségi média, Nemzetbiztonsági Szemle, 5:(1) pp. 59-77. (2018).

17.2. Ajánlott irodalom:

1. Mádi-Nátor Anett – Kardos Zoltán (2014): Információbiztonság-tudatosság gyakorlat. Budapest: NKE, ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel;
2. Leitold Ferenc. Sebezhetőségvizsgálatok a gyakorlatban, NKE VTKI, Budapest, 2014.;
3. Bencsik Balázs – Sabjanics István: Digitális környezetünk fenyegetettsége a mindennapokban, Dialóg Campus Kiadó 2018, Budapest, ISBN 978-615-5920-89-9;
4. Berzsenyi Dániel: A kiberbiztonság humán oldala, Nemzet és Biztonság 2017/2. szám 54–67.
5. Hadnagy, Cristopher : Social engineering: The art of Human Hacking, Wiley Publishing, Inc. 2011. ISBN 978-0470639535;

Budapest, 2021.01.05.

Dr. Dobák Imre, PhD,
egyetemi docens sk.

NEMZETI KÖZSZOLGÁLATI EGYETEM
Államtudományi és Nemzetközi Tanulmányok Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** ÁLLTM08
2. **A tantárgy megnevezése (magyarul):** A magyar közigazgatás szervezeteinek és szakigazgatási rendszereinek működése
3. **A tantárgy megnevezése (angolul):** The institutions and processes of the Hungarian Public Administration
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):** kiberbiztonsági MA
6. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** Államtudományi és Nemzetközi Tanulmányok Kar, Lőrincz Lajos Közigazgatási Jogi Tanszék
7. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Kovács Éva Margit, PhD, egyetemi docens
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 célja, hogy a megismertesse a hallgatókat a közigazgatás, mint szervezetrendszer felépítésével, az alapvető szervezési elvekkel, különösen a közigazgatás funkcionális, szakágazatok szerinti tagozódásával. A tantárgy keretében a hallgatók átfogó ismereteket kapnak a magyar közigazgatási szervezetrendszer működési gyakorlatáról, a magyar közigazgatás szervezeti és hatásköri rendszeréről, a közigazgatási szervek típusairól és jellegzetességeiről. A heterogén közigazgatási funkciók és hatáskörök szervezetekhez/szervezettípusokhoz rendelésével a tantárgy komplex módon kívánja bemutatni a magyar közigazgatás szerteágazó és több szintű hálózati rendszerét.

   A tantárgy szakmai tartalma (angolul) (Course description): The aim of the course is to provide an introduction for students to the institutions and structure of public administration and public policies. From an organisation theory approach the course provides an overview on the basic organisational management principles withing the public administration, such as the divisiion of task and functions and the concept of bureaucratic organization, .During the semester students will get a comprehensive knowledge of the practices and concepts of government institutions and processes. the administrative layers of the Hungarian governement and the divison of power and tasks between administrative layers and the scope of authoirties of public organizations. By presenting heterogeneous administrative functions and policy fields the course aims to provide an overall understanding on the multi-level government system in Hungary.

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

Tudása: Ismeri azokat a fontosabb előírásokat a szabályozásokból, amelyek a mindennapi munkáját befolyásolják.

Képességei: Képes értelmezni a jogszabályokból eredő követelményeket.

Attitűdje: A maga komplexitásában tervezi meg az információbiztonsági irányítási rendszert.

Autonómiája és felelőssége: Értékkötelezett módon vesz részt a kibertér komplexitásának és kölcsönhatásainak ismerete által a különböző hivatásrendek feladatainak szervezésében.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: Specifications of regulations that have an immediate impact on his/her daily work.

Capabilities: He/she is capable interpreting legal requirements.

Attitude: His/her personal attitude is characterized by an effort to design the cyber security management system in its own complexity..

Autonomy and responsibility: To take part in organising tasks of the various professions by having an overview of the complexity and interactions of cyber space.

11. Előtanulmányi követelmények: -

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

12.1. A közigazgatási szervezetrendszer szervezési elvei és felépítése. Szervezetelméleti ismeretek (The general principles and structure of the public administration as an organization system. Introduction to the Organizational Theories);

12.2. A közigazgatás szervezési elvei: centralizáció, dekoncentráció, decentralizáció, delegáció és koordináció (The organizational principals of public adminitsration: centralization, deconcentration, decentralization, delegation and coordination);

12.3. A közigazgatási szervek típusai és hatáskörei. Az egyes közigazgatási szervek és funkciójuk áttekintése (Overview on the different types of public organization and their functions);

12.4. A közigazgatás vertikális tagozódása: a központi igazgatás (The vertical division of public administration: central government);

12.5. A közigazgatás vertikális tagozódása: a területi igazgatás (The vertical division of public administration: the territorial level og the government);

12.6. A közigazgatás vertikális tagozódása: a helyi igazgatás (The vertical division of public administration: the local government);

12.7. A közigazgatás szakágaztok szerinti tagozódása (The sectoral/ horizontal division of the public administration);

12.8. A gazdasági területek igazgatása: Piacfelügyelet (Public policies on the economic sector. Market surveillance);

12.9. A gazdasági területek igazgatása: Hatósági tevékenység (Public policies on the economic sector. Regulative and administrative measures);

12.10. A humánszolgáltatások igazgatása (szociális ellátás, oktatásügy) (Public policies and the administration of human services (welfare, education));

12.11. A humánszolgáltatások igazgatása (nyugdíj igazgatás, egészségügy) (Public policies and the administration of human services (elderley care and the pension system, heath sector));

12.12. A rendvédelmi, közbiztonsági feladatok igazgatása (Public security and law enforcement);

12.13. Szakpolitika alkotás folyamata (The Processes of Public Policy);

12.14. Ismeretellenőrzés (Mid - term exam).

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 hallgató köteles a foglalkozások legalább 75 %-án részt venni. Amennyiben a hallgató az elfogadható hiányzások mértékét túllépi , nem szerez aláírást. Hiányzás esetén az órai részvétel pótolható a tananyag önálló feldolgozásával és arról írásban történő számadással az oktatóval előre egyeztetve.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A félév során öt , az oktató által kiadott esettanulmány feldolgozása és az esettanulmányokkal összefüggő kérdések megválaszolása. Egy zárthelyi dolgozat eredményes megírása (50%+ 1 pont elérése).

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

16.1. Az aláírás megszerzésének feltételei:

A hallgató köteles a foglalkozások legalább 75 %-án részt venni. Egy zárthelyi dolgozat eredményes megírása (50%+ 1 pont elérése).

16.2. Az értékelés:

A félévközi zárthelyi dolgozatra kapott érdemjegy 50% -ban, az esettanulmányokra kapott értékelés 50% -ban számít be az évvégi érdemjegy kialakításánál. Mindkét komponensből szükséges a minimum elégséges (2) értékelése megszerzése.

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. Kovács Éva Margit (2016) A magyar közigazgatás szervezeti és hatásköri rendszere. Nemzeti Közszolgálati Egyetem, Budapest. 75. o.
2. Kovács - Radics -Bauer – Kovács (2017): Szakigazgatási ismeretek II.Budapest: Nemzeti Közszolgálati Egyetem, 2017. ;
3. Kovács - Jámbor – Téglásiné Kovács – Mikó (2017): Szakigazgatás I. Budapest: Nemzeti Közszolgálati Egyetem, 2016. 121 p.
4. Lapsánszky András – Patyi András – Takács Albert (2018): A közigazgatás szervezete és szervezeti joga - A magyar közigazgatás és közigazgatási jog általános tanai III. Dialóg Campus Kiadó, Budapest

17.2. Ajánlott irodalom:

1. Lőrincz Lajos (2007): A közigazgatás alapintézményei. 2. kiadás. HVG–Orac, Budapest;
2. Ongaro, E - Van Thiel, S. (2018) : The Palgrave Handbook of Public Administration and Management in Europe. Palgrave Macmillan UK. eBook ISBN 978-1-137-55269-3;
3. E. Ferlie–L. E. Lynn.–C. Pollitt (szerk).: The Oxford Handbook of Public Management. Oxford, Oxford University Press, 2007.

Budapest, 2021.01.05.

Dr. Kovács Éva Margit, PhD,
egyetemi docens sk.

NEMZETI KÖZSZOLGÁLATI EGYETEM
Államtudományi és Nemzetközi Tanulmányok Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** ÁKINTM08
2. **A tantárgy megnevezése (magyarul):** Adatvédelem
3. **A tantárgy megnevezése (angolul):** Data protection
4. **Kreditérték és képzési karakter:**
   - **4.1.** 3 kredit
   - **4.2.** a tantárgy elméleti vagy gyakorlati jellegének mértéke: 0% gyakorlat, 100% 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. Péterfalvi Attila, PhD, egyetemi docens
8. **A tanórák száma és típusa**
   - **8.1.** össz óraszám/félév:
   - 8.1.1. nappali munkarend: 28 (28 EA + 0 GY)
   - 8.1.2. levelező munkarend: 8 (8 EA + 0 GY)
   - **8.2.** heti óraszám - nappali munkarend: 2 (2 EA + 0 GY)
   - **8.3.** Az ismeret átadásában alkalmazandó további sajátos módok, jellemzők: -
9. **A tantárgy szakmai tartalma (magyarul):** A hallgatók az alapképzésben szerzett ismeretekre alapozva átfogó és elmélyült ismereteket szereznek az adatvédelem, köz és magánszféra adatkezelése területén, megismerkednek a hazai és nemzetközi joggyakorlattal. A tantárgyhoz kapcsolódó jogesetek feldolgozása. Ismereteket szereznek a közérdekből nyilvános személyes adat kezeléséről.

   A tantárgy szakmai tartalma (angolul) (Course description): The students will acquire comprehensive and in-depth knowledge of data protection, the data processing of the public and the private sector, and will learn about the national and the international legal practice, based on their initial education. Processing of legal cases related to the subject. They will acquire knowledge of the processing of personal data accessible on public interest grounds.

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

Tudása: Ismeri az adatvédelem körében alkalmazandó hazai és uniós szabályokat. Ismeri az adatvédelem alapfogalmait és alapintézményeit. Ismeri az adatvédelem alapelveit. Ismeri az adatvédelem területén az érintett jogokat. Ismeri az adatkezelői kötelezettségeket. Ismeri az adatbiztonsági eljárásokat. Ismeri a Nemzeti Adatvédelmi és Információszabadság Hatóság eljárásait, feladatkörét, joghatóságát, hatáskörét, illetékességét. Ismeri az adatvédelem körében a tanúsítás és az akkreditáció szabályait.

Képességei: Képes azonosítani, ha egy tevékenység adatkezelésnek minősül, illetve képes megállapítani az egyes adatkezelési műveletek, valamint a kezelt személyes adatok körét. Képes szakmailag megfelelő módon meghatározni az adatkezelés jogalapját, az adatkezelési célokat. Képes szakmailag megfelelő módon elhatárolni egymástól az adatkezelőt és az adatfeldolgozót. Képes a Nemzeti Adatvédelmi és Információszabadság Hatóság eljárásait a gyakorlatban értelmezni. Képes az adatvédelmi incidensek azonosítására, kezelésére és bejelentésére.

Attitűdje: Fontosnak tartja az adatvédelem jogi, szervezeti, igazgatási, gyakorlati vetületeivel

kapcsolatos kérdések magabiztos ismeretét. Törekszik az adatvédelmi kockázatok azonosítására, elemzésére és kezelésére. Törekszik az adatvédelmi tudatosítás minél szélesebb körű megvalósítására. Fontosnak tartja az adatbiztonság minél hatékonyabb megvalósulását. Nyitott az adatkezelői kötelezettségek megismerése és gyakorlati támogatása iránt.

Autonómiája és felelőssége: Felelősen viszonyul az új uniós adatvédelmi rezsim megismeréséhez és megértéséhez. Megfelelő ismeretekkel rendelkezik az adatbiztonság érvényre juttatásához. Önállóan képes egy adatkezelés során a kockázatok kiszűrésére, a körülmények reális értékelésére és a felmerülő problémák kezelésére.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: Knowledge of applicable national and EU rules in the field of data protection. Knowing the basic concepts and institutions of data protection. Knowing the basic principles of data protection. Thorough knowledge of the rights of the data subject. Thorough knowledge of the data controller's responsibilities. Knowledge of data security procedures. Being familiar with the status, responsibility, jurisdiction, powers, and competence of the Hungarian National Authority for Data Protection and Freedom of Information (NAIH). Knows the practicies of certification and accreditation in the field of data protection.

Capabilities: Ability to idenfity if an activity qualifies as data processing and to specify the relevant processing operations and the personal data being processed. Ability to identify, in a professional manner, the legal basis and the purposes of the data processing. Ability to distinguish, in a professional manner, between the data controller and the processor. Being able to apply the procedural rules before the Hungarian National Authority for Data Protection and Freedom of Information in practice. Ability to identify, handle and notify personal data breaches.

Attitude: Finding important to have a strong knowledge of the legal, organizational, administrative and practical aspects of data protection. Seeks to identify, analyze and manage data protection risks. Strive to achieve a high level of privacy awareness. Finds it important to achieve the appropriate level of data security as effectively as possible. The student is open to study good practices that facilitate the implementation of the data controller's obligations.

Autonomy and responsibility: Responsible for learning and understanding the new EU data protection regime. Has the appropriate knowledge to implement data security measures. Able to eliminate risks, to assess relevant circumstances and to manage problems regarding the data processing.

11. Előtanulmányi követelmények: -

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

12.1. Az adatvédelmi jog kialakulása és helye a jogrendszerben (The formation and place of data protection law in the Hungarian legal regime);

12.2. A hazai adatvédelmi szabályozás általános bemutatása, különös tekintettel az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényre [a továbbiakban: Infotv.] (General overview of Hungarian data protection regulation, particularly Act CXII of 2011 on the right to informational self-determination and freedom of information [the Privacy Act]);

12.3. Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) [a továbbiakban: GDPR] általános bemutatása General overview of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [General Data Protection Regulation, GDPR]);

12.4. A GDPR és az Infotv. személyi, tárgyi és területi hatálya (The personal, material and territorial

scope of the GDPR and the Privacy Act);

12.5. Alapfogalmak, alapelvek (Definitions, principles);

12.6. Az adatkezelési jogalapok rendszerének bemutatása (Introduction to the system of legal bases for data processing);

12.7. Az érintetti jogok általános bemutatása (Introduction to the rights of data subjects);

12.8. Az elszámoltathatóság alapelvének részletes bemutatása (A detailed introduction to the principle of accountability);

12.9. Az elszámoltathatóság alapelvének való megfelelést segítő, GDPR-ban nevesített és GDPR-on kívüli eszközei (The means of compliance with the principle of accountability under and outside the GDPR);

12.10. Az adatkezelő feladatai (The duties of the data controller);

12.11. A beépített és alapértelmezett adatvédelem (Data protection by design and default);

12.12. Az adatkezelési tevékenységek nyilvántartása (Recording data processing activities);

12.13. Az adatvédelmi tisztviselő (The Data Protection Officer);

12.14. Az adatbiztonság (Data security);

12.15. Egyéb adatkezelői kötelezettségek általános ismertetése (adatvédelmi incidens bejelentése, adatvédelmi hatásvizsgálat) (General introduction to other data controller obligations (reporting a privacy breaches, data protection impact assessment));

12.16. A Nemzeti Adatvédelmi és Információszabadság Hatóság eljárásai (The proceedures of the Hungarian National Authority for Data Protection and Freedom of Information);

12.17. Akkreditáció és tanúsítás, magatartási kódexek, harmadik országba történő adattovábbítás (Accreditation, certification, codes of conduct, transfers of personal data to third countries or international organisations).

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:

Követelmény a tanórákon történő részvétel. Az elfogadható hiányzások mértéke 25%, az e feletti távolmaradás esetén a tantárgy oktatója által meghatározott feladatot szükséges teljesíteni (házidolgozat, kiselőadás).

15. Félévközi feladatok, ismeretek ellenőrzésének rendje:

Nincs félévközi feladat.

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

16.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele az előző pontban meghatározott arányú részvétel a foglalkozásokon.

16.2. Az értékelés:

A vizsga alapját a kötelező irodalom és az előadások anyaga képezi. Vizsga formája írásbeli. Az értékelés ötfokozatú: 0-50% - elégtelen, 51-70% - elégséges, 71-80% - közepes, 81-90% - jó, 91-100% - jeles.

16.3. A kreditek megszerzésének feltételei:

A kreditek megszerzésének feltétele az aláírás megszerzése és legalább elégséges kollokvium (K).

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. Bíró János et.al.: Jogalapok, érintetti jogok, NKE, Budapest, 2018;
2. Árvay Viktor György et.al.: Az elszámoltathatóság alapelve és az adatkezelői kötelezettségek, NKE, Budapest, 2018;
3. Sziklay Júlia – Bendik Tamás: Az adatvédelem hazai és európai uniós szabályozása és alapintézményei, NKE, Budapest, 2019;
4. Balogh Gyöngyi et.al.: Az adatvédelmi jog alapelvei, fogalmai, szereplői, profilalkotás, a személyes adatok különleges kategóriái, bűnügyi személyes adatok, NKE, Budapest, 2019

17.2. Ajánlott irodalom:

1. A Nemzeti Adatvédelmi és Információszabadság Hatóság általános adatvédelmi rendelettel kapcsolatos állásfoglalásai 2018, Magyar Közlöny Lap- és Könyvkiadó Kft., Budapest, 2019., ISBN 978-615-5710-64-3
2. A 29. cikk alapján létrehozott adatvédelmi munkacsoport véleményei és iránymutatásai;
3. Az Európai Adatvédelmi Testület (EDPB) véleményei, iránymutatásai;

Budapest, 2021.01.05.

Dr. Péterfalvi Attila, PhD,
egyetemi docens sk.

NEMZETI KÖZSZOLGÁLATI EGYETEM
Rendészettudományi Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** RBGVB109
2. **A tantárgy megnevezése (magyarul):** Bevezetés a kiberbiztonság szakterületi ismereteibe
3. **A tantárgy megnevezése (angolul):** Introduction to cybersecurity
4. **Kreditérték és képzési karakter:**
   - **4.1.** 5 kredit
   - **4.2.** a tantárgy elméleti vagy gyakorlati jellegének mértéke: 50% gyakorlat, 50% elmélet
5. **A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):** kiberbiztonsági MA
6. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** Rendészettudományi Kar, Bűnügyi, Gazdaságvédelmi és Kiberbűnözés Elleni Tanszék
7. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Muha Lajos, PhD, egyetemi docens
8. **A tanórák száma és típusa**

   8.1. össz óraszám/félév:

   8.1.1. nappali munkarend: 56 (28 EA + 28 GY)

   8.1.2. levelező munkarend: 16 (8 EA + 8 GY)

   8.2. heti óraszám - nappali munkarend: 4 (2 EA + 2 GY)

   8.3. Az ismeret átadásában alkalmazandó további sajátos módok, jellemzők: -
9. **A tantárgy szakmai tartalma (magyarul):** A hallgató megismeri a kiberbiztonság fogalmi alapjait, a kibernetika matematikai elméleteit és a biztonsgi modelljeit.

   A tantárgy szakmai tartalma (angolul) (Course description): Students will learn about the conceptual basics of cyber security, mathematical theories of cybernetics and security models.

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

Tudása: Tisztában van az állami kibervédelmi rendszerrel.

Képességei: Képes átlátni a kibertér speciális jogállását.

Attitűdje: Munkája során figyelembe veszi és alkalmazza a kiberbiztonsággal kapcsolatos jogszabályokat.

Autonómiája és felelőssége: Felelősséget vállal a kiberbiztonság összefüggő ismeretének és a meghatározó jogi, szabályozási és gazdasági összefüggések ismeretének alapján a szakmai javaslatok kidolgozásában.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: The cyber security system of the state.

Capabilities: Having an overview of the special legal status of cyberspace.

Attitude: His/her personal attitude is characterized by an attention to and application of laws of cyber security in his/her work.

Autonomy and responsibility: To take responsibility for making professional proposals based on comprehensive knowledge of cyber security and dominant legal, regulatory and economical processes.

11. Előtanulmányi követelmények: -

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

12.1. Bevezetés (Introduction);

12.2. Az információs rendszerek fenyegetéseinek és védelmének fejlődése. (Development of threats and protection of information systems);

12.3. Alapfogalmak. A kibertér fogalma. A kiberfenyegetések. (Basic Concepts. The concept of cyberspace. Cyber threats);

12.4. Az informatikai rendszerek védelme 90-es évekig az USA-ban. Az informatikai rendszerek védelme 90-es évek után a világban. (Protecting IT Systems in the US in the 90s. Protecting IT Systems in the World after the 90s);

12.5. Az informatikai rendszerek védelme 90-es évekig az Magyarországon. Az informatikai rendszerek védelme 90-es évek után Magyarországon. A vonatkozó hazai jogszabályok (Protection of IT systems in Hungary in the 1990s. Protection of IT systems in Hungary after the 1990s. Relevant domestic law);

12.6. Az információbiztonság alapvető fogalmai (Basic concepts of information security);

12.7. A kibernetika megjelenése a tudományok között. (The emergence of cybernetics among the sciences);

12.8. A kibernetika tartalma (Content of cybernetics);

12.9. A rendszerelmélet (System theory);

12.10. A matematikai modellezés (Mathematical modeling;);

12.11. A játékelmélet (Game theory);

12.12. Az információelmélet (Information Theory;);

12.13. Számítógép védelmi modellek (Computer security models);

12.14. Az ISO/IEC 27xxx sorozat (The ISO / IEC 27xxx series);

12.15. Az ISO/IEC 27001 (Információbiztonsági Irányítási Rendszer) (ISO / IEC 27001 (Information Security Management System);

12.16. PDCA-modell;

12.17. Információbiztonsági menedzsment alapvetései (Basics of Information Security Management);

12.18. Összefoglalás (Summary).

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:

Nincs félévközi feladat.

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

16.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele az előző a meghatározott arányú részvétel a foglalkozásokon.

16.2. Az értékelés:

A félév értékelése kollokvium – írásbeli és szóbeli vizsga. A Tanszék felkészülési kérdéseket ad ki. A vizsga értékelése szummatív: 0-50% - elégtelen, 51-70% - elégséges, 71-80% - közepes, 81-90% - jó, 91-100% - jeles.

16.3. A kreditek megszerzésének feltételei:

A kreditek megszerzésének feltétele az aláírás megszerzése és legalább elégséges kollokvium (K).

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. Muha Lajos, Krasznay Csaba: Az elektronikus információs rendszerek biztonságának menedzselése, Budapest, 2018, Nemzeti Közszolgálati Egyetem, ISBN 978-615-5870-27-9;
2. Kovács László: A kibertér védelme, Budapest, 2018, Dialóg Campus Kiadó, ISBN 978-615-5889-63-9 (nyomtatott) ISBN 978-615-5889-64-6 (elektronikus).

17.2. Ajánlott irodalom:

1. Singer, P. W., Friedman, Allen: Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, 2014. ISBN: 0199918112;
2. Brown, Lawrie, Stalling, William: Computer Security: Principles and Practice, Pearson, 2018. (4. kiadás) ISBN 978-0134794105.

Budapest, 2021.01.05.

Dr. Muha Lajos, PhD,
egyetemi docens sk.

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. László Gábor, 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, 2021.01.05.

Dr. László Gábor, PhD,
egyetemi docens sk.

NEMZETI KÖZSZOLGÁLATI EGYETEM
Hadtudományi és Honvédtisztképző Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** HKHIRA56
2. **A tantárgy megnevezése (magyarul):** Biztonsági tesztelés
3. **A tantárgy megnevezése (angolul):** Security testing
4. **Kreditérték és képzési karakter:**
   - **4.1.** 3 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:** Hadtudományi és Honvédtisztképző Kar, Híradó Tanszék
7. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Tóth András, PhD, adjunktus
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 informatikai rendszerek biztonsági tesztelése tervezésének, végrehajtásának és a vizsgálatok dokumentálásának ismertetése a hallgatókkal. Laborgyakorlatok során a hallgatók elsajátítják a biztonsági tesztlabor tervezésének és kialakításának lépéseit (virtualizációs technológia, célpont és biztonsági tesztelő munkaállomások bemutatásán keresztül). Elsajátítják az IT rendszerek biztonsági tesztelésének különböző módszertanait (OWASP, PCI, OSSTMM), a sérülékenység keresés típusait (blackbox, whitebox, greybox), és a végrehajtásuk lépéseit. Megismerik az informatikai rendszerek fejlesztése, rendszerbe integrálása, üzemelésének ellenőrzése során alkalmazható biztonságtesztelő módszerek fő típusait (kód audit, fuzzing, stress testing, usability testing, stb.). Gyakorlati ismereteket kapnak a biztonsági eszközök vizsgálatának lehetőségeiről (hálózati és kliens oldali védelmi megoldások tesztelésének módszereit), a hálózati támadások „klasszikus" életciklusáról (felderítés, célpont azonosítás, védelmi technológiák kikerülése, támadás végrehajtása, tevékenység rejtése, későbbi hozzáférés biztosítása, újabb célpontok azonosítása és kompromittálása), helyi és távoli sérülékenység keresés és kihasználás módszerekről. Megismerik az automatizált sérülékenység keresés szerepét, előnyeit és hátrányait, az eredmények értelmezésének és validálásának lépéseit, az alkalmazások és szolgáltatások tesztelésének lehetőségeit Windows és Linux operációs rendszereken, webszolgáltatások és adatbázisok biztonsági tesztelését, a felhasználói biztonságtudatossági vizsgálatokat (technikai social engineering támadások), a vezetéknélküli rendszerek tesztelésének módszertanát (a 802.11 szabványcsalád, Bluetooth család, RFID, mobil technológiákon keresztül), a beágyazott rendszerek vizsgálatának lehetőségeit, a mobil eszközök (okoseszközök) tesztelésének lehetőségeit, illetve a biztonsági tesztelő csapat kommunikációjának, és a vizsgálatok dokumentálásának lehetőségeit (technikai mérési eredmények megosztásának, feldolgozásának és bemutatásának módszereit), valamint a továbbképzés és önképzés egyéni és csoportos lehetőségeit (tanfolyamok, elearning anyagok, certificate-ek, CTF-ek, kiberbiztonsági gyakorlatok).

A tantárgy szakmai tartalma (angolul) (Course description): The aim of the course is to introduce to the students the planning, implementation and documentation of security testing of information systems. During lab exercises students will learn the steps of designing and building a security test labs (through demonstration of virtualization technology, target and security test workstations). They learn the different methods of security testing of IT systems (OWASP, PCI, OSSTMM), the types of vulnerability search (blackbox, whitebox, greybox) and the steps of their implementation. They learn about the main types of security testing methods (code audit, fuzzing, stress testing, usability testing, etc.) that can be used in the development, integration and operation of IT systems. They will gain practical insights into how to scan security tools (methods for testing network and client-side security solutions), the "classic" lifecycle of network attacks (discovery, target identification, security technology evasion, attack execution, hide activity, new targets identification and compromising), local and remote vulnerability discovery and exploitation techniques. Get knowledge about the role, advantages and disadvantages of automated vulnerability search, steps to interpret and validate results, how to test applications and services on Windows and Linux operating systems, security testing of Web services and databases, user security awareness tests (technical social engineering attacks), wireless systems testing methodologies (via 802.11 family of standards, Bluetooth family, RFID, mobile technologies), testing capabilities of embedded systems, testing of mobile devices (smart devices), possible communication capabilities of the security testing team, and documentation of testing (technical measurement results sharing, processing and presentation methods), as well as individual and group advanced studies possibilities (courses, elearning materials, certificates, CTFs, cyber security exercises).

10. Elérendő kompetenciák (magyarul):

Tudása: Ismeri a kibertámadás esetén alkalmazandó eljárásokat.

Képességei: Képes támogatni szervezetét a kibervédelmi képességek kialakításában.

Attitűdje: Hatékony lépéseket tesz a kibertámadások megelőzése érdekében, így csökkentve a szervezete kitettségét.

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

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: Is familiar with the procedures applicable in case of a cyber attack.

Capabilities: Is capable of supporting his/her organisation in developing cyber security skills.

Attitude: 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.

Autonomy and responsibility: To put the results of scientific research in the field into his/her practice.

11. Előtanulmányi követelmények: Információs rendszerek és hálózatok biztonsága [HKHIRA55]

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

12.1. Biztonsági tesztlabor tervezésének és kialakításának lépései (Steps to design and build a security test lab);

12.2. IT rendszerek biztonsági tesztelésének különböző módszertanai (Different methodologies for security testing of IT systems);

12.3. Biztonságtesztelő módszerek fő típusai (The main types of security testing methods);

12.4. Biztonsági eszközök vizsgálatának lehetőségeiről (Opportunities for testing security devices);

12.5. Biztonsági funkcionális tesztelés (Functional safety testing);

12.6. Sérülékenység-vizsgálat (Vulnerability testing);

12.7. Behatolás tesztelés (Penetration testing);

12.8. Helyi és távoli sérülékenység keresés és kihasználás (Local and remote vulnerability discovery and exploitation);

12.9. Alkalmazások és szolgáltatások tesztelésének lehetőségei (Opportunities for testing applications and services);

12.10. Webszolgáltatások és adatbázisok biztonsági tesztelése (Security testing of web services and databases);

12.11. Felhasználói biztonságtudatossági vizsgálatok (User safety awareness tests);

12.12. Vezetéknélküli rendszerek tesztelésének módszertana (Methodology for testing wireless systems);

12.13. Mobil eszközök (okoseszközök) tesztelésének lehetőségei (Opportunities for testing mobile devices (smart devices));

12.14. Beágyazott rendszerek vizsgálatának lehetőségei (Possibilities of testing embedded systems);

12.15. Továbbképzés és önképzés egyéni és csoportos lehetőségei (Individual and group opportunities for further education and self-education).

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 hallgató köteles az elméleti és gyakorlati foglalkozások legalább 75 %-án részt venni. Amennyiben a hallgató valamilyen igazolt okból nem tud részt venni a foglalkozásokon, azokat előre egyeztetett időpontban a szorgalmi időszak alatt egy alkalommal pótolhatja.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A gyakorlati feladat az oktatás során alkalmazott hálózatbiztonsági szoftver által végrehajtandó a témaköröket átfogóan érintő biztonsági tesztelő feladat végrehajtása.

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

16.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele a a gyakorlati feladat legalább elégséges (minimum 60%-os) szintű abszolválása. Továbbá az aláírás megszerzésének feltétele a gyakorlati foglalkozásokon való legalább 75%-os részvétel.

16.2. Az értékelés:

A gyakorlati feladat értékelése ötfokozatú skálán történik, az elégséges szint eléréséhez legalább 60%-ot kell teljesíteni. (60 %-tól elégséges, 70 %-tól közepes, 80-tól % jó, 90 %-tól jeles).

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. Frész Ferenc, Kálovics Tamás, Puha Gábor: Hálózatok Biztonsága NKE, 2014. ÁROP –2.2.21 Tudásalapú közszolgálati előmenetel;
2. Tihanyi Norbert, Vargha Gergely, Frész Ferenc: Biztonsági tesztelés a gyakorlatban, NKE, 2014. ÁROP –2.2.21 Tudásalapú közszolgálati előmenetel, ISBN 978-615-5491-59-7;

17.2. Ajánlott irodalom:

1. Hertzog, Raphael, O'Gorman, Jim (2017): Kali Linux Revealed: Mastering the Penetration

Testing Distribution. Offsec Press, ISBN 978-0997615609;
2. Kim, Peter (2018): The Hacker Playbook 3: Practical Guide To Penetration Testing. ISBN 978-1980901754;
3. OWASP ajánlás;
4. RTFM - Red Team Field Manual;
5. Sérülékenység keresési link gyűjtemények;
6. PCI Data Security Standard (PCI DSS) - Information Supplement:Penetration Testing Guidance
7. Open Source Security Testing Methodology Manual – OSSTMM

Budapest, 2021.01.05.

Dr. Tóth András, PhD,
adjunktus sk.

NEMZETI KÖZSZOLGÁLATI EGYETEM
Hadtudományi és Honvédtisztképző Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** HHKNBTTMA03
2. **A tantárgy megnevezése (magyarul):** Biztonságpolitika
3. **A tantárgy megnevezése (angolul):** Security policy
4. **Kreditérték és képzési karakter:**
   - **4.1.** 3 kredit
   - **4.2.** a tantárgy elméleti vagy gyakorlati jellegének mértéke: 0% gyakorlat, 100% elmélet
5. **A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):** kiberbiztonsági MA
6. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** Hadtudományi és Honvédtisztképző Kar, Nemzetközi Biztonsági Tanulmányok Tanszék
7. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Molnár Anna, PhD, egyetemi tanár
8. **A tanórák száma és típusa**
   - **8.1.** össz óraszám/félév:
   - 8.1.1. nappali munkarend: 28 (28 EA + 0 GY)
   - 8.1.2. levelező munkarend: 8 (8 EA + 0 GY)
   - **8.2.** heti óraszám - nappali munkarend: 2 (2 EA + 0 GY)
   - **8.3.** Az ismeret átadásában alkalmazandó további sajátos módok, jellemzők: -
9. **A tantárgy szakmai tartalma (magyarul):** A tantárgy elsődleges célja, hogy a képzésében részt vevő hallgatók számára megfelelő elméleti alapismeretek elsajátítását biztosítsa a biztonságpolitika, a biztonsági tanulmányok területén. A hallgatók ismereteket szereznek a biztonsági tanulmányok alapjairól, a nemzetközi kapcsolatokról és intézményrendszerről, továbbá megismerkednek a konfliktusok lokális, regionális és globális vonatkozásaival. Ezen túlmenően a kurzus során kiemelt figyelmet fordítunk a biztonság különböző szektorainak működésére, az új típusú biztonság kihívások megjelenésére és azok következményeire. A hallgatók ennek keretében betekintést kapnak a kiberbiztonság aktuális kérdéseibe, illetve a kibertérben fellépő veszélyek természetébe.

   A tantárgy szakmai tartalma (angolul) (Course description): The primary objective of the course is to provide a comprehensive understanding of the security policy and security studies. Students will learn the basic concepts of security studies, international relations and institutional system and will learn about the local, regional and global aspects of conflict. In addition, the course focuses on the functioning of different security sectors, the emergence of new types of security challenges and their consequences. In this context, the course focuses on current issues in cyber security and the nature of cyber threats.

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

Tudása: Átlátja a kibertérrel kapcsolatos diplomáciai, illetve politikai információmegosztás folyamatát, valamint az esetleges válaszlépéseket.

Képességei: Képes a keletkezett információk megosztásának szükségességével kapcsolatban komplex következtetések levonására.

Attitűdje: Megérti és elfogadja a nemzetközi kiberjog komplexitását, ennek köszönhetően a munkája során törekszik ennek a komplexitásnak a kezelésére.

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

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: He/she is familiar with the procedure of diplomatic and political information sharing related to cyberspace, as well as possible responses.

Capabilities: He/she is capable of drawing complex conclusions in terms of the necessity of sharing information.

Attitude: his/her personal attitude is characterized by An understanding and acceptance of the complexity of international cyber law and thus strives to handle this complexity in his/her work.

Autonomy and responsibility: Having autonomy and responsibility to put the results of scientific research in the field into his/her practice.

11. Előtanulmányi követelmények: -

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

12.1. Bevezetés (Introduction);

12.2. Biztonságpolitika (Security Policy);

12.3. Fogalmi keretek (Conceptual framework);

12.4. Főbb nemzetközi biztonsági szervezetek I. (Major international security organizations I.);

12.5. Főbb nemzetközi biztonsági szervezetek II. (Major international security organizations II.);

12.6. Főbb nemzetközi biztonsági szervezetek III. (Major international security organizations III.);

12.7. Főbb nemzetközi biztonsági szervezetek IV. (Major international security organizations IV.);

12.8. A biztonság szektorai I. (Security Sectors I.);

12.9. A biztonság szektorai II. (Security Sectors I.);

12.10. A biztonság szektorai III. (Security Sectors II.);

12.11. A kiberbiztonság aktuális kérdése (Current issues of cyber security);

12.12. Új típusú biztonság kihívások I. (New security challenges I.);

12.13. Új típusú biztonság kihívások II. (New security challenges II.);

12.14. Zárthelyi dolgozat (End-of-term writing test);

12.15. Zárthelyi dolgozat javítás (End-of-term writing test (correction)).

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 hallgató köteles a foglalkozások legalább 75 %-án részt venni. Az igazolatlan hiányzás nem pótolható. 25% feletti igazolatlan hiányzással az aláírás megtagadásra kerül.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A feladatok pótlása a tárgyfelelőssel egyeztetve történik.

A zárthelyi dolgozat esetében az értékelés a hallgató által elért pontok alapján a következő módon történik:

0-50% = elégtelen (1)

51%-62,5%= elégséges (2)

63%-75% = közepes (3)

76%- 87,5%= jó (4)

88%-100 = jeles (5)

Megajánlott jegy adható a zárthelyi dolgozatok végeredménye alapján (a kapott jegyek átlaga). A megajánlott jegy feltétele az aláírás megszerzése és legalább elégséges zárthelyi dolgozati eredmények.

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

16.1. Az aláírás megszerzésének feltételei:

Az aláírás feltétele a foglakozásokon legalább 75%-os részvétel.

16.2. Az értékelés:

A vizsga követelménye a tanórákon átadott ismeretekre és a kötelező irodalomra épül. A zárthelyi dolgozatok és az írásbeli kollokvium esetében az értékelés a hallgató által elért pontok alapján a következő módon történik:

0-50% = elégtelen (1)

51%-62,5%= elégséges (2)

63%-75% = közepes (3)

76%- 87,5%= jó (4)

88%-100 = jeles (5)

A zárthelyi dolgozatok eredménye alapján megajánlott jegy kapható.

16.3. A kreditek megszerzésének feltételei:

A kreditek megszerzésének feltétele az aláírás megszerzése és legalább elégséges kollokvium (K).

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. Gazdag Ferenc – Remek Éva: A biztonsági tanulmányok alapjai. Budapest. Dialóg Campus Kiadó. 2018. ISBN 9786155845871;
2. Egedy Gergely: Bevezetés a nemzetközi kapcsolatok elméletébe. Budapest. HVG-ORAC. 2011. ISBN 9789632581361;
3. Molnár Anna: Az Európai Unió külkapcsolati rendszere és eszközei: a külkapcsolatoktól a kül- , a biztonság- és védelempolitikáig, Budapest, Magyarország : Dialóg Campus Kiadó (2018) , 326 p. ISBN: 9786155877070;
4. Gärtner, Heinz: Nemzetközi biztonság - Fogalmak A-tól Z-ig. Zrínyi Kiadó, Budapest, 2007. ISBN 9789633274439;
5. Gazdag Ferenc (szerk.): N. Rózsa Erzsébet-Péczeli Anna (szerk.): Egy békésebb világ eszközei. Fegyverzetellenőrzés, leszerelés, non-proliferáció. Osiris-MKI, Budapest, 2013. ISBN 97896338994894.

17.2. Ajánlott irodalom:

1. Steve Tulliu, Steve – Thomas Schmalberger: A biztonság megértése felé. Genf – Budapest. UNIDIR-SVKK. 2003. ISBN 9638117907;
2. Diplomáciai lexikon, A nemzetközi kapcsolatok kézikönyve. Budapest, Éghajlat Könyvkiadó. 2018. ISBN 9789639862142;
3. Prandler Árpád, Blahó András: Nemzetközi szervezetek és intézmények, Akadémiai Kiadó, 2014. ISBN: 9789630595278.

Budapest, 2021.01.05.

Dr. Molnár Anna, PhD,
egyetemi tanár sk.

NEMZETI KÖZSZOLGÁLATI EGYETEM
Államtudományi és Nemzetközi Tanulmányok Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** ÁKINTM13
2. **A tantárgy megnevezése (magyarul):** Biztonságtechnika
3. **A tantárgy megnevezése (angolul):** Physical Security
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):** 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. László Gábor, PhD, egyetemi docens
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 hallgatók megismerik a komplex vagyonvédelem fogalmát, felépítését, összetevőit, valamint az elemeinek egymásra épülését. Ezen belül bemutatásra kerülenek a mechanikai védelem elemei és eszközei (falazat, nyílászárók, zárak, rácsok, kerítések). Részletesen foglalkoznak az elektronikus vagyonvédelem területeivel és az integrált vagyonvédelem kialakításával, így a behatolás-jelző rendszerek felépítésével, eszközeivel (pl. behatolásjelző-rendszerek, passzív infravörös mozgásérzékelő, Reed-relé, üvegtörés-érzékelő). Bemutatásra kerülnek a video felügyeleti (CCTV) rendszerek alkalmazási területei, jogi hátterük. Megismerkednek a tűzjelző rendszerek felépítésével, funkcióival, fajtáival és tűzjelző érzékelőkkel (pontszerű füstérzékelő, aspirációs, hősebesség-érzékelő, optikai érzékelők).

   A tantárgy szakmai tartalma (angolul) (Course description): Students will learn about the concept, structure, components and complexity of complex physical asset protection. Within this, the elements and tools of mechanical protection (masonry, windows, locks, lattices, fences) are presented. The course deals in detail with the areas of electronic security and the development of integrated security, such as the intrusion detection systems and devices (eg intrusion detection systems, passive infrared motion detector, Reed relay, glass break detector). Applications of video surveillance (CCTV) systems and their legal background will be introduced. They get acquainted with the structure, functions, types and fire detectors of fire alarm systems (point smoke detector, aspiration, heat speed detector, optical detector) and enry control systems.

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

Tudása: Ismeri a fizikai védelem eszközredszerét.

Képességei: Képes támogatni szervezetét a kibervédelmi képességek kialakításában.

Attitűdje: Megérti a fizikai biztonság szerepét a komplex információbiztonságban.

Autonómiája és felelőssége: Mindig figyelemmel követi a fizikai kockázatokat.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: Knows the pysical security controls.

Capabilities: Supporting his/her organisation in developing cyber security skills.

Attitude: An understanding and acceptance of the phisical security in the complex information security.

Autonomy and responsibility: Always aware of physical risks.

11. Előtanulmányi követelmények: -

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

12.1. A komplex vagyonvédelem fogalma, felépítése, összetevői, egymásra épülésük (Complex security: elements and their interconnection);

12.2. Mechanikai védelem elemei (Mechanical protection);

12.3. Az elektronikus vagyonvédelem területei. (Fields of electronic protection);

12.4. Behatolás-jelző rendszerek (Burglar alarm systems);

12.5. Behatolás-jelző érzékelők (Burglar alarm sensors);

12.6. Tűzjelző rendszerek működésének fizikai alapjai: tűzjellemzők, füstterjedés (Physical basics of fire alarm systems);

12.7. Tűzjelző központok kialakítása (Implementation of fire alarm systems);

12.8. Tűzjelző érzékelők: pontszerű érzékelés (Fire alarm sensors: point sensing);

12.9. Tűzjelző érzékelők: térbeli érzékelés (Fire alarm sensors: area sensing);

12.10. Beépített automatikus oltórendszerek kiválasztása (Fire suppression system selection);

12.11. Video felügyeleti (CCTV) rendszerek eszközei (CCTV devices);

12.12. Video felügyeleti (CCTV) rendszerek kialakítása (CCTV implementation);

12.13. Video felügyeleti (CCTV) rendszerek alkalmazási területei, jogi hátterük (CCTV applications and legal compliance);

12.14. Beléptető rendszerek fajtái, funkcióik, felépítésük (Entry control system types and functions).

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 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. Berek Lajos: Biztonságtechnika. Budapest: NKE, 2014. ISBN 9786155491511.
2. Lukács Gy., Gábor L. (szerk.) et al: Új Vagyonvédelmi Nagykönyv. Cedit 2000 Kft., Budapest, 2002. ISBN 963-8180-39-0
3. Tóth Levente: CCTV magyarul. BM Nyomda, Budapest, 2003. ISBN 963 217 074 1

17.2. Ajánlott irodalom:

1. Knoke, Michael E., Peterson, Kevin E. (eds.): Physical Security Principles. ASIS International, 2015. ISBN 978-1934904619.

Budapest, 2021.01.05.

Dr. László Gábor, PhD,
egyetemi docens sk.

NEMZETI KÖZSZOLGÁLATI EGYETEM
Rendészettudományi Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** RBGVB111
2. **A tantárgy megnevezése (magyarul):** Digitális nyomrögzítés
3. **A tantárgy megnevezése (angolul):** Digital Forensics
4. **Kreditérték és képzési karakter:**
   - **4.1.** 3 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:** Rendészettudományi Kar, Bűnügyi, Gazdaságvédelmi és Kiberbűnözés Elleni Tanszék
7. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Nagy Zoltán András, 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 biztonságot sértő bűncselekmények, incidensek felderítéséhez nélkülözhetetlen az ezt bizonyító elektronikus adatok jogszerű, szakszerű rögzítése, ahogy ennek a kriminológiai és kriminalisztikai tudásanyaga.

   A tantárgy szakmai tartalma (angolul) (Course description): In order to detect crimes and incidents that violate security, it is indispensable to lawfully and professionally record electronic data proving this, as well as knowledge of criminal procedure and criminalistics.

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

Tudása: Tisztában van a nyomozóhatóság feladataival az egyes állami szervezetek, vállalatok és intézményeket érő támadások esetén.

Képességei: Képes együttműködni a nyomozóhatósággal a kiberbiztonsági eseményeket érintő nyomozások során.

Attitűdje: Hatékony lépéseket tesz a kibertámadások megelőzése érdekében, így csökkentve a szervezete kitettségét.

Autonómiája és felelőssége: Vállalja a kiberbiztonsági fenyegetések kezelésének felelősségét.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: The tasks of investigative authorities in case of attacks against state organs, enterprises and institutions.

Capabilities: Cooperating with investigative authorities in investigations of cyber security incidents.

Attitude: An effort to take effective measures in order to prevent cyber attacks, by this means reducing the exposure of his/her organisation.

Autonomy and responsibility: To handle cyber security threats.

11. Előtanulmányi követelmények: Kiberbűnözés [RBGVB110]

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

12.1. A bizonyíték és bizonyítási eszköz fogalma (The concept of evidence and means of proof);

12.2. Az elektronikus adat - digitális adat fogalma jogban (Concetpt of electronic data and digital data in law);

12.3. A bizonyítékok forrásai a kibertérben (Sources of evidence in cyberspace);

12.4. Digitális eszközök ismerete (Knowledge of digital devices)

12.5. Hálózati ismeretek I. A helyhez kötött hálózati szolgáltatások (Networking Knowledge I. Fixed Network Services)

12.6. Hálózati ismeretek II. A mobilhálózatok (Networking Knowledge II. Mobile networks)

12.7. Az OSINT szerepe, terepe a kibertérben (The role and field of OSINT in cyberspace);

12.8. A számítógépben, kibertérben kutatásra vonatkozó jogi rendelkezések (Legal Provisions of resaerch in computer and cyberspace);

12.9. A lefoglalásra vonatkozó jogi rendelkezések (Legal provisions on seizure);

12.10. A megőrzésre kötelezés intézménye (Preservation for large databases);

12.11. A jogellenes szerzett bizonyítékokra vonatkozó rendelkezések (Provisions concerning evidence obtained unlawfully);

12.12. A szakértők szerepe, segítsége (Role and assistance of experts);

12.13. A digitális nyomrögzítés krimináltechnikai és kriminálmetodika kérdései (Issues of digital forensic and criminal methodology of digital tracking).

13. A tantárgy meghirdetésének gyakorisága/a tantervben történő félévi elhelyezkedése: 3. félév

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

A hallgató köteles a foglalkozások legalább 75%-án részt venni. Igazolt hiányzás esetén a részvétel a tanárral való egyeztetés alapján meghatározott házi dolgozat készítésével pótolható.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje:

Zárthelyi dolgozat a bizonyítékokról, bizonyítékok forrásairól, az elektronikus - digitális adatok témakörből.

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

16.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele a meghatározott arányú részvétel a foglalkozásokon.

16.2. Az értékelés:

A tematikában szereplő témákból 20 ezer karakternyi írásbeli záródolgozat. A zárthelyi dolgozat és az önállóan készített záródolgozat két érdemjegye alapján kerül az ötfokozatú értékelés kialakítva.

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. Goricsán Tamás: A kényszerintézkedések végrehajtásának sajátosságai a számítástechnikai eszközök felhasználásával megvalósított bűncselekmények nyomozása körében. In: Informatika és büntetőjog (szerkesztette: Gál István – Nagy Zoltán András). Pécs, 2006. 72 – 83..o. ISBN 978—963-642-115-1.;
2. Máté István Zsolt: A bizonyítékok kezelése: Az igazságügyi informatikai szakértő a büntetőeljárásban. Magyar Rendészet XIV.évf. 2014. 2. sz. 29-38. o. ISSN 1416-5511

17.2. Ajánlott irodalom:

1. Simon Béla: A bűnüldözés előtt álló digitális kihívások, In. MAGYAR RENDÉSZET 17 : 5 pp. 83-105. , 23 p. (2017);
2. Luttgens, Jason T., Pepe, Matthew, Mandia, Kevin (2014): Incident Response & Computer Forensics, Third Edition. McGraw-Hill Education, ISBN 978-0071798686;
3. Du, Xiaoyu, Le-Khac, Nhien-An: Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service, In. Conference: 16th European Conference on Cyber Warfare and Security (ECCWS 2017), At: Dublin, Ireland;
4. Holtet. al. Cybercrime and Digital Forensics: An Introduction. vol. Second edition, Routledge, 2018.

Budapest, 2021.01.05.

Dr. Nagy Zoltán András, PhD,
egyetemi docens sk.

NEMZETI KÖZSZOLGÁLATI EGYETEM
Hadtudományi és Honvédtisztképző Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** HKKNBM05
2. **A tantárgy megnevezése (magyarul):** Hírszerzés a kibertérben
3. **A tantárgy megnevezése (angolul):** Intelligence in cyberspace
4. **Kreditérték és képzési karakter:**
   - **4.1.** 3 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:** Hadtudományi és Honvédtisztképző Kar, Katonai Nemzetbiztonsági Tanszék
7. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Magyar Sándor, PhD, adjunktus
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):** Az előadás bemutatja a hírszerzés önálló ágait, a nyílt forrású adatszerzés helyét és szerepét. A hallgató megismeri a nyílt forrású adatszerzés alapfogalmait, a nyílt forrású adatszerzés forrásai, valamint a nyílt forrású adatszerzés módszereit (gyűjtés, keresés, analizálás). Bemutatásra kerül az OSINT technikai eszközrendszere, a keresőmotorok lehetőségei. A hallgató megismeri a közösségi média hírszerzésben betöltött szerepét, a digitális helymeghatározás lehetőségeit, a digitális információk metaadatainak tartalomelemzését. A gyakorlat során felhasználásra kerülnek a nyílt forrású adatszerzésben használható ingyenes szoftverek.

   A tantárgy szakmai tartalma (angolul) (Course description): The lecture introduces the individual types of intelligence, and the place and role of open source intelligence. The student will get to know the basic concepts of open source intelligence and the methods of open source intelligence (collecting, searching, analysing). OSINT's technical tools and search engine capabilities will be introduced. Students will learn about the role of social media in intelligence, the possibilities of digital positioning, and content analysis of digital information metadata. This exercise will use free software for open source data mining.

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

Tudása: Ismeri a fedett környezetből történő információgyűjtés eljárásait.

Képességei: Képes a szükséges mértékben alkalmazni a nyílt forrású adatszerzés eljárásait.

Attitűdje: Megérti és elfogadja a interneten megjelenő adatok komplexitását, kereshetőségét, ennek köszönhetően a munkája során törekszik ennek a komplexitásnak a kezelésére.

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

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: He/she is familiar with the procedures of covert information gathering.

Capabilities: Is capable of applying open source intelligence procedures to the necessary extent.

Attitude: He/she is understanding and acceptance the complexity and searchability of the data appearing on the Internet, thanks to which she strives to deal with this complexity in her work.

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. Hírszerzés önálló ágai, a nyílt forrású adatszerzés helye szerepe (Intelligence independent branches, the role of Open Source Intelligence);

12.2. Nyílt forrású adatszerzés alapfogalmai (Basic concepts of Open Source Intelligence);;

12.3. Nyílt forrású adatszerzés forrásai (Source of Open Source Intelligence);

12.4. Nyílt forrású adatszerzés módszerei (gyűjtés, keresés, analizálás) (Open Source Intelligence methods (collecting, searching, analyzing));

12.5. OSINT technikai eszközrendszere (OSINT technical toolset);

12.6. Gyakorlat 1. (practical course 1.);

12.7. Keresőmotorok lehetőségei (Search engine possibilities);

12.8. Gyakorlat 2. (practical course 2.);

12.9. Közösségi média, helymeghatározás, képek tartalma (Social media, positioning, image content);

12.10. Gyakorlat 3. (practical course 3.);

12.11. Nyílt forrású adatszerzésben használható ingyenes szoftverek (Free software for Open Source Intelligence);

12.12. Gyakorlat 4. (practical course 4.);

12.13. Gyakorlat 5. (practical course 5.);

12.14. Gyakorlat 6. (practical course 6.).

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 tantárgy elfogadásához a tanórák legalább 70 %-án jelen kell lennie a hallgatónak. A távollétet a hiányzást követő első foglalkozáson kell igazolnia. Hiányzás esetén a hallgató köteles az előadás anyagát beszerezni, abból önállóan felkészülni.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A tanulmányi munka alapja a szemináriumok látogatása, az előírt olvasmányok ismerete. A hallgató a félév során kettő feleletválasztós tesztet ír. Az elérendő teljesítmény százaléka 60 %-tól elégséges, 70 %-tól közepes, 80-tól % jó, 90 %-tól jeles. A félév végén egy vizsgafeladat gyakorlati megvalósítása. A félévközi feladatok összesítéséből áll a gyakorlati jegy. A TVSZ rendezi a sikertelen értékelés-összetevő javítását.

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

16.1. Az aláírás megszerzésének feltételei:

A foglalkozásokon való részvétel meghatározott aránya, illetve a félévközi feladatok teljesítése.

16.2. Az értékelés:

A gyakorlati jegy a 2 félévközi feleltválasztós teszt értékeléséből és a vizsgafeladatra adott érdemjegyekből adódik.

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. Resperger István (szerk.) (2018): A nemzetbiztonság elmélete a közszolgálatban. Dialóg Campus, Budapest, ISBN 978-615-5845-65-9 (nyomtatott)ISBN 978-615-5845-66-6 (elektronikus);
2. NATO Open Source Intelligence Handbook.

17.2. Ajánlott irodalom:

1. Ferenczy Gábor Zoltán: Internet alapú nyílt információszerzés elvi rendszertechnikai megvalósítása: doktori (PhD) értekezés 2009.;
2. Bazzell, Michael (2018): Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information. CreateSpace Independent Publishing Platform. ISBN 978-1984201577.

Budapest, 2021.01.05.

Dr. Magyar Sándor, PhD,
adjunktus sk.

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, 2021.01.05.

Dr. Krasznay Csaba, PhD,
egyetemi docens sk.

NEMZETI KÖZSZOLGÁLATI EGYETEM
Hadtudományi és Honvédtisztképző Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** HKHIRA55
2. **A tantárgy megnevezése (magyarul):** Információs rendszerek és hálózatok biztonsága
3. **A tantárgy megnevezése (angolul):** Information system and network security
4. **Kreditérték és képzési karakter:**
   - **4.1.** 6 kredit
   - **4.2.** a tantárgy elméleti vagy gyakorlati jellegének mértéke: 50% gyakorlat, 50% elmélet
5. **A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):** kiberbiztonsági MA
6. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** Hadtudományi és Honvédtisztképző Kar, Híradó Tanszék
7. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Tóth András, PhD, adjunktus
8. **A tanórák száma és típusa**
   - **8.1.** össz óraszám/félév:
     - 8.1.1. nappali munkarend: 84 (42 EA + 42 GY)
     - 8.1.2. levelező munkarend: 24 (12 EA + 12 GY)
   - **8.2.** heti óraszám - nappali munkarend: 6 (3 EA + 3 GY)
   - **8.3.** Az ismeret átadásában alkalmazandó további sajátos módok, jellemzők: -
9. **A tantárgy szakmai tartalma (magyarul):** Átfogó ismeretek nyújtása a korszerű számítógépek felépítéséről, működéséről. Ismeretek átadása a számítógép-architektúrák, operációs rendszerek funkciói, belső szerkezete, működési elvei területén. Konkrét számítógép-rendszerek és operációs rendszerek dokumentációinak gyors megértésének elősegítése, üzemeltetési, konfigurálási, karbantartási feladatok gyors megtanulásának megalapozása. A hálózati infrastruktúra megismerése, hálózati protokollok és kommunikáció, a hálózatokhoz történő kapcsolódás, az OSI modell, a TCP/IP modell, az Ethernet szabvány, a hálózati réteg, a szállítási, az alkalmazási réteg funkcióinak, az IPv4 és az IPv6 címzés, az IP alhálózatok tervezésének és kialakításának bemutatása. Bevezetés a kapcsolt hálózatokba, kapcsolás (switching) alapja és beállítása, forgalomirányítási (routing) alapok, statikus forgalomirányítás, dinamikus forgalomirányítás, DHCP, IPv4 hálózati címfordítás (NAT). VLAN kialakítási, valamint forgalomirányítási lehetőségek, az IPv4 és IPv6 hozzáférés vezérlési listák konfigurálása és megvalósítása, különböző WAN technológiák jellemzőinek bemutatása, előnyeik meghatározása, a virtuális magánhálózatok (VPN) működésének leírása. Átfogó elméleti és gyakorlati ismereteket nyújtani a hálózati kapcsolatok beállítási és hibaelhárítási lehetőségeiben, különösen a hálózati diagnosztika, a hitelesítési és titkosítási protokollok alapjai, valamint a proxyk, tűzfalak alkalmazása vonatkozásában. A Windows és Linux operációs rendszerek hálózati szolgáltatásainak és beállításainak megismerése. A hálózati forgalomelemzés aktív és passzív módszereinek, a vezetéknélküli hálózatok működése vizsgálatának, az Ethernet szabványok összehasonlító mérésének, a hálózati eszközök (HUB, switch, router, tűzfal, proxy) működésének protokollanalizátor segítségével végzett vizsgálatának, a hálózati eszközök terheléses vizsgálatának, és a hálózati eszközök funkcionális vizsgálatának lehetőségeinek megismerése. IP forgalom titkosításának lehetőségeinek (hálózati, szállítási, alkalmazás rétegbeli lehetőségek) bemutatása. Tűzfalak típusainak és funkcióinak gyakorlati vizsgálata.

   A tantárgy szakmai tartalma (angolul) (Course description): Providing comprehensive

knowledge of the structure and operation of modern computers. Providing of knowledge in the field of computer architectures, operating system functions, internal structure, operating principles. Promote a quick understanding of specific documentation of computer and operating systems, and provide a basis for rapid learning of operation, configuration, and maintenance tasks. Understanding network infrastructures, network protocols and communications, network connectivity, OSI model, TCP / IP model, Ethernet standard, network layer functions, transport layer functions, IPv4 and IPv6 addressing, designing and setting up IP subnets, application layer functions. Introduction to switched networks, basics in configuration in switching, routing, static routing, dynamic routing, DHCP, IPv4 network address translation (NAT). Configuring and implementing IPv4 and IPv6 access control lists, demonstrating the features of various WAN technologies, defining their benefits, and describing how virtual private networks (VPNs) work. Provide comprehensive theoretical and practical knowledge of network connection setup and troubleshooting, especially network diagnostics, basics of authentication and encryption protocols, and the use of proxies and firewalls. Learn about network features and settings for Windows and Linux operating systems. Get knowledge about active and passive methods of network monitoring, testing of wireless networks, benchmarking of Ethernet standards, protocol analysis of network devices (HUB, switch, router, firewall, proxy), load testing of network devices, and network devices to explore the possibilities of functional testing. Showing IP traffic encryption capabilities (network, transport, application layer capabilities). Practical study of types and functions of firewalls.

10. Elérendő kompetenciák (magyarul):

Tudása: Ismeri a kártékony kódok fogalmát és hatásmechanizmusát.

Képességei: Képes átlátni a kibertér aktuális fenyegetéseit.

Attitűdje: 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: He/she is familiar with the concept and mode of action of malware codes.

Capabilities: Is capable of understanding the current threats of cyber space.

Attitude: His/her personal attitude is characterized by cooperation in preventing his/her organisation and him/herself from becoming a victim of a cyber attack.

Autonomy and responsibility: To put the results of scientific research in the field into his/her practice.

11. Előtanulmányi követelmények: -

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

12.1. Korszerű számítógépek felépítése, működése (Construction and operation of modern computers);

12.2. Operációs rendszerek funkciói, működési elvei (Functions and principles of operating systems);

12.3. Hálózati protokollok és kommunikáció, Ethernet szabvány (Network protocols and communications, Ethernet standard);

12.4. Hálózati és szállítási réteg (Network and transport layer);

12.5. Alkalmazási réteg (Application layer);

12.6. Kapcsolt hálózatok, a kapcsolás beállításainak alapjai (Switched networks, basics of switching settings);

12.7. VLAN-ok (VLANs);

12.8. A forgalomirányítás alapjai (The basics of routing);

12.9. Statikus, dinamikus forgalomirányítás (Static, dynamic routing);

12.10. Hozzáférés vezérlési listák, DHCP, IPv4 hálózati címfordítás (Access control lists, DHCP, IPv4 network address translation);

12.11. WAN technológiák jellemzői (Features of WAN technologies);

12.12. Virtuális magánhálózatok (VPN) működése (Operation of Virtual Private Networks (VPNs));

12.13. Hálózati diagnosztika, a hitelesítési és titkosítási protokollok alapjai (Network diagnostics, basics of authentication and encryption protocols);

12.14. A hálózat monitorozása, hálózati hibaelhárítás (Network monitoring, network troubleshooting);

12.15. Tűzfalak típusainak és funkcióinak gyakorlati vizsgálata (Practical study of types and functions of firewalls).

13. A tantárgy meghirdetésének gyakorisága/a tantervben történő félévi elhelyezkedése: 3. félév

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

A hallgató köteles az elméleti és gyakorlati foglalkozások legalább 75 %-án részt venni. Amennyiben a hallgató valamilyen igazolt okból nem tud részt venni a foglalkozásokon, azokat előre egyeztetett időpontban a szorgalmi időszak alatt egy alkalommal pótolhatja.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A gyakorlati feladat az oktatás során alkalmazott hálózati topológia tervező szoftver által végrehajtandó a témaköröket átfogóan érintő hálózattervezői feladat végrehajtása.

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

16.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele a zárthelyi dolgozat, illetve a gyakorlati feladat legalább elégséges (minimum 60%-os) szintű abszolválása. Továbbá az aláírás megszerzésének feltétele az elméleti és gyakorlati foglalkozásokon való legalább 75%-os részvétel.

16.2. Az értékelés:

A zárthelyi dolgozat és a gyakorlati feladat értékelése ötfokozatú skálán történik, az elégséges szint eléréséhez legalább 60%-ot kell teljesíteni. (60 %-tól elégséges, 70 %-tól közepes, 80-tól % jó, 90 %-tól jeles). A végső érdemjegy az így kapott két érdemjegy átlagszámításával kerül meghatározásra. A tantárgy jellegéből adódóan az x,5-ös átlagok esetében a gyakorlati jegy a súlyozott, így az határozza meg a végső érdemjegy eredményét.

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. Andrew S. Tanenbaum: Számítógép hálózatok [Computer Networks]; Panem Kft., 2013, 968 oldal; ISBN 9789635455294;
2. Andrew S. Tanenbaum: Számítógép-architektúrák Panem Kft., 2007, ISBN 9789635454570;
3. Petrényi József: TCP/IP – alapok I. és II. kötet http://mek.oszk.hu/08300/08374/;
4. Dr. Kónya László: Számítógép-hálózatok, LSI OMAK Alapítvány, 2002, 262 oldal, ISBN 96357722X;
5. James F. Kurose - Keith W. Ross: Számítógép-hálózatok működése, Panem Kiadó, 2008; 758 oldal; ISBN 9789635454983.

17.2. Ajánlott irodalom:

1. Brown, L., Stalling, W.: Computer Security: Principles and Practice, Pearson, 2018. (4. kiadás) ISBN 978-0134794105;
2. Borbély Balázs: Otthoni és irodai hálózatok zsebkönyve [Home and office network pocketbook], Jedlik Oktatási Stúdió, 2014, 186 oldal, ISBN: 9786155012266;
3. Joe Casad: Tanuljuk meg a TCP/IP használatát 24 óra alatt [Learn TCP / IP over 24 hours], Kiskapu, 2010, 448 oldal, ISBN 9789639637689;
4. Ciprian Adrian Rusen: Számítógépes eszközök hálózatba kötése lépésről lépésre [Networking of computer devices step by step], Szak Kiadó, 2011, 474 oldal, ISBN 9789639863217;
5. Gál Tamás - Szabó Levente - Szerényi László: Rendszerfelügyelet rendszergazdáknak [System Administration for Administrators]; Szak Kiadó, 2007; 416 oldal; ISBN 978-963-9131-98-9.

Budapest, 2021.01.05.

Dr. Tóth András, PhD,
adjunktus sk.

NEMZETI KÖZSZOLGÁLATI EGYETEM
Államtudományi és Nemzetközi Tanulmányok Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** ÁLLTM07
2. **A tantárgy megnevezése (magyarul):** Jogi és közigazgatási ismeretek
3. **A tantárgy megnevezése (angolul):** Introduction to Law and Public Administration
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):** kiberbiztonsági MA
6. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** Államtudományi és Nemzetközi Tanulmányok Kar, Lőrincz Lajos Közigazgatási Jogi Tanszék
7. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Szalai András, PhD, egyetemi docens
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 hallgató megismeri a joggal és a jogrendszerrel, a jogállamisággal kapcsolatos fogalmakat, összefüggéseket, amelyek megalapozzák a közigazgatás elhelyezését az állami szervek rendszerében, és mint jogalkotót a jogforrási hierarchiában. A legfontosabb érintett témakörök következők: norma és jog; jogalkotás és jogforrási hierarchia; az alkotmányos állam eszméje; a közigazgatással foglakozó tudományok; a közigazgatás kapcsolata a gazdasággal és a politikával; a közigazgatási szervek és szervezetrendszerek; a közigazgatás személyzeti rendszerei; a közigazgatás ellenőrzése.

   A tantárgy szakmai tartalma (angolul) (Course description): Students become familiar with the concepts of law and the legal system, the rule of law, and the relationships that underpin the placement of public administration in the system of state organs and as a legislator in the hierarchy of sources of law. The most important topics involved are: norm and law; legislation and hierarchy of sources; the idea of a constitutional state; public administration sciences; the relationship between public administration and the economy and politics; administrative bodies and organizational systems; personnel systems in public administration; administrative control.

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

    Tudása: Ismeri azokat a fontosabb előírásokat a szabályozásokból, amelyek a mindennapi munkáját befolyásolják. Megismeri a közigazgatás-tudomány tárgyát, a közigazgatás-tudomány egyes irányzatait. Ismeri a közigazgatás alapintézményeit, tisztában van a közigazgatás funkcióival, felépítésével és működésével. Átlátja a jogrendszert, és annak tagozódását, elsajátítja a jogállamiság alapelveit.

    Képességei: Képes értelmezni a jogszabályokból eredő követelményeket. A kompetenciák birtokában a hallgató képes elhelyezni a közigazgatást az állami szerveztrendszerben és a jogrendszerben, emellett használja a megfelelő szakterminológiát. Képes a jogszabályok értelmezésére, a legfontosabb jogelvek alkalmazására.

Attitűdje: Nyitott az alapozó ismeretek gyarapítása és a jogi összefüggések iránt.

Autonómiája és felelőssége: Önállóan képes felismerni és megfeltetni a közigazgatás jogálli elemeit, jogszerű mőkédésére választ adni.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: Specifications of regulations that have an immediate impact on his/her daily work. He/she get acquainted with the subject of public administration science and certain tendencies of public administration science. He/she knows the basic institutions of public administration, knows the functions, structure and operation of public administration; and understands the legal system and its structure and learns the principles of the rule of law.

Capabilities: Interpreting legal requirements. The student is able to place public administration in the state organizational and legal system, and to use appropriate terminology. It is able to interpret laws and apply the most important principles of law.

Attitude: They will open to basic knowledge and legal correlations.

Autonomy and responsibility: He is able to recognize and expose the legal elements of public administration independently, and to respond to its legal functioning.

11. Előtanulmányi követelmények: -

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

12.1. Az állam, az állam szervezete (The state, the organization of the state);

12.2. A közigazgatás fogalma és kialakulása (Concept and evolution of public administration);

12.3. A közigazgatás feladatai, funkciói és tevékenységfajtái(Functions, functions and activities of public administration);

12.4. A közigazgatás szervezete I. A központi közigazgatás (Organization of Public Administration I. Central administration);

12.5. A közigazgatás szervezete II. A helyi igazgatás (Organization of public administration II. Local administration);

12.6. A közszolgáltatások és a közszolgáltatásokat ellátó szervek (Public services and bodies providing public services);

12.7. A jog fogalma. A jogrendszer és tagozódása. A jogágak viszonya egymáshoz (Concept of law. The legal system and its division. The relationship between the branches of law);

12.8. A közigazgatási jog fogalma, kialakulása, jellemzői (Concept, formation and characteristics of administrative law);

12.9. A közigazgatási jog forrásai. A közigazgatási jogviszony (Sources of administrative law. Administrative legal relationship);

12.10. A közigazgatás jogalkalmazó tevékenysége (Law enforcement activities of public administration);

12.11. A közigazgatás felelőssége (Responsibility of public administration);

12.12. A közigazgatás személyi állománya (Administrative staff).

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 hallgató köteles a tréningfoglalkozások legalább 70%-án részt venni. A rövid/tartós távolmaradás indokolt esetben (orvosi, szolgálati) pótolható, amely pótlás egyéni megbeszélés szerint történik. A távollétet a hiányzást követő első foglalkozáson kell igazolnia. A hiányzás esetén a hallgató

köteles az előadás anyagát beszerezni, abból önállóan felkészülni.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A tanulmányi munka alapja az előadások látogatása, az előírt olvasmányok ismerete, aktiv órai részvétel, a félév során egy dolgozat elkészítése és annak prezetálása. Az oktató az alábbi szempontok mentén értékeli a beadott és előadott anyagot 1-5-ig terjedő skálán: szakmaiság, szaknyelv alkalmazása, felkészültség, tájékozottság, reflektivitás szintje.

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

16.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele a 14. pontban meghatározott arányú részvétel a foglalkozásokon és a 15. pontban meghatározott félévközi feladatok legalább elégséges teljesítése.

16.2. Az értékelés:

A félév értékelése kollokvium – írásbeli vizsga. A Tanszék felkészülési kérdéseket ad ki. A vizsga tartalmát az előadáson elhangzottak és az alább felsorolt kötelező és ajánlott irodalmak anyagai képezik. A vizsgadolgozat értékelése szummatív: 0-50% - elégtelen, 51-70% - elégséges, 71-80% - közepes, 81-90% - jó, 91-100% - jeles.

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. LAPSÁNSZKY András – PATYI András –TAKÁCS Albert: A közigazgatás szervezete és szervezeti joga, Institutiones Administrationis III. Budapest, Dialóg Campus, 2017. - a tematikához kapcsolódó fejezetei
2. VARGA ZS. András: A közigazgatás és a közigazgatási jog alkotmányos alapjai. Institutiones Administrationis I. Budapest, Dialóg Campus, 2017. - a tematikához kapcsolódó fejezetei

17.2. Ajánlott irodalom:

1. Bauer - Knill - Eckhard (eds.): , International Bureaucracy: Challenges and Lessons for Public Administration Research. Palgrave Macmillan, 2017., ISBN: 978-1349956920;
2. LŐRINCZ Lajos (szerk.): Közigazgatástudományi Antológia I.–II. ÁIF - ELTE, 2003.
3. − LŐRINCZ Lajos: A közigazgatási alapintézményei. Harmadik bővített, átdolgozott kiadás. HVG-Orac. Budapest, 2010.
4. − MAGYARY Zoltán: Magyar Közigazgatás. Királyi Magyar Egyetemi Nyomda, Budapest, 1942.
5. − PATYI András: A közigazgatás működésének jogi alapkérdései. Institutiones Administrationis II. Budapest, Dialóg Campus, 2017

Budapest, 2021.01.05.

Dr. Szalai András, PhD
egyetemi docens sk.

NEMZETI KÖZSZOLGÁLATI EGYETEM
Rendészettudományi Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** NPNBM25
2. **A tantárgy megnevezése (magyarul):** Kiberbiztonság pszichológiai aspektusai
3. **A tantárgy megnevezése (angolul):** Psychological aspects of cybersecurity
4. **Kreditérték és képzési karakter:**
   - **4.1.** 2 kredit
   - **4.2.** a tantárgy elméleti vagy gyakorlati jellegének mértéke: 0% gyakorlat, 100% elmélet
5. **A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):** kiberbiztonsági MA
6. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** Rendészettudományi Kar, Polgári Nemzetbiztonsági Tanszék
7. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Dobák Imre, PhD, egyetemi docens
8. **A tanórák száma és típusa**
   - **8.1.** össz óraszám/félév:
     - 8.1.1. nappali munkarend: 28 (28 EA + 0 GY)
     - 8.1.2. levelező munkarend: 8 (8 EA + 0 GY)
   - **8.2.** heti óraszám - nappali munkarend: 2 (2 EA + 0 GY)
   - **8.3.** Az ismeret átadásában alkalmazandó további sajátos módok, jellemzők: -
9. **A tantárgy szakmai tartalma (magyarul):** A tárgy a kiberbiztonság pszichológiai kérdésköréhez kapcsolódóan tárgyalja a kibertérben zajló megtévesztés és befolyásolás széles kérdéskörét. Társadalomtudományi megközelítéssel ismerteti az állami és nem állami szereplők kapcsán megfigyelhető folyamatokat, a lélektani műveletek, a megtévesztés, a befolyásolás, az információgyűjtés, és információterjesztés, álhírek sajátosságait, azok jelenlétét, lehetséges céljait, hatásait. Példákon, esettanulmányokon keresztül hívja fel a figyelmet a jelenségre, különös tekintettel a közösségi média szerepére.

   A tantárgy szakmai tartalma (angolul) (Course description): The subject deals with the issue of cyber-deception and influence in the context of psychological issue of cybersecurity, It examines a social science approach to the processes observed in relation to state and non-state actors, the specialties of psychological operations, deception, influence, information gathering, and dissemination of information, their presence, possible purposes and effects. It draws attention to the phenomenon through examples and case studies, with particular reference to the role of social media.

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

Tudása: Megérti a szervezeti feladatokat a kibervédelemben.

Képességei: Képes olyan védelmi intézkedések meghozatalára, amelyek segítik a humán fenyegetettségből eredő kockázatok csökkentését.

Attitűdje: 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: Taking defensive measures that ensure the reduction of risk resulting from threat against humans.

Attitude: 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: A kiberbiztonság humán tényezői [NPNBM24]

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

12.1. Pszichológiai „műveletek" értelmezése és jelentősége a kibertérben (Understanding and importance of psychological operations in the cyberspace);

12.2. Céljai, szereplői (nemzet)biztonsági szemmel (Main aims, actors by national security aspects) (N/2, L/0 tanóra);

12.3. A megtévesztés lehetőségei, technikái, nemzetközi példái, az álhírek sajátosságai, céljai, hatásai, az információk terjedése (Possibilities and techniques of deception) (N/6, L/1 tanóra);

12.4. A befolyásolás jelensége, lehetséges céljai, sajátosságai, példái (Phenomenon of influence, its possible aims and peculiarities) (N/3, L/1 tanóra);

12.5. Céljai, szereplői (nemzet)biztonsági szemmel (Peculiarities, aims, and effects of Fake News) (N/2, L/1 tanóra);

12.6. A közösségi média és egyéb platformok szerepe (The Role of Social Media) (N/5, L/2 tanóra);

12.7. Információgyűjtés a kibertérben (Collecting information in cyberspace) (N/2, L/1 tanóra);

12.8. Esettanulmányok (nemzetközi kitekintés) (Case Studies (International Perspective)) (N/6, L/2 tanóra).

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 hallgató köteles a tanórák min. 70 %-án részt venni. Amennyiben a hallgató az elfogadható hiányzások mértékét túllépi, köteles az elmaradt órai tananyag beszerzéséről gondoskodni, a részvétel a tanárral való egyeztetés alapján meghatározott házi dolgozat készítésével pótolható.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A félév során félévközi feladatként nappali képzésben két zárthelyi dolgozat megírására kerül sor a 5. és 7. témakör zárását követően. (Levelező képzésben egy zárthelyi a 7. témakört követően.) A zárthelyi legalább elégséges eredménnyel történő teljesítése az aláírás feltétele. A zárthelyi ötfokozatú kerül értékelésre (60 %-tól elégséges, 70 %-tól közepes, 80-tól % jó, 90 %-tól jeles). Sikertelen zárthelyi dolgozat a szorgalmi időszak végéig pótolható.

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

16.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele a 14. pontban meghatározott arányú részvétel a foglalkozásokon és a 15. pontban meghatározott félévközi feladat legalább elégséges teljesítése.

16.2. Az értékelés:

Kollokvium (írásbeli vagy szóbeli – a csoport létszámától függ). A kollokviumhoz a tanszék felkészülési kérdéseket ad ki. A kollokvium ötfokozatú értékelésű. Írásbeli kollokvium esetén annak értékelése szummatív: 0-50% - elégtelen, 51-70% - elégséges, 71-80% - közepes, 81-90% -

jó, 91-100% - jeles.

16.3. A kreditek megszerzésének feltételei:

A kreditek megszerzésének feltétele az aláírás megszerzése és legalább elégséges kollokvium (K).

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. Haig Zsolt: Információs műveletek a kibertérben, Dialóg Campus Kiadó, Budapest, 2018, ISBN 978-615-5945-05-2;
2. Bányász Péter: A közösségi média szerepe a lélektani műveletekben az elmúlt időszak válságainak tükrében, Szakmai Szemle 2016. I. szám, Budapest pp.: 61–81.o.;
3. Rózsa Tibor: A befolyásolás művészete, Hadtudományi Szemle 2014/2. szám. 44-53.o.;
4. Dornfeld et. al.: A virtuális tér geopolitikája, Műhelymunkák 2016/1, Geopolitikai Tanács Közhasznú Alapítvány, ISBN 978-963-9816-34-3.

17.2. Ajánlott irodalom:

1. Haig Zsolt: Információ – társadalom – biztonság. NKE Szolgáltató Kft., Budapest, 2015., ISBN: 9786155527081;
2. Rózsa Tibor: Az információs műveletek vizsgálata, különös tekintettel a befolyásolási képességek alkalmazásának lehetőségeire a Magyar Honvédség feladatrendszerében, PhD értekezés NKE 2016.;
3. Cialdini, Robert B.: Hatás - A befolyásolás pszichológiája, HVG Könyvek kiadó, 2009., ISBN 9789639686779;
4. Newton Lee (2016): Facebook Nation- Total Information Awarness. Springer, ISBN 978-1493944750.

Budapest, 2021.01.05.

Dr. Dobák Imre, PhD,
egyetemi docens sk.

NEMZETI KÖZSZOLGÁLATI EGYETEM
Államtudományi és Nemzetközi Tanulmányok Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** ÁKINTM10
2. **A tantárgy megnevezése (magyarul):** Kiberbiztonsági stratégia és vezetés
3. **A tantárgy megnevezése (angolul):** Cybersecurity Strategy and Leadership
4. **Kreditérték és képzési karakter:**
   - **4.1.** 3 kredit
   - **4.2.** a tantárgy elméleti vagy gyakorlati jellegének mértéke: 0% gyakorlat, 100% 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. Bányász Péter, PhD, adjunktus
8. **A tanórák száma és típusa**
   - **8.1.** össz óraszám/félév:
   - 8.1.1. nappali munkarend: 28 (28 EA + 0 GY)
   - 8.1.2. levelező munkarend: 8 (8 EA + 0 GY)
   - **8.2.** heti óraszám - nappali munkarend: 2 (2 EA + 0 GY)
   - **8.3.** Az ismeret átadásában alkalmazandó további sajátos módok, jellemzők: -
9. **A tantárgy szakmai tartalma (magyarul):** A tantárgy felkészít az információbiztonsági stratégia kifejlesztésére, az üzleti célok, funkciók és az információbiztonság kapcsolatának megértésére. A hallgatók elsajátítják a stratégiai tervek készítéséhez szükséges stratégiai költségtervezési és riport eljárásokat, a biztonsági beruházásokhoz szükséges költségek vezetés felé történő elfogadtatásnak a módjait. Az információbiztonsági vezetés tekintetében megismerik az információbiztonsági vezető feladatköreit, illetve gyakorlati példákon keresztül ennek végrehajtási módját. Az ellenőrzés tekintetében a kulcs metrikák (KPI-k) kiválasztására és implementálására irányuló eljárásokat, illetve a mutatók ellenőrzési módjait ismerik meg a hallgatók.

   A tantárgy szakmai tartalma (angolul) (Course description): The course prepares the students to develop an information security strategy, understanding the relationship between business objectives, functions and information security. Students will learn the strategic cost planning and reporting procedures needed to make strategic plans, and how to manage the cost of security investments. With regard to information security management, they will learn about the responsibilities of the information security manager and how to implement it through practical examples. In terms of control, students will learn the procedures for selecting and implementing key metrics (KPIs) and how to control metrics.

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

Tudása: Ismeri a vállalati stratégia eszköztárát és annak alkalmazhatóságát a kiberbiztonságban.

Képességei: Képes a keletkezett információk megosztásának szükségességével kapcsolatban komplex következtetések levonására.

Attitűdje: Felelős vezetőként a vezetéstudomány átültetése a kiberbiztonsági gyakorlatba.

Autonómiája és felelőssége: Önállóan dolgozza fel az új és összetett információkat, problémákat, illetve jelenségeket rendszerszerű és kritikus módon. Kezdeményező módon lép fel az alternatív,

eredeti megoldások kidolgozásában, bemutatásában és a bonyolult, nem tipikus helyzetekben történő adekvát döntések meghozatalában. Önállóan és pontosan vesz részt a kiberbiztonsági fenyegetések technológiai, politikai és adminisztratív megoldásában. Kezdeményezőként dolgozik a technikai és operatív teendők stratégiai célokká való konvertálásában.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: Knows the toolset of business startegy and its implementation in the cybersecurity.

Capabilities: Drawing complex conclusions in terms of the necessity of sharing information.

Attitude: As a resposible leader, applying leadership science in cybersecurity practice.

Autonomy and responsibility: To process new and complex information, problems and phenomena in a systematic and critical way. To initiate and introduce alternative and original solutions and appropriate decision making in complex, atypical contexts. To take part in providing technological, political and administrative solutions to cyber threats. To take the initiative to convert technical and operative tasks into strategic targets.

11. Előtanulmányi követelmények: Vezetéselmélet [ÁKINTM07]

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

12.1. Információbiztonsági irányítási rendszer (Information Security Management System);

12.2. Az információbiztonsági stratégia kialakítása (Defining an IS strategy);

12.3. Információbiztonsági stratégia bemenő adatai (Input data of IS strategy);

12.4. Stratégia kialakításának tényezői (Factors of IS strategy);

12.5. Az üzleti célok, funkciók és az információbiztonság kapcsolata (Business and IS strategy);

12.6. Az információbiztonság irányítása, a stratégia megvalósítása (Governance of IS, strategy implementation);

12.7. Stratégiai tervek készítése (Strategic planning);

12.8. Stratégiai költségtervezés és riport eljárások (Cost planning and reporting);

12.9. A szervezeti struktúrák (Organizational Structures);

12.10. Metrikák és mérés (Metrics and measurement);

12.11. Szabályzati környezet (Regulation);

12.12. Védelmi intézkedések (IS Measures);

12.13. Információbiztonsági szemlélet (IS mindset);

12.14. A stratégia megvalósításának lehetséges buktatói (Issues of implementation);

12.15. Rendszeres riportok, jelentése (Reporting);

12.16. Audit (Audit)

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

15. Félévközi feladatok, ismeretek ellenőrzésének rendje:

Nincs félévközi feladat.

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

16.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele a 75%-os arányú részvétel a foglalkozásokon.

16.2. Az értékelés:

A tárgyból írásbeli vizsga lesz a vizsgaidőszakban, a kiadott tételsor alapján.

16.3. A kreditek megszerzésének feltételei:

A kreditek megszerzésének feltétele az aláírás megszerzése és legalább elégséges kollokvium (K).

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. Oroszi Eszter Diána: Információbiztonsági stratégia és vezetés. Budapest: NKE, 2014.
2. Yigal Behar: Digital War: Digital War: The One Cybersecurity Strategy You Need to Implement Now to Secure Your Business. 2017. ISBN 1548459712

17.2. Ajánlott irodalom:

1. Ellis, Scott (2016): The CSO Guide: The Chief Information Security Officer (CISO) Handbook. ISBN 978-1519090348.

Budapest, 2021.01.05.

Dr. Bányász Péter, PhD,
adjunktus sk.

NEMZETI KÖZSZOLGÁLATI EGYETEM
Rendészettudományi Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** RBGVB108
2. **A tantárgy megnevezése (magyarul):** Kiberbiztonsági szabályozások és szabványok
3. **A tantárgy megnevezése (angolul):** Cybersecurity regulations and standards
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:** Rendészettudományi Kar, Bűnügyi, Gazdaságvédelmi és Kiberbűnözés Elleni Tanszék
7. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Muha Lajos, 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 hallgató megismeri a kiberbiztonságra vonatkozó nemzeti és nemzetközi szabályozókat és a legfontosabb szabványokat.

   A tantárgy szakmai tartalma (angolul) (Course description): The student will become familiar with national and international cyber security regulators and key standards.

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

    Tudása: Ismeri azokat a fontosabb előírásokat a szabályozásokból, amelyek a mindennapi munkáját befolyásolják.

    Képességei: Képes értelmezni a jogszabályokból eredő követelményeket.

    Attitűdje: Munkája során figyelembe veszi és alkalmazza a kiberbiztonsággal kapcsolatos jogszabályokat.

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

    Elérendő kompetenciák (angolul) (Competences – English):

    Knowledge: Specifications of regulations that have an immediate impact on his/her daily work.

    Capabilities: He/she is capable of having an overview of the special legal status of cyberspace.

    Attitude: An attention to and application of laws of cyber security in his/her work.

    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. A kiberbiztonsággal kapcsolatos hazai és nemzetközi szabályozások (National and international cyber security regulations):

12.2. Az Európai Parlament és a Tanács (EU) 2016/1148 Irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (NIS) (Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union);

12.3. A 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (L. 2013 the law on Electronic Information Security of State and Local government Bodies);

12.4. 2009. évi CLV. törvény a minősített adat védelméről (CLV 2009 the law on the protection of classified information);

12.5. A Sarbanes–Oxley Act (SOX);

12.6. A kiberbiztonsággal kapcsolatos szabványok (Cybersecurity standards);

12.7. A szabványok fogalma, az információbiztonsági szabványok összefüggései és felhasználásai lehetőségeik (The concept of standards, the context of information security standards and their uses);

12.8. ISO 19011:2011 – Guidelines for auditing management systems;

12.9. A NIST SP 800 sorozat és az SP 800-53 (NIST SP 800 series and SP 800-53);

12.10. A Common Criteria;

12.11. A COBIT;

12.12. Az ITIL;

12.13. Az Enterprise Information Security Architecture (EISA);

12.14. A Payment Card Industry Data Security Standard (PCI DSS).

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. A meg nem írt, vagy sikertelen zárthelyi dolgozat miatt megtagadott aláírás a TVSZ vonatkozó pontjai szerint pótolható a szorgalmi időszak utolsó hetében.

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

16.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele az előző a meghatározott arányú részvétel a foglalkozásokon.

16.2. Az értékelés:

A félév értékelése két zárthelyi dolgozat eredménye alapján történik, és gyakorlati jeggyel zárul. Értékelése: ötfokozatú, maximális pontszám 0-60%-a elégtelen, 61-70%-a elégséges, 71-80%-a közepes, 81-90%-a jó, 91-100%-a jeles.

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. Szádeczky Tamás (2014): Információbiztonsági szabványok. Budapest: NKE, ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel;
2. Muha Lajos, Krasznay Csaba: Az elektronikus információs rendszerek biztonságának menedzselése, Budapest, 2018, Nemzeti Közszolgálati Egyetem, ISBN 978-615-5870-27-9.

17.2. Ajánlott irodalom:

1. Muha Lajos, Szádeczky Tamás (2014): Irányítási rendszerek. Budapest: NKE, ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel;
2. Douglas J. Landoll (2016): Information Security Policies, Procedures, and Standards: A Practitioner's Reference. Auerbach Publications, ISBN 978-1482245899;
3. ISO/IEC 27xxx sorozat vagy KIB 25. ajánlás IBIR és IBIK kötetei, COBIT;
4. Common Criteria
5. 41/2015. (VII. 15.) BM rendelet,
6. Control Objectives for Information and Related Technologies (COBIT)

Budapest, 2021.01.05.

Dr. Muha Lajos, PhD,
egyetemi docens sk.

NEMZETI KÖZSZOLGÁLATI EGYETEM
Rendészettudományi Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** RBGVB110
2. **A tantárgy megnevezése (magyarul):** Kiberbűnözés
3. **A tantárgy megnevezése (angolul):** Cybercrime
4. **Kreditérték és képzési karakter:**
   - **4.1.** 5 kredit
   - **4.2.** a tantárgy elméleti vagy gyakorlati jellegének mértéke: 50% gyakorlat, 50% elmélet
5. **A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):** kiberbiztonsági MA
6. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** Rendészettudományi Kar, Bűnügyi, Gazdaságvédelmi és Kiberbűnözés Elleni Tanszék
7. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Nagy Zoltán András, PhD, egyetemi docens
8. **A tanórák száma és típusa**
   - **8.1.** össz óraszám/félév:
     - 8.1.1. nappali munkarend: 56 (28 EA + 28 GY)
     - 8.1.2. levelező munkarend: 16 (8 EA + 8 GY)
   - **8.2.** heti óraszám - nappali munkarend: 4 (2 EA + 2 GY)
   - **8.3.** Az ismeret átadásában alkalmazandó további sajátos módok, jellemzők: -
9. **A tantárgy szakmai tartalma (magyarul):** A tárgy átfogó képet kíván nyújtani a kiberbűnözés jellemzőiről, típusairól, jövőben várható tendenciáiról, annak anyagi-, eljárás-, nemzetközi jogi ismérveiről.

   A tantárgy szakmai tartalma (angolul) (Course description): The subject aims to provide a comprehensive overview of the characteristics, types, future trends of cybercrime, its material, procedural and international legal aspects.

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

Tudása: Ismeri a hazai - és a nemzetközi jog alkalmazhatóságát a kibertérben.

Képességei: Képes átlátni a kibertér aktuális fenyegetéseit.

Attitűdje: Megérti és elfogadja a nemzetközi kiberjog komplexitását, ennek köszönhetően a munkája során törekszik ennek a komplexitásnak a kezelésére.

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

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: Knows the applicability of domestic and international law in cyberspace.

Capabilities: Understanding the current threats of cyber space.

Attitude: An understanding and acceptance of the complexity of international cyber law and thus strives to handle this complexity in his/her work.

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. A kibertérhez nem kötött bűncselekmények általában (Non-cybercrime in virtual space – generally);

12.2. Szellemi tulajdonjog megsértése (copyright law, 3D nyomtatás stb.).(Infringement of Intellectual Property Rights (Copyright Law, 3D printing etc.));

12.3. Pénzmosás (Money Laudering);

12.4. A kiber térhez kötött bűncselekmények (Cybercrime);

12.5. Adathalászat esetei. Hacking, wardriving.Social engineerin, phishing. (Business e-mail phisihng);

12.6. A tartalomközléssel megvalósuló bűncselekmények (Content-crime in cyberspace);

12.7. Becsületsértő, rágalmazó, rasszista, homofób tartalmak közlése (Posting defamatory, racist, homofobic content in cyberspace);

12.8. Támadó jellegű bűncselekmények – általános jellemzői (Offensive attack in cyberspace – generally);

12.9. Internetes zaklatás típusai, „bosszú-pornó" (Cyberbullying. Cyber mobbing. „Revenge porn");

12.10. DoS, DDoS támadások, zsarolóvírusok (DoS, DDoS attack, ransomwares);

12.11. Malware-támadások, defacing (Malware-attacks, defacing);

12.12. A bűnügyi jogsegélyre vonatkozó jogszabályok (Mutual Assistance).

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 hallgató köteles a foglalkozások legalább 75%-án részt venni. Igazolt hiányzás esetén a részvétel a tanárral való egyeztetés alapján meghatározott házi dolgozat készítésével pótolható.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje:

Zárthelyi dolgozat a kibertérhez nem kötött (tradiconális) bűncselekmények megjelenése témakörből.

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

16.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele a meghatározott arányú részvétel a foglalkozásokon.

16.2. Az értékelés:

A tematikában szereplő témákból 20 ezer karakternyi írásbeli záródolgozat. A zárthelyi dolgozat és az önállóan készített záródolgozat két érdemjegye alapján kerül az ötfokozatú értékelés kialakítva.

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. Deres Petronella: Internetes bűnözés – Cybercrime. In: Technológiai jog – Új globális

technológiák jogi kihívásai. Szerkesztő: Dr. Tóth András. KRE ÁJK: Budapest, 2016.;
2. Parti Katalin: Gyermekpornográfia az Interneten, Miskolc, Bíbor Kiadó, 2009.;
3. Nagy Zoltán András: Bűncselekmények számítógépes környezetben Ad Librum Kiadó, Budapest, 2009. ISBN: 9789639888920;
4. Kiss Tibor (szerk): Kibervédelem a bűnügyi tudományokban. (megjelenés alatt);
5. Blaskó Béla,Hautzinger Zoltán,Madai Sándor,Pallagi Anikó,Polt Péter,Schubauer László: Büntetőjog Különös rész I.-II. Rejtjel Kiadó, Budapest, 2015. ISBN 978 963 7255 95 3;

17.2. Ajánlott irodalom:

1. Kovács László: A kibertér védelme. Dialóg Campus Kiadó, Budapest, 2018.;
2. Haig Zsolt: Információ, társadalom, biztonság. NKE, 2015. ISBN: 9786155527081;
3. Holt et. al. Cybercrime and Digital Forensics: An Introduction. vol. Second edition, Routledge, 2018.;
4. Cybercrime and Criminological Theories. In: Thomas J. Holt – Adam M. Borster – Kathryn Seigfried – Spellar: Cybercrime and Digital Forensic. Routledge, London - New York, 2017.;
5. Goodman, Marc: Future Crimes. Penguin Random House LLC, New York, 2015 ISBN: 978-0-8041-7145-8.

Budapest, 2021.01.05.

Dr. Nagy Zoltán András, PhD,
egyetemi docens sk.

NEMZETI KÖZSZOLGÁLATI EGYETEM
Hadtudományi és Honvédtisztképző Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** HHKNBTTMA04
2. **A tantárgy megnevezése (magyarul):** Kiberdiplomácia
3. **A tantárgy megnevezése (angolul):** Cyber Diplomacy
4. **Kreditérték és képzési karakter:**
   - **4.1.** 4 kredit
   - **4.2.** a tantárgy elméleti vagy gyakorlati jellegének mértéke: 0% gyakorlat, 100% elmélet
5. **A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):** kiberbiztonsági MA
6. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** Hadtudományi és Honvédtisztképző Kar, Nemzetközi Biztonsági Tanulmányok Tanszék
7. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Molnár Anna, PhD, egyetemi tanár
8. **A tanórák száma és típusa**
   - **8.1.** össz óraszám/félév:
     - 8.1.1. nappali munkarend: 42 (42 EA + 0 GY)
     - 8.1.2. levelező munkarend: 12 (12 EA + 0 GY)
   - **8.2.** heti óraszám - nappali munkarend: 3 (3 EA + 0 GY)
   - **8.3.** Az ismeret átadásában alkalmazandó további sajátos módok, jellemzők: -
9. **A tantárgy szakmai tartalma (magyarul):** A tantárgy elsődleges célja, hogy átfogó képes nyújtson a nemzetközi kapcsolatok kiberteret érintő főbb kérdéseiről, betekintést adva az aktuális trendekről és kihívásokról. A hallgató megismeri azokat a kiberdiplomáciával kapcsolatos alapvető fogalmakat, összefüggéseket, amelyek segítséget nyújtanak a komplex témakör megértésében és megalapozzák a jövőbeni szakmai fejlődést. Az általános trendek bemutatásán túl a kurzus alatt kiemelt figyelem irányul a témát érintő olyan meghatározó kérdésekre, mint a kiberteret érintő jogi szabályozás lehetőségei, a kiberhadviselés és a kiberkémkedés veszélyei, a kiberelrettentés, az internet kormányzás nemzetközi aspektusai, vagy a különböző nemzetközi szervezetek tevékenységei.

   A tantárgy szakmai tartalma (angolul) (Course description): The primary objective of the course is to provide a comprehensive understanding of the major cyber issues in international relations, providing insight into current trends and challenges. Students will learn the basic concepts and contexts of cyber diplomacy, which will help them to understand the complexity of the topic and lay the foundations for future professional development. In addition to presenting general trends, the course focuses on key issues relevant to the topic, such as the potential for cyber law enforcement; the dangers of cyber-bullying and cyber-espionage; as well as cyber-deterrence, and international aspects of internet governance, or activities.

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

    Tudása: Átlátja a kibertérrel kapcsolatos diplomáciai, illetve politikai információmegosztás folyamatát, valamint az esetleges válaszlépéseket.

    Képességei: Képes a keletkezett információk megosztásának szükségességével kapcsolatban komplex következtetések levonására.

    Attitűdje: Megérti és elfogadja a nemzetközi kiberjog komplexitását, ennek köszönhetően a munkája során törekszik ennek a komplexitásnak a kezelésére.

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

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: He/she is familiar with the procedure of diplomatic and political information sharing related to cyberspace, as well as possible responses.

Capabilities: He/she is capable of drawing complex conclusions in terms of the necessity of sharing information.

Attitude: His/her personal attitude is characterized by An understanding and acceptance of the complexity of international cyber law and thus strives to handle this complexity in his/her work.

Autonomy and responsibility: Having autonomy and responsibility to put the results of scientific research in the field into his/her practice.

11. Előtanulmányi követelmények: -

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

12.1. Bevezetés (Introduction);

12.2. Kiberdiplomácia (Cyber Diplomacy);

12.3. A kiberteret érintő jogi szabályozás lehetőségei (Opportunities for legal regulation in cyberspace);

12.4. A kiberhadviselés és a kiberkémkedés veszélyei, a kiberelrettentés (Cyber warfare and cyber espionage, cyber deterrence);

12.5. Az internet kormányzás nemzetközi aspektusai (International aspects of internet governance);

12.6. Nemzetközi szervezetek tevékenysége a kibertérben (Activities of international organizations in the field of cyberspace);

12.7. Az Európai Unió diplomáciai tevékenysége a kibertérben I. (European Union diplomatic activity in cyberspace I .);

12.8. Az Európai Unió diplomáciai tevékenysége a kibertérben II. (European Union diplomatic activity in cyberspace II .);

12.9. Nemzeti szintű kiberdiplomácia I. (National Cyber Diplomacy I.);

12.10. Nemzeti szintű kiberdiplomácia II. (National Cyber Diplomacy II.);

12.11. Nemzeti szintű kiberdiplomácia III. (National Cyber Diplomacy III .);

12.12. Nemzeti szintű kiberdiplomácia IV. (National Cyber Diplomacy IV .);

12.13. Zárthelyi dolgozat (End-of-term writing test);

12.14. Zárthelyi dolgozat javítás (End-of-term writing test (correction)).

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 hallgató köteles a foglalkozások legalább 75 %-án részt venni. Az igazolatlan hiányzás nem pótolható. 25% feletti igazolatlan hiányzással az aláírás megtagadásra kerül.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A feladatok pótlása a tárgyfelelőssel egyeztetve történik.

A zárthelyi dolgozat esetében az értékelés a hallgató által elért pontok alapján a következő módon történik:

0-50% = elégtelen (1)

51%-62,5%= elégséges (2)

63%-75% = közepes (3)

76%- 87,5%= jó (4)

88%-100 = jeles (5)

Megajánlott jegy adható a zárthelyi dolgozatok végeredménye alapján (a kapott jegyek átlaga). A megajánlott jegy feltétele az aláírás megszerzése és legalább elégséges zárthelyi dolgozati eredmények.

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

16.1. Az aláírás megszerzésének feltételei:

Az aláírás feltétele a foglakozásokon legalább 75%-os részvétel.

16.2. Az értékelés:

A vizsga követelménye a tanórákon átadott ismeretekre és a kötelező irodalomra épül. A zárthelyi dolgozatok és az írásbeli kollokvium esetében az értékelés a hallgató által elért pontok alapján a következő módon történik:

0-50% = elégtelen (1)

51%-62,5%= elégséges (2)

63%-75% = közepes (3)

76%- 87,5%= jó (4)

88%-100 = jeles (5)

A zárthelyi dolgozatok eredménye alapján megajánlott jegy kapható.

16.3. A kreditek megszerzésének feltételei:

A kreditek megszerzésének feltétele az aláírás megszerzése és legalább elégséges kollokvium (K).

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. Berzsenyi Dániel, Krasznay Csaba: Nemzetközi kapcsolatok a kibertérben. Nemzeti Közszolgálati Egyetem (megjelenés alatt);
2. Molnár Anna: Az Európai Unió kiberbiztonsággal kapcsolatos tevékenysége In: Bonnyai Tünde; Danyek Miklós; Görgey Péter; Kriskó Edina; Molnár Anna; Tikos Anita; Deák Veronika: Kritikus információs infrastruktúrák védelme, Budapest, Magyarország : Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézet, 2019. pp. 40-63. ISBN: 978-963-498-239-5;
3. Molnár Dóra: Törékeny nagyhatalmiság: a kiberbiztonság. Az európai kibertér brit, német és francia szegmensei, Budapest, Magyarország : Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézet, 2019. ISBN: 978-963-498-173-2.

17.2. Ajánlott irodalom:

1. Choucri, Nazli (et al): Cyberspace and International Relations. The MIT Press, 2012. ISBN: 0262517698;
2. Singer, P. W.: Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, 2014. ISBN: 0199918112;
3. N Schmitt, Michael (szerk.): Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, 2017. ISBN: 9781316822524;
4. Christou, George: Cybersecurity in the European Union Resilience and Adaptability in Governance Policy. Palgrave Macmillan, 2016. ISBN: 9781137400529;
5. Clarke, Richard A., Knake, Robert K.: Cyber War: The Next Threat to National Security and

What to Do About It. Ecco, 2011. ISBN: 0061962244;

Budapest, 2021.01.05.

Dr. Molnár Anna, PhD,
egyetemi tanár sk.

NEMZETI KÖZSZOLGÁLATI EGYETEM
Hadtudományi és Honvédtisztképző Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** HKEHVM63
2. **A tantárgy megnevezése (magyarul):** Kiberhadviselés
3. **A tantárgy megnevezése (angolul):** Cyberwarfare
4. **Kreditérték és képzési karakter:**
   - **4.1.** 3 kredit
   - **4.2.** a tantárgy elméleti vagy gyakorlati jellegének mértéke: 0% gyakorlat, 100% elmélet
5. **A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):** kiberbiztonsági MA
6. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** Hadtudományi és Honvédtisztképző Kar, Elektronikai Hadviselés Tanszék
7. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Kovács László, PhD, egyetemi tanár
8. **A tanórák száma és típusa**
   - **8.1.** össz óraszám/félév:
     - 8.1.1. nappali munkarend: 28 (28 EA + 0 GY)
     - 8.1.2. levelező munkarend: 8 (8 EA + 0 GY)
   - **8.2.** heti óraszám - nappali munkarend: 2 (2 EA + 0 GY)
   - **8.3.** Az ismeret átadásában alkalmazandó további sajátos módok, jellemzők: -
9. **A tantárgy szakmai tartalma (magyarul):** A képzésben résztvevő hallgatók megismerkednek a komplex információs támadások összetevőivel és hatásaival. Ezen belül ismertetésre kerülnek az információs infrastruktúrák és támadható pontjaik; a támadási módok; az offenzív kiberműveleti képességek és a kiberelrettentés összefüggései; illetve a kiberhadviselés és a nemzetközi jogi normák öszefüggései. A tárgy kitér a kiberhadviselés összetevőire, amelyben a felderítés és információszerzés; a kibertámadások módszertana; a kibervédelem és stratégia összefüggései kerülnek bemutatásra. A kiberhadviselés kapcsolatainak ismeretése során az információs műveletek, elektronikai hadviselés médiahadviselés és a befolyásolás, valamint a kiberterrorizmus kerül bemutatásra.

   A tantárgy szakmai tartalma (angolul) (Course description): Students will learn about the components and effects of complex information attacks. This includes information infrastructures and their vulnerabilities; attack modes; relationships between offensive cyber abilities and cyber-deterrence; and the relationship between cyber warfare and international legal norms. The subject also covers the components of cyber warfare, which is exploration and acquisition of information; the methodology of cyberattacks and the links between cyber defense and strategy. Understanding the relationships of cyber warfare with information operations; electronic warfare; media coverage and influence, as well as cyber terrorism.

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

Tudása: Átlátja a kibertérrel kapcsolatos diplomáciai, illetve politikai információmegosztás folyamatát, valamint az esetleges válaszlépéseket. Ismeri a kibertámadás esetén alkalmazandó eljárásokat és a kibertármadások összefüggéseit és hatásmechanizmusát.

Képességei: Képes átlátni a kibertér aktuális fenyegetéseit.

Attitűdje: Megérti és elfogadja a kiberhadviselés komplexitását, ennek köszönhetően a munkája során törekszik a védelem komplexitásának a kezelésére.

Autonómiája és felelőssége: Önállóan és pontosan vesz részt a kiberbiztonsági fenyegetések technológiai, politikai és adminisztratív megoldásában.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: The student is familiar with the procedure of diplomatic and political information sharing related to cyberspace, as well as possible responses as well as the procedures in cyber warfare, its coplexity and mechanism of its effects.

Capabilities: Understanding the current threats of cyber space.

Attitude: An understanding and acceptance of the complexity of international cyber law and thus strives to handle this complexity in his/her work.

Autonomy and responsibility: To take part in providing technological, political and administrative solutions to cyber threats.

11. Előtanulmányi követelmények: -

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

12.1. A komplex információs támadások összetevőivel és hatásai (Complex information attacks and their components and effects);

12.2. Az információs infrastruktúrák és támadható pontjaik (Information infrastructures and their vulnerabilities);

12.3. A támadási módok (Attack modes);

12.4. Az offenzív kiberműveleti képességek és a kiberelrettentés összefüggései (Relationships between offensive cyber capabilities and cyber-deterrence);

12.5. A kiberhadviselés és a nemzetközi jogi normák öszefüggései (Relationships between cyber warfare and international legal norms);

12.6. A felderítés és információszerzés (Intelligence and information gathering);

12.7. A kibertámadások módszertana (The methodology of cyberattacks);

12.8. A kibervédelem és stratégia összefüggései (Links between cyber defense and strategy);

12.9. Az információs műveletek, elektronikai hadviselés médiahadviselés és a befolyásolás (Information operations, electronic warfare, media warfare and influence);

12.10. A kiberterrorizmus (Cyber terrorism).

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 tantárgy elfogadásához a tanórák legalább 70 %-án jelen kell lennie a hallgatónak. A távollétet a hiányzást követő első foglalkozáson kell igazolnia. Hiányzás esetén hallgató köteles az előadás anyagát beszerezni, abból önállóan felkészülni.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A félév során 1 zh kerül megírásra az utolsó elődást követően. A zárthelyi dolgozat értékelése ötfokozatú skálán történik az alábbiak szerint: 51 %-tól elégséges, 63 %-tól közepes, 75 %-tól jó, 87 %-tól jeles. A meg nem írt, vagy sikertelen zárthelyi dolgozat miatt megtagadott aláírás a TVSZ vonatkozó pontjai szerint pótolható a szorgalmi időszak végéig.

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

16.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele a tanórák legalább 70 %-án való hallgatói jelenlét és a ZH

legalább elégséges szintű értékelése.

16.2. Az értékelés:

Típusa: szóbeli vizsga (kollokvium) . A szóbeli vizsga a szorgalmi időszak végéig kiadott kérdések alapján történik. Az értékelés szintjei: jeles (5), jó (4), közepes (3), elégséges (2), elégtelen (1).

16.3. A kreditek megszerzésének feltételei:

A kreditek megszerzésének feltétele az aláírás megszerzése és legalább elégséges kollokvium (K).

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. Kovács László (2018): A kibertér védelme. Dialóg Campus, Budapest, 2018., ISBN 978-615-5889-63-9 (nyomtatott)ISBN 978-615-5889-64-6 (elektronikus);
2. Kovács László (2018): Kiberbiztonság és-stratégia. Dialóg Campus, Budapest, 2018., ISBN 978-615-5920-92-9 (nyomtatott)ISBN 978-615-5920-93-6 (elektronikus).

17.2. Ajánlott irodalom:

1. Jason Andress, Steve Winterfeld (2013): Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. Syngress, ISBN 978-0124166721;
2. N Schmitt, Michael (szerk.): Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, 2017. ISBN: 9781316822524.

Budapest, 2021.01.05.

Dr. Kovács László, PhD,
egyetemi tanár sk.

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, 2021.01.05.

Dr. Krasznay Csaba, PhD,
egyetemi docens sk.

NEMZETI KÖZSZOLGÁLATI EGYETEM
Államtudományi és Nemzetközi Tanulmányok Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** ÁKINTM11
2. **A tantárgy megnevezése (magyarul):** Közmenedzsment
3. **A tantárgy megnevezése (angolul):** Public Management
4. **Kreditérték és képzési karakter:**
   - **4.1.** 2 kredit
   - **4.2.** a tantárgy elméleti vagy gyakorlati jellegének mértéke: 0% gyakorlat, 100% 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. Budai Balázs, PhD, egyetemi docens
8. **A tanórák száma és típusa**

   8.1. össz óraszám/félév:

   8.1.1. nappali munkarend: 28 (28 EA + 0 GY)

   8.1.2. levelező munkarend: 8 (8 EA + 0 GY)

   8.2. heti óraszám - nappali munkarend: 2 (2 EA + 0 GY)

   8.3. Az ismeret átadásában alkalmazandó további sajátos módok, jellemzők: -

9. **A tantárgy szakmai tartalma (magyarul):** A tantárgy átfogó ismereteket közvetít a közmenedzsment főbb tárgyalási területeiről, alapfogalmairól. Kitér azokra a menedzsment területekre és technikákra, amelyek mellőzése egy korszerű közigazgatási szervezet működésében elképzelhetetlen. Az átfogó megközelítést a tantárgy második felében több, kiemelt, funkcionális terület tárgyalása veszi át. Azon területeké, amelyeket szak más tantárgyai nem érintenek.

   A tantárgy szakmai tartalma (angolul) (Course description): The course conveys the overall knowledge of public managements basic concepts and key areas. It covers those areas and management technics, which can't be ignored in a modern, public administrational organisation. Some emphasized, functional area takes over the comprehensive approach at the second part of the subject. Those areas, which are not covered by program's other subjects.

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

    Tudása: Ismerni fogják az alapfogalmakat, használni fogják tudni az interaktív technikákat. Felismerik a tudásmenedzsment, a minőségmenedzsment, a teljesítménymenedzsment és más atipikus üzleti módszertanok alkalmazási lehetőségeit a közigazgatásban, látni fogják ezek hatékonysági mérési lehetőségeit. megoldásokra. Megérti a szervezeti feladatokat a kibervédelemben.

    Képességei: Képes támogatni szervezetét a kibervédelmi képességek kialakításában.

    Attitűdje: Nyitottakká vállnak az innovatív közigazgatási megoldásokra.

    Autonómiája és felelőssége: Értékkötelezett módon vesz részt a kibertér komplexitásának és kölcsönhatásainak ismerete által a különböző hivatásrendek feladatainak szervezésében. Gyakorlatába beépíti és alkalmazza az e szakterületen folyó kutatások eredményeit.

    Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: They will know the basic concepts, they will be able to use interactive techniques. They can recognize the knowledge management's, quality management's, performance management's and other business methodologies's atypical adaptation opportunities in the public sector, and they will see its performance measurement capabilities. Is familiar with organisational tasks in cyber security.

Capabilities: Students will be able to evaluate the place and role of the public management. They will understand and form an opinion on the strategic plans.

Attitude: They will become open for the innovative administrative solutions.

Autonomy and responsibility: Autonomy and responsibility to take part in organising tasks of the various professions by having an overview of the complexity and interactions of cyber space. Autonomy and responsibility to put the results of scientific research in the field into his/her practice.

11. Előtanulmányi követelmények: -

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

12.1. A közigazgatási menedzsment meghatározása, elhelyezkedése a szervezéstudomány rendszerében (Definition of public administrative management and its position in the system of organizational science);

12.2. A közmenedzsment alapfogalmai és irányzatainak fejlődéstörténete (Development history of the basic concepts and trends of public management);

12.3. A szervezési munka általános modellje (General model of organizational work);

12.4. Interaktív technikák a közigazgatásban (Interactive techniques in public administration);

12.5. Stratégiai alapfogalmak (Strategic basic terms);

12.6. Stratégiai irányzatok, alapmodellek (Strategic trends, basic models);

12.7. A stratégiai tervezés módszertana (Methodology of strategic planning);

12.8. Stratégiai tervezés a közigazgatásban (Strategic planning in public administration);

12.9. Emberi Erőforrás Menedzsment (Human resource Management);

12.10. A jövő stratégiaformáló irányzatai - geostratégia (The future trends shaping strategy – Geostrategic);

12.11. Tudásmenedzsment a közigazgatásban (Knowledge management in public administration);

12.12. Minőségmenedzsment és teljesítménymenedzsment a közigazgatásban (Quality management and performance management in public administration);

12.13. Az üzleti szféra atipikus menedzsment módszerei a közigazgatásban (Methods of atypical business management in public administration);

12.14. Informatikai menedzsment(IT management);

12.15. A közmenedzsment hatékonyságának mérése (Measuring the efficiency of public management).

13. A tantárgy meghirdetésének gyakorisága/a tantervben történő félévi elhelyezkedése: 3. 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 és a gyakorlat anyagát beszerezni, abból önállóan felkészülni.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje:

Csoportmunka-feladat, a félév elején ismertetett témakörből.

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

16.1. Az aláírás megszerzésének feltételei:

A csoportmunka teljesítése és a foglalkozások látogatása a tematika szerint.

16.2. Az értékelés:

Írásbeli számonkérés, öt fokozatú értékeléssel: 0-50% - elégtelen, 51-70% - elégséges, 71-80% - közepes, 81-90% - jó, 91-100% - jeles.

16.3. A kreditek megszerzésének feltételei:

A kreditek megszerzésének feltétele az aláírás megszerzése és legalább elégséges évközi értékelés (ÉÉ).

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. Budai Balázs: Az e-közigazgatás elmélete (második, átdolgozott kiadás) Akadémiai Kiadó, Budapest, 2014.;
2. Budai Balázs: A közigazgatás újragondolása; Akadémiai Kiadó, Budapest, 2017.;
3. Almásy Gyula – Belényesi Emese –Gáspár Mátyás (2015): Önkormányzati szervezetfejlesztés. Nemzeti Közszolgálati Egyetem;
4. Almásy Gyula: Bevezetés a közigazgatási menedzsmentbe, E-Government Alapítvány, Budapest, 2012.

17.2. Ajánlott irodalom:

1. Antal Zsuzsanna - Drótos György - Kiss Norbert - Kováts Gergely - Révész Éva - Varga Polyák Csilla (2011): Közszolgálati szervezetek vezetése. Egyetemi jegyzet. Aula Kiadó, Budapest;
2. Horváth M. Tamás: Közmenedzsment, Dialog Campus, Budapest, 2012.;
3. Nemes Ferenc: Vezetési ismeretek és módszerek. Szent István Egyetemi Kiadó. 2007.

Budapest, 2021.01.05.

Dr. Budai Balázs, PhD,
egyetemi docens sk.

NEMZETI KÖZSZOLGÁLATI EGYETEM
Hadtudományi és Honvédtisztképző Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** HKKNBM04
2. **A tantárgy megnevezése (magyarul):** Közszolgálati információs rendszerek védelme
3. **A tantárgy megnevezése (angolul):** Protection of information systems for public services
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):** kiberbiztonsági MA
6. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** Hadtudományi és Honvédtisztképző Kar, Katonai Nemzetbiztonsági Tanszék
7. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Magyar Sándor, PhD, adjunktus
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 képzésben résztvevő hallgatók átfogó módon ismerkedhetnek meg a magyar közszolgálati információs rendszerek védelmét szabályozó jogszabályokkal, valamint a védelem eszközeinek alapjaival. Az elméleti ismeretek elsajátítása interaktív szamináriumi foglalkozások keretében valósul meg. Az előadások rámutatnak az egyes védelmi elemek kapcsolódási pontjaira, egymáshoz való viszonyára is.

   A tantárgy szakmai tartalma (angolul) (Course description): The students participating in the course will get a comprehensive introduction to the background of legistlation and regulation on the protection of hungarian information systems for public service and the basics of the means and methods of protection. Theoretical knowledge is acquired through interactive seminars. The presentations also point out the connections of each defense element and their relation to each other.

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

Tudása: Ismeri a nemzetközi jog alkalmazhatóságát a kibertérben. 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.

Képességei: Képes olyan technológiai védelmi intézkedések meghozatalára, amelyek a cyber kill chain egyes elemeihez kapcsolódnak. Képes támogatni szervezetét a kibervédelmi képességek kialakításában.

Attitűdje: Hatékony lépéseket tesz a kibertámadások megelőzése érdekében, így csökkentve a szervezete kitettségét.

Autonómiája és felelőssége: Vállalja a szakterület, a szakmai praxis módszertanának fejlesztéséhez szükséges elméleti, tudományos kutatási és gyakorlati információk beszerzésének, értékelésének és hasznosításának végrehajtását.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: The applicability of international law in cyberspace. The need for introducing internal regulations defined by employers in order to maintain integrity and availability of the data stored in information systems. Organisational tasks in cyber security.

Capabilities: Is capable of supporting his/her organisation in developing cyber security skills. Is capable of taking technological defensive measures related to elements of the cyber kill chain.

Attitude: An effort to take effective measures in order to prevent cyber attacks, by this means reducing the exposure of his/her organisation.

Autonomy and responsibility: To obtain, evaluate and utilize theoretical, scientific and practical information necessary for the improvement of the field and the methodology of professional practice.

11. Előtanulmányi követelmények: -

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

12.1. Állami és önkormányzati rendszerek védelmének alapjai (2013. évi L. törvény., 41/2015. (VII. 15.) BM., 185/2015. (VII. 13.) Korm. rendelet, 186/2015. (VII. 13.) Korm. rendelet, 187/2015. (VII. 13.) Korm. rendelet) Fundamentals of the Protection of State and Local Government Systems (Act L. of 2013, Government Decree 41/2015 (VII. 15.) BM., 185/2015 (VII. 13.) Government Decree 186/2015 (VII. 13) .) Government Decree 187/2015 (VII. 13.) Government Decree);

12.2. Hazai kibervédelmi szervezetek (Domestic cyber defense organizations);

12.3. Kiberbiztonsági feladat és felelősségelhatárolás az állami és önkormányzati rendszereknél (Segregation of cybersecurity tasks and responsibilities in state and local government systems);

12.4. AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/1148 IRÁNYELVE (2016. július 6.) és a 410/2017. (XII.15.) Korm. rendelet (DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 and amending Regulation (EU) No 410/2017 (XII.15.) Government Decree);

12.5. Az állami és önkormányzati létfontosságú információs infrastruktúrák védelme (Protection of state and municipal critical information infrastructures);

12.6. A védelem eszközei: Információbiztonság alapok, megfontolások (The means and methods of protection: basics os information security, considerations);

12.7. Biztonsági kizárások: incidensek megelőzése, kezelése: védelmi technológiák, folyamatok, proaktív – preventív – reaktív védelem, sérülékenység-menedzsment, sérülékenységvizsgálatok, vizibilitás biztosítása (Security exclusions: incident prevention and management: defense technologies, processes, proactive - preventive - reactive protection, vulnerability management, vulnerability testing, provision of visibility);

12.8. Biztonságos beengedések: hitelesítés, engedélyezés, hozzáférés-kezelési technológiák, kiemelt jogosultsággal rendelkezők kezelése (Secure access: authentication, authorization, access management technologies, privileged management);

12.9. Kockázatmenedzsment: kockázatkezelési alapelvek, GRC (Governance, risk management, and compliance) rendszere (Risk management: principles of risk management, GRC (Governance, risk management, and compliance) system).

13. A tantárgy meghirdetésének gyakorisága/a tantervben történő félévi elhelyezkedése: 3. félév

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

A hallgató köteles az előadások legalább 80%-án részt venni. Rövid/tartós távolmaradás indokolt esetben (orvosi, szolgálati) pótolható, amely pótlás egyéni megbeszélés szerint történik.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A félév során minden tanulónak egy, a félév elején kiadott listából választott témából kiselőadást kell tartania. A kiselőadás ötfokozatú skálán kerül értékelése. Az elméleti anyagából egy évközi ZH sikeres, legalább elégséges (kettes) érdemjegyre történő megírása. A zárthelyi dolgozat értékelése: ötfokozatú értékelés – (a helyes válaszok aránya 0-60% elégtelen; 61-70% elégséges; 71-80% közepes; 81-90% jó; 91-100% jeles osztályzat). Eredménytelen zárthelyi dolgozat kétszer javítható.

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

16.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele a Foglalkozásokon való részvétel pontban meghatározott arányú részvétel a foglalkozásokon és a Félévközi feladatok, ismeretek ellenőrzésének rendje pontban meghatározott félévközi feladatok legalább elégséges teljesítése.

16.2. Az értékelés:

A félév értékelése gyakorlati jegy a tanórai aktivitás (20%), a megtartott kiselőadás (40%) és a zárthelyi dolgozat (40%) eredményéből .

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. 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról;
2. 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről41/2015. (VII. 15.) BM;
3. 185/2015. (VII. 13.) Korm. rendelet a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól;
4. AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/1148 IRÁNYELVE (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről
5. Kovács Zoltán– Mikó Zoltán – Sági Gábor: A biztonság, mint szolgáltatás megteremtése az állami, önkorm ányzati elektronikus információs rendszereknél I.-II. Belügyi Szemle, 2018/4-5.

17.2. Ajánlott irodalom:

1. Muha Lajos – Krasznay Csaba: Az elektronikus információs rendszerek biztonságának menedzselése Nemzeti Közszolgálati Egyetem. 2018., ISBN: 978- 615-5870-27-9;
2. Anne Kohnke, Ken Sigler (2017): Implementing Cybersecurity: A Guide to the National Institute of Standards and Technology Risk Management Framework. Auerbach Publications, ISBN 978-1498785143;
3. NIST Special Edition 800-as sorozat;
4. Magyar Informatikai Biztonság Irányítási Keretrendszer (MIBIK) – KIB 25. számú ajánlás 1., 1-1., 1-2., 1-3. kötete, Budapest, 2008.

Budapest, 2021.01.05.

Dr. Magyar Sándor, PhD,
adjunktus sk.

NEMZETI KÖZSZOLGÁLATI EGYETEM
Hadtudományi és Honvédtisztképző Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** HKKNBM06
2. **A tantárgy megnevezése (magyarul):** Kriptográfia a közszolgálatban
3. **A tantárgy megnevezése (angolul):** Cryptography in the public service
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):** kiberbiztonsági MA
6. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** Hadtudományi és Honvédtisztképző Kar, Katonai Nemzetbiztonsági Tanszék
7. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Magyar Sándor, PhD, adjunktus
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 kurzus bemutatja a kriptográfia történetét, a titkosítás alkalmazási területeit. Foglalkozik a kriptográfiai alapfogalmaival, a szteganográfiával, a főbb titkosítási fajtákkal (Hash, Symmetric, Asymmetric).l egyaránt. Ismerteteti a tanúsítványok és az elektronikus aláírás gyakorlatát. Bemutatja a kriptográfiai megoldások elleni támadásokat.

   A tantárgy szakmai tartalma (angolul) (Course description): The course will introduce the history of cryptography and the applications of encryption. It deals with basic cryptographic concepts, steganography, and major types of encryption (Hash, Symmetric, Asymmetric). Describes the practice of certificates and electronic signatures. Introduces attacks on cryptographic solutions.

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

Tudása: Ismeri a kriptográfia történetének alapjait, ismeri a titkosítás megoldásait, tisztában van a kriptográfia alkalmazásával, támadási lehetőségeivel.

Képességei: Képes értelmezni a jogszabályokból eredő, incidenskezelésre és jelentésre vonatkozó követelményeket.

Attitűdje: Hatékony lépéseket tesz a kibertámadások megelőzése érdekében, így csökkentve a szervezete kitettségét.

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

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: He/she is familiar with the history of cryptography and the use of cryptography.

Capabilities: Is capable of supporting his/her organisation in developing cyber security skills. Is capable of taking technological defensive measures related to elements of the cyber kill chain.

Attitude: An effort to take effective measures in order to prevent cyber attacks, by this means reducing the exposure of his/her organisation.

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

11. Előtanulmányi követelmények: Biztonsági technológiák alkalmazása [ÁKINTM06]

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

12.1. A kriptográfia története (History of cryptography);

12.2. Kriptográfiai alapfogalmak (Basic cryptographic concepts);

12.3. Titkosítás alkalmazási területei (Applications of encryption);

12.4. Szteganográfia (Steganography);

12.5. Gyakorlat 1. (practical course 1.);

12.6. Szimmetrikus (titkos) kulcsú rendszerek (Symmetric key systems);

12.7. Gyakorlat 2. (practical course 2.)

12.8. Aszimmetrikus (nyilvános) kulcsú rendszerek (Asymmetric key systems);

12.9. Gyakorlat 3. (practical course 3.);

12.10. Tanúsítványok és elektronikus aláírás (Certificates and electronic signatures);

12.11. Gyakorlat 4. (practical course 4.);

12.12. Titkosítás elleni támadások (Attacks agains Encryption);

12.13. Gyakorlat 5. (practical course 5.)

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 tantárgy elfogadásához a tanórák legalább 70 %-án jelen kell lennie a hallgatónak. A távollétet a hiányzást követő első foglalkozáson kell igazolnia. Hiányzás esetén a hallgató köteles az előadás anyagát beszerezni, abból önállóan felkészülni.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A tanulmányi munka alapja a szemináriumok látogatása, az előírt olvasmányok ismerete. A hallgató a félév során kettő feleletválasztós tesztet ír. Az elérendő teljesítmény százaléka 60 %-tól elégséges, 70 %-tól közepes, 80-tól % jó, 90 %-tól jeles. A félév végén egy vizsgafeladat gyakorlati megvalósítása. A félévközi feladatok összesítéséből áll a gyakorlati jegy. A TVSZ rendezi a sikertelen értékelés-összetevő javítását.

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

16.1. Az aláírás megszerzésének feltételei:

A foglalkozásokon való részvétel meghatározott aránya, illetve a félévközi feladatok teljesítése.

16.2. Az értékelés:

A gyakorlati jegy a 2 félévközi feleltválasztós teszt értékeléséből és a vizsgafeladatra adott érdemjegyekből adódik.

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. Buttyán Levente, Vajda István (2004): Kriptográfia és alkalmazásai, Typotex Kft., Budapest, ISBN: 978-963-2796-96-3;
2. Virasztó Tamás (2004): Titkosítás és adatrejtés - Biztonságos kommunikáció és algoritmus adatvédelem. Netacademia, ISBN 9789632142531.

17.2. Ajánlott irodalom:

1. Schneier, Bruce (2015). Applied Cryptography: Protocols, Algorithms and Source Code in C. Wiley, ISBN 978-1119096726.

Budapest, 2021.01.05.

Dr. Magyar Sándor, PhD,
adjunktus sk.

NEMZETI KÖZSZOLGÁLATI EGYETEM
Rendészettudományi Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** VIBTM02
2. **A tantárgy megnevezése (magyarul):** Kritikus információs infrastruktúra védelem
3. **A tantárgy megnevezése (angolul):** Critical information infrastructure protection (CIIP)
4. **Kreditérték és képzési karakter:**
   - **4.1.** 3 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:** Rendészettudományi Kar, Polgári Nemzetbiztonsági Tanszék
7. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Dobák Imre, PhD, egyetemi docens
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):** Definíciós környezet evolúciója a kétezres évektől napjainkig, nemzetközi és hazai viszonylatban. A kritikus infrastruktúrák és kritikus információs infrastruktúrák értelmezése, összefüggések és eltérések. A kapcsolódó EU-s szabályozási környezet (a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló 2016/1148 Irányelv; az ENISA-ról és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről szóló 2019/881. EU rendelet; és kapcsolódó szabályozók). Magyarországi jogszabályi környezet. A hatósági és eseménykezelési tevékenység Magyarországon. Információbiztonsági követelményrendszer a kritikus információs infrastruktúrákra vonatkozóan.

   A tantárgy szakmai tartalma (angolul) (Course description): International and domestic evolution of the definitions from the 2000s to present days. Interpretation, relationships, and differences between critical infrastructures and critical information infrastructures. he related EU regulatory environment (Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union; on ENISA and on information and communications technology cybersecurity certification and repealing Regulation No 526/2013 (Cybersecurity Act), and related regulators). Legal environment in Hungary. Authorities and CSIRT's in Hungary. Cybersecurity requirements related to critical information infrastructures.

10. **Elérendő kompetenciák (magyarul):**
    Tudása: Ismeri a kritikus infrastruktúrák jogi szabályozási előírásait, ezen belül a kritikus információs infrastruktúrák fogalmát, rendszerelemeit, jellemzőit, veszélyeztető tényezőit. Magas szinten ismeri a kritikus információs infrastruktúrák védelmével foglalkozó nemzetközi és hazai szabályozást és annak hatósági alkalmazási rendjét.

Képességei: Képes a kritikus információs infrastruktúrák védelmével kapcsolatos jogszabályokból eredő követelmények, valamint a kapcsolódó hatósági és védelmi intézkedések meghatározására. Képes a kritikus információs infrastruktúra védelmi feladatok rendszerszemléletű megközelítésére és azok gyakorlati alkalmazására.

Attitűdje: Elkötelezett a kritikus információs infrastruktúrák védelmével kapcsolatos szabályozásokban foglaltak érvényesítésére. Elkötelezett a kibertámadások megelőzése iránt és ezt a tudatosság előmozdítása érdekében a szakmai és a szélesebb társadalmi közösség felé hitelesen közvetíti.

Autonómiája és felelőssége: Tudatosan törekszik a kritikus információs infrastruktúrák védelme és a kiberbiztonság sajátosságainak megfelelő, korszerű ismeretek hazai és nemzetközi szinten történő gyakorlati alkalmazására. Önállóan irányítja és tervezi a kritikus információs infrastruktúrák védelmét és a kiberbiztonságot érintő információk, problémák feldolgozását, illetve az ehhez kapcsolódó feladatok megszervezését és végrehajtását.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: Aware of the important requirements of critical infrastructures law including the concept, constituents, characteristics and threats to critical information infrastructures. High level of knowledge of international and domestic regulation of critical information infrastructure protection and its authority implementation.

Capabilities: Capable of determining the requirements from legislation of critical information infrastructure protection and the related regulatory and security measures implementation. Capable of a systematic approach to tasks of critical information infrastructure security and their practical application.

Attitude: Committed to enforcing regulations related to the protection of critical information infrastructures. Committed to preventing cyberattacks and authentically conveys this to the professional and social community in order to promote awareness.

Autonomy and responsibility: Consciously endeavour to ensure the practical application of modern knowledge at national and international level to protect of critical information infrastructures and to adapt to the specificities of cybersecurity. Independently manages and plans to process information and problems affecting critical information infrastructures and cybersecurity and to organise and carry out related tasks.

11. Előtanulmányi követelmények: Létfontosságú rendszerek és létesítmények védelme [VIBTM01]

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

12.1. A tantárgy programjának, illetve a tanulmányi követelmények ismertetése. Fogalomrendszerek és a kapcsolódó szakmai terminológia ismertetése. Definíciós környezet evolúciója a kétezres évektől napjainkig, nemzetközi és hazai viszonylatban (Description of the programme of the subject and the requirements for study. Description of concepts and related professional terminology. The evolution of the definition environment from the 2000s to the present day, internationally and domestically);

12.2. Nemzetközi kitekintés a kiberbiztonság fejlődése vonatkozásában. A kritikus infrastruktúrák és kritikus információs infrastruktúrák értelmezésének, összefüggéseinek és az eltérések bemutatása (International outlook on the development of cybersecurity. Description of the interpretation, context and divergence of critical infrastructures and critical information infrastructures);

12.3. A hálózati és információs rendszerek biztonságával kapcsolatos Európai Uniós szabályozási környezet ismertetése, külön részletezve az irányelvi és rendeleti kötelezettségeket a tagállamokban (Description of the regulatory environment in the European Union for the security of network and information systems, particular details of the obligations of directives and regulations in the Member States);

12.4. A hálózati és információs rendszerek biztonságával kapcsolatos magyarországi jogszabályi

követelmények ismertetése, beleértve a szervezeti rendszert, a felelősségi köröket és a kötelezettségeket (Description of the legal requirements in Hungary relating to the security of network and information systems, including the organisational system, responsibilities and obligations);

12.5. A kibertámadások megelőzésére vonatkozó eszközök és módszerek bemutatása a hatósági feladatrendszerek keretében, valamint a kritikus információs infrastruktúrákat érintő események kezelésének szabályai, folyamata (Presentation of the tools and methods for preventing cyber-attacks in the framework of authority task systems and the rules and processes for managing events affecting critical information infrastructures);

12.6. Információbiztonsági követelmények értelmezése és nevesítése a kritikus információs infrastruktúrák kapcsán (Interpretation and naming of information security requirements for critical information infrastructures);

12.7. Zárthelyi dolgozat (Classroom test).

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 foglalkozásokon a részvétel kötelező (minimum 70%); rövid/tartós távolmaradás indokolt esetben (orvosi, szolgálati) pótolható, amely pótlás egyéni megbeszélés szerint történik. A hallgató köteles az előadás anyagát beszerezni, abból önállóan felkészülni.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A tanulmányi munka alapja nappali és levelező munkarendű képzésben az előadások rendszeres látogatása (a 14. pont szerint), a foglalkozások témájából (a 12. pont szerint) a szorgalmi időszakban zárthelyi dolgozat megírása. A zárthelyi dolgozat értékelése: ötfokozatú értékelés – (a helyes válaszok aránya 0-60% elégtelen; 61-70% elégséges; 71-80% közepes; 81-90% jó; 91-100% jeles osztályzat). Eredménytelen zárthelyi dolgozat kétszer javítható.

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

16.1. Az aláírás megszerzésének feltételei:

A foglakozás anyagainak és a kötelező irodalom feldolgozása, az előadásokon való igazolt részvétel, a zárhelyi dolgozat eredményes teljesítése. Eredményes a zárthelyi dolgozat, ha a helyes válaszok elérik a több mint 60%-ot.

16.2. Az értékelés:

Zárthelyi dolgozat a tantárgy tematikájából és a kötelező irodalomból összeállított feladatlap felhasználásával a gyakorlati jegy megszerzéséhez. A hatályos TVSZ szerinti ötfokozatú értékelési rendszer alkalmazása.

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. Bonnyai Tünde- Danyek Miklós- Görgey Péter- Kriskó Edina- Molnár Anna- Tikos Anita: Kritikus információs infrastruktúrák védelme (éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára). Budapest, Magyarország, Nemzeti Közszolgálati Egyetem, Közigazgatási Továbbképzési Intézet 2019.;
2. Bonnyai Tünde- Bognár Balázs- Vámosi Zoltán: Kritikus infrastruktúrák védelme I. Budapest, Magyarország, Dialóg Campus Kiadó-Nordex Kft (2019) ISBN: 9786155920363;
3. Haig Zsolt- Kovács László: Kritikus infrastruktúrák és kritikus információs infrastruktúrák.

Tanulmány 2012. Nemzeti Közszolgálati Egyetem, TÁMOP 4.2.2/B-10/1-2010-0001.

17.2. Ajánlott irodalom:

1. Nyikes Zoltán: Az információbiztonság növelése a felhasználó támogatásának lehetőségeivel. Doktori (PhD) értekezés. 2019.;
2. Molnár Dóra: Törékeny nagyhatalmiság: a kiberbiztonság – Az európai kibertér brit, német és francia szegmensei. Budapest, Magyarország, Nemzeti Közszolgálati Egyetem, Közigazgatási Továbbképzési Intézet 2018.;
3. Puskás Béla: A kritikus információs infrastruktúrák biztonságos üzemeltetésének vizsgálata hálózatelméleti megközelítésből, az ember-technika-környezet relációjában. Doktori (PhD) értekezés. 2017.;
4. Muha Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme. Doktori (PhD) értekezés. 2007.

Budapest, 2021.01.05.

Dr. Dobák Imre, PhD,
egyetemi docens sk.

NEMZETI KÖZSZOLGÁLATI EGYETEM
Rendészettudományi Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** VIBTM01
2. **A tantárgy megnevezése (magyarul):** Létfontosságú rendszerek és létesítmények védelme
3. **A tantárgy megnevezése (angolul):** Critical Infrastructure Protection
4. **Kreditérték és képzési karakter:**
   - **4.1.** 3 kredit
   - **4.2.** a tantárgy elméleti vagy gyakorlati jellegének mértéke: 0% gyakorlat, 100% elmélet
5. **A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):** kiberbiztonsági MA
6. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** Rendészettudományi Kar, Katasztrófavédelmi Műveleti Tanszék
7. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Vass Gyula, PhD, egyetemi docens
8. **A tanórák száma és típusa**
   - **8.1.** össz óraszám/félév:
     - 8.1.1. nappali munkarend: 28 (28 EA + 0 GY)
     - 8.1.2. levelező munkarend: 8 (8 EA + 0 GY)
   - **8.2.** heti óraszám - nappali munkarend: 2 (2 EA + 0 GY)
   - **8.3.** Az ismeret átadásában alkalmazandó további sajátos módok, jellemzők: -
9. **A tantárgy szakmai tartalma (magyarul):** Iparbiztonság a katasztrófavédelem rendszerében. A létfontosságú rendszerek és létesítmények védelmével (kritikus infrastruktúra védelem, KIV) kapcsolatos nemzetközi és hazai szabályozás. Az ágazati és katasztrófavédelmi feladatok, hatáskörök, KIV üzemeltetői követelmények és azok végrehajtása. A KIV elemekkel kapcsolatos tervezési, dokumentáció-készítési, hatósági és ellenőrzési, információbiztonsági szektor-specifikus feladatellátás.

   A tantárgy szakmai tartalma (angolul) (Course description): Industrial safety in the disaster management system. International and domestic safety regulation for critical system and facility protection (critical infrastructure protection, CIP). Sectoral and disaster management tasks and competencies, CIP operator duties and their implementation. Sector-specific elements tasks to planning, documentation, authority and control, information security activities related to CIP.

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

Tudása: Ismeri az iparbiztonsági szakterület jogi szabályozási előírásait, ezen belül a létfontosságú rendszerelemek fogalmát, rendszerelemeit, létesítménycsoportjainak jellemzőit, veszélyeztető tényezőit. Magas szinten ismeri a kritikus infrastruktúra védelem nemzetközi és hazai szabályozását és annak hatósági alkalmazási rendjét. Mélyrehatóan ismeri a kritikus infrastruktúra védelem hazai szabályozási környezetében elkülönített ágazati sajátosságokat.

Képességei: Képes a kritikus infrastruktúra védelemmel kapcsolatos jogszabályokból eredő követelmények, valamint a kapcsolódó hatósági és védelmi intézkedések meghatározására. Képes a kritikus infrastruktúra védelmi feladatok rendszerszemléletű megközelítésére és azok gyakorlati alkalmazására.

Attitűdje: Elkötelezett a létfontosságú rendszerek védelmével és a kiberbiztonsággal kapcsolatos szabályozásokban foglaltak érvényesítésére. Elkötelezett a kibertámadások megelőzése iránt és ezt a tudatosság előmozdítása érdekében a szakmai és a szélesebb társadalmi közösség felé hitelesen

közvetíti.

Autonómiája és felelőssége: Tudatosan törekszik a létfontosságú rendszerek védelme és a kiberbiztonság sajátosságainak megfelelő, korszerű ismeretek hazai és nemzetközi szinten történő gyakorlati alkalmazására. Önállóan irányítja és tervezi a létfontosságú rendszerek védelmét és a kiberbiztonságot érintő információk, problémák feldolgozását, illetve az ehhez kapcsolódó feladatok megszervezését és végrehajtását.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: Aware of the important requirements of industrial safety law including the concept of critical system components, system elements, characteristics and hazards of groups of facilities. High level of knowledge of international and domestic regulation of critical infrastructure protection and its authority implementation. In-depth knowledge of sector specificities in the domestic regulatory for critical infrastructure protection.

Capabilities: Capable of determining the requirements from critical infrastructure protection legislation and the related regulatory and security measures implementation. Capable of a systematic approach to critical infrastructure security tasks and their practical application.

Attitude: Committed to enforcing regulations related to the protection of critical systems and cybersecurity. Committed to preventing cyberattacks and authentically conveys this to the professional and social community in order to promote awareness.

Autonomy and responsibility: Consciously endeavour to ensure the practical application of modern knowledge at national and international level to protect critical systems and to adapt to the specificities of cybersecurity. Independently manages and plans to process information and problems affecting critical systems and cybersecurity and to organise and carry out related tasks.

11. Előtanulmányi követelmények: -

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

12.1. Biztonságpolitikai alapismeretek, EU Biztonsági Stratégia, nemzeti stratégiák, hazai megközelítések. Az infrastruktúrákat veszélyeztető tényezők (Basic knowledge of security policy, EU Security Strategy, national strategies, national approaches. Risks to infrastructures);

12.2. Infrastruktúra és kritikus infrastruktúra definíciós környezete. NATO és EU létfontosságú rendszerek (kritikus infrastruktúrák) védelme és szabályozása (Definition for infrastructure and critical infrastructure. Protection and regulation of NATO and EU critical systems (critical infrastructure));

12.3. A létfontosságú rendszerek védelmének szabályozása Magyarországon. Ágazatok és általános jellemzőik. A KIV elemek felmérése, azonosítása és kijelölése. Ágazati hatósági feladatok teljesítése (Regulation of protection of critical systems in Hungary. Sectors and their general characteristics. Assess, identify and designate CIP elements. Implementation of sectoral authority duties);

12.4. A katasztrófavédelem hatósági tevékenysége központi, területi és helyi szinten. Az üzemeltetői biztonsági terv készítésének célja és alapvető módszere, a biztonsági összekötő szerepe (Disaster management authority activity at central, regional and local level. The purpose and basic method of preparing the operator security plan, the role of the security liaison);

12.5. A horizontális kritériumok vizsgálatának folyamata, az érintett szervezetek feladatai. Hatályos ágazati szabályozással rendelkező ágazatokra vonatkozó követelmények (The process of examining the horizontal criteria, the tasks of the organisations concerned. Sectors with existing sectoral regulations);

12.6. Információbiztonsági feladatellátás a kritikus infrastruktúrák védelme kapcsán (Information security task provision for critical infrastructure protection);

12.7. Zárthelyi dolgozat (Classroom test).

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 foglalkozásokon a részvétel kötelező (minimum 70%); rövid/tartós távolmaradás indokolt esetben (orvosi, szolgálati) pótolható, amely pótlás egyéni megbeszélés szerint történik. A hallgató köteles az előadás anyagát beszerezni, abból önállóan felkészülni.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A tanulmányi munka alapja nappali és levelező munkarendű képzésben az előadások rendszeres látogatása (a 14. pont szerint), a foglalkozások témájából (a 12. pont szerint) a szorgalmi időszakban ZH dolgozat megírása. A zárthelyi dolgozat értékelése: ötfokozatú értékelés – (a helyes válaszok aránya 0-60% elégtelen; 61-70% elégséges; 71-80% közepes; 81-90% jó; 91-100% jeles osztályzat). Eredménytelen zárthelyi dolgozat kétszer javítható.

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

16.1. Az aláírás megszerzésének feltételei:

A foglakozás anyagainak és a kötelező irodalom feldolgozása, az előadásokon való igazolt részvétel, a ZH dolgozat eredményes teljesítése. Eredményes a zárthelyi dolgozat, ha a helyes válaszok elérik a több mint 60%-ot.

16.2. Az értékelés:

Zárthelyi dolgozat a tantárgy tematikájából és kötelező irodalomból összeállított feladatlap felhasználásával. A hatályos TVSZ szerinti ötfokozatú értékelési rendszer alkalmazása.

16.3. A kreditek megszerzésének feltételei:

A kreditek megszerzésének feltétele az aláírás megszerzése és legalább elégséges évközi értékelés (ÉÉ).

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. Bonnyai, Tünde - Bognár, Balázs ; Vámosi, Zoltán: Kritikus infrastruktúrák védelme I. Budapest, Magyarország : Dialóg Campus Kiadó-Nordex Kft (2019) ISBN: 9786155920363;
2. Haig Zsolt - Kovács László: Kritikus infrastruktúrák és kritikus információs infrastruktúrák. Tanulmány 2012. Nemzeti Közszolgálati Egyetem, TÁMOP 4.2.2/B-10/1-2010-0001;
3. Ted G. Lewis (2014): Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. Wiley, ISBN 978-1118817636
4. Bonnyai Tünde: A kritikus infrastruktúra védelem elemzése a lakosságfelkészítés tükrében. Doktori (PhD) értekezés. 2014.
5. Fejezetek a kritikus infrastruktúra védelemből – tanulmánykötet. Magyar Hadtudományi Társaság, Budapest, 2013. ISBN 978-963-08-6926-3

17.2. Ajánlott irodalom:

1. Bognár Balázs, Bonnyai Tünde, Görög Katalin, Katai-Urban Lajos, Vass Gyula: Létfontosságú rendszerek és létesítmények védelme (kézikönyv a katasztrófavédelmi feladatok ellátására), NKE KVI, Budapest, 2015, ISBN 978-615-5057-52-6, ISBN 978-615-5057-49-6 ISBN 978-615-5057-50-2 (on-line);
2. Bognár Balázs, Kátai-Urbán Lajos, Kossa György, Kozma Sándor, Szakál Béla, Vass Gyula: Iparbiztonságtan I: Kézikönyv az iparbiztonsági üzemeltetői és hatósági feladatok ellátásához. Budapest: Nemzeti Közszolgálati és Tankönyv Kiadó Zrt., 2013. 564 p. (ISBN:978-615-5344-12-1).

Budapest, 2021.01.05.

Dr. Vass Gyula, PhD,
egyetemi docens sk.

NEMZETI KÖZSZOLGÁLATI EGYETEM
Államtudományi és Nemzetközi Tanulmányok Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** ÁTKTM05
2. **A tantárgy megnevezése (magyarul):** Válságmenedzsment és kommunikáció
3. **A tantárgy megnevezése (angolul):** Crisis management and communication
4. **Kreditérték és képzési karakter:**
   - **4.1.** 3 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, Társadalmi Kommunikáció Tanszék
7. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Kriskó Edina, PhD, adjunktus
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 kurzus hallgatói megismerkednek a vállalati krízisek kialakulásának főbb motívumaival, valamint betekintést nyerhetnek a hatékony kríziskommunikáció alapvető jellemzőivel. Esettanulmányokon keresztül jó gyakorlatokkal is megismerkednek.

   A tantárgy szakmai tartalma (angolul) (Course description): The students will be introduced to the main patterns of the professional institutions' crises, and will get an insight into the basic features of a successful crisis communication. Through case studies they will be familiar with the best practices of the field.

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

Tudása: Ismeri a nemzetközi tárgyalások és kommunikáció, illetve a közösségi média nemzetközi kapcsolatokban betöltött szerepét és a protokoll jellemzőit a közszolgálatban. Ismeri a hazai közszolgálati életpályák jellemzőit, a közszolgálatra vonatkozó jogszabályokat és a nemzetközi szervezetekben való alkalmazás feltételeit.

Képességei: Képes hatékony közszolgálati kommunikációra − eredményes tárgyalási és együttműködési technikák alkalmazására − és az ügyfelekkel való ügy- és ügyfélorientált kommunikációra. Képes a kreatív és megoldásközpontú munkavégzésre.

Attitűdje: Alkalmazkodik a változó munkateherhez és kellően flexibilis. Érzékeny és nyitott a társadalmi problémákra, szemléletét áthatja a szakmai és emberi szolidaritás.

Autonómiája és felelőssége: Szervezeti struktúrában elfoglalt helyének megfelelő önállósággal és felelősséggel és a hivatali út betartásával szervezi munkáját és az irányítása alatt dolgozó munkatársak tevékenységét.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: The role of international negotiations and communication and social media in international relations, and the characteristics of protocol in public service. The characteristics of career paths in public service in Hungary, legislation of public service and its relevance in international organisations.

Capabilities: Interpreting duties, tasks and procedures arising from international connections, membership and other organisational relations and of utilising these in the decision-making procedure of the public service organisation. Working creatively and focusing on solutions.

Attitude: An ability to adapt to changing workload and flexibility.

Autonomy and responsibility: To organise his/her work and that of his/her inferiors with autonomy, responsibility and respect for official means in line with his/her position in the organisation.

11. Előtanulmányi követelmények: -

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

12.1. A vállalati kommunikáció fő területei (The main fields of organizational communication);

12.2. Külső és belső PR; (Internal and external public relations);

12.3. Krízis PR (The public relation management of crises);

12.4. A krízis fogalma és értelmezései (The concepts and interpretations of crises);

12.5. Válságmenedzsment és válságkommunikáció (Crisis management and crisis communication);

12.6. A kríziskommunikáció módszertanai (The methodologies of crisis communication);

12.7. A krízisterv (The crisis plan);

12.8. A krízis előre jelezhetősége (The predicabiltites of crises);

12.9. A kríziskommunikáció fő célcsoportjai (The main tartget groups of crisis communication);

12.10. A hatékony kríziskommunikáció alapjai (The basics of effective crisis communication);

12.11. Közösségi kommunikáció, közösségi média és kríziskezelés (Social communications, social media and crisis management);

12.12. Jó gyakorlatok a kríziskommunikáció történetéből (Best practices from the history of crisis communication).

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 tantárgy elfogadásához a tanórák legalább 75 %-án jelen kell lennie a hallgatónak. A távollétet a hiányzást követő első foglalkozáson kell igazolnia. A hallgató köteles az előadás anyagát beszerezni, abból önállóan felkészülni. A 25 százalékot meghaladó hiányzás esetén a tanárral való egyeztetés szükséges annak megbeszélésére, hogy a hiányzás pótolható-e beadandó írásos esszével.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A tanulmányi munka alapja a szemináriumok látogatása, az előírt olvasmányok ismerete, aktiv órai részvéte, egy esettanulmány készítése és teszt megírása megadott szempontok szerint.

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

16.1. Az aláírás megszerzésének feltételei:

A félévi aláírás megszerzésének feltétele a kurzust záró feleletválasztós teszt kitöltése , valamint az órák minimum 75 százalékán való részvétel.

16.2. Az értékelés:

Gyakorlati jegy a tanórai aktivitás, az esettanulmányra kapott értékelés és a teszt eredményéből . A tanórák legalább 75 százalékán kötelező a részvétel, az esettanulmány elkészítése és előadása szintén kötelező, valamint a tesztre kapott legalább elégséges osztályzat (60%-tól elégséges, 70%-tól közepes, 80%-tól jó és 90%-tól jeles).

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. Anthonissen P. F. (2009): Kríziskommunikáció. A válságkezelés és reputációmenedzsment pr-stratégiái, HVG, Budapest.

17.2. 2. Barlai Róbert-Kővágó György: Krízismenedzsment, kríziskommunikáció, Századvég Kiadó, 2004., ISBN 9639211893; **Ajánlott irodalom:**

1. 1. Sellnow, T. L.-Seeger, M. W. (2013): Theorizing crisis communication, Wiley-Blackwell, West-Sussex. UK.
2. 2. Kotter John P (2009): Tettvágy - Változásmenedzsment stratégiai vezetőknek, HVG Könyvek, Budapest.
3. 3. Kulikova, Olga-Heil-Ronald-Berg Jan van den-Peters, Wolter (2012): Cyber Crisis Management: A decision-support framework for disclosing security incident information, 2012 International Conference on Cyber Security, Washington, DC, USA, 14-16 Dec. 2012. (IEEE), DOI: 10.1109/CyberSecurity.2012.20

Budapest, 2021.01.05.

Dr. Kriskó Edina, PhD,
adjunktus sk.

NEMZETI KÖZSZOLGÁLATI EGYETEM
Államtudományi és Nemzetközi Tanulmányok Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** ÁKINTM07
2. **A tantárgy megnevezése (magyarul):** Vezetéselmélet
3. **A tantárgy megnevezése (angolul):** Leadership and management
4. **Kreditérték és képzési karakter:**
   - **4.1.** 2 kredit
   - **4.2.** a tantárgy elméleti vagy gyakorlati jellegének mértéke: 0% gyakorlat, 100% 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. Sasvári Péter László, PhD, egyetemi docens
8. **A tanórák száma és típusa**
   - **8.1.** össz óraszám/félév:
     - 8.1.1. nappali munkarend: 28 (28 EA + 0 GY)
     - 8.1.2. levelező munkarend: 8 (8 EA + 0 GY)
   - **8.2.** heti óraszám - nappali munkarend: 2 (2 EA + 0 GY)
   - **8.3.** Az ismeret átadásában alkalmazandó további sajátos módok, jellemzők: -
9. **A tantárgy szakmai tartalma (magyarul):** A képzésben résztvevő hallgatók megismerkedhetnek a vezetés fogalomrendszerével és szerepével egy szervezet vagy egy munkacsoport működésében. A feldogozott témák érintik az emberek irányításának, csoportmunkának, kommunikációnak és a szervezeti rendszer kiépítésének alapvető kihívásait. Az elméleti modellek mellett olyan esetpéldák bemutatására és feldolgozására kerül sor, amelyek jó példaként szolgálnak a vezetőként eléjük kerülő problémák megoldásához.

   A tantárgy szakmai tartalma (angolul) (Course description): Students get an overview of the leadership theory and the management in organizational and a team. Topics of the lectures cover the main issues of managing people, team coordination, communication and organizational design. Beyond the theoretical models, there are case studies involved that may support as best practices during the work.

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

    Tudása: Megérti a szervezeti feladatokat a kibervédelemben, megismeri a menedzsment feladatát, jogköreit és felelősségét.

    Képességei: Képes olyan védelmi intézkedések meghozatalára, amelyek segítik a humán fenyegetettségből eredő kockázatok csökkentését szervezési eszközök alkalmazásával. Képes megfelelően támogatni szervezetét és a külső feleket egy kibertámadás kezelésében.

    Attitűdje: A maga komplexitásában tervezi meg az információbiztonsági irányítási rendszert, azt össze tudja hangolni a szervezet irányításási rendszerével. Hatékony lépéseket tesz a kibertámadások megelőzése érdekében, így csökkentve a szervezete kitettségét, és az intézkedések hatásait szervezeti összefüggésben értékeli.

    Autonómiája és felelőssége: Önállóan és pontosan vesz részt a kiberbiztonsági fenyegetések technológiai, politikai és adminisztratív megoldásában, a szervezet működését hozzáigazítja a

felmerülő kihívásokhoz. Gyakorlatába beépíti és alkalmazza az e szakterületen folyó kutatások eredményeit a változások és konfliktusok kezelése területén.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: Organisational tasks in cyber security, understanding the function, authority, responsibility of the management.

Capabilities: Taking defensive measures that ensure the reduction of risk resulting from threat against humans by organizational tools. Supporting his/her organisation and external parties in handling a cyber attack.

Attitude: An effort to design the cyber security management system in its own complexity, the ability to synchronize it with the management system. An effort to take effective measures in order to prevent cyber attacks, by this means reducing the exposure of his/her organisation, readiness for evaluating the impacts in organizational context.

Autonomy and responsibility: To take part in providing technological, political and administrative solutions to cyber threats, adjusting the organization to the challanges. To put the results of scientific research in the field into his/her practice according to change and conflict management.

11. Előtanulmányi követelmények: -

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

12.1. A vezetés fogalma, feladatai. A leadership és management fogalmak különbsége (Concept of leadership. The difference between leadership and management);

12.2. Vezetési iskolák: személyiség-elméletek (Leadership theories: Trait theory);

12.3. Vezetési iskolák: stíluselméletek (Leadership theories: Leadership style);

12.4. Vezetési iskolák: kontingencia-elméletek és típuselméletek (Leadership theories: contingency theory and transformational theory);

12.5. Szervezés fogalma, munkaszervezés története (Taylor, Fayol, Weber) (Organizational theory, historical background of organization of work (Taylor, Fayol, Weber));

12.6. Szervezet kialakítása, alapvető szervezeti formák jellemzői (Organizational design, characteristics of primary forms);

12.7. Változás a szervezet működésében, változások és konfliktusok kezelése (Change and conflict management);

12.8. Szervezeti stratégiai kialakítása, stratégiai menedzsment (Elaboration of organizational strategy, strategic management);

12.9. Emberek a szervezetben: motiváció és teljesítményértékelés (People in the organization: motivation and performance evaluation);

12.10. Emberek a szervezetben: kommunikáció (People in the organization: communication);

12.11. Emberek a szervezetben: csoportmunka (People in the organization: teamwork);

12.12. Projektek a szervezet működésében, projektek vezetése (The role of projects, project management);

12.13. Projektmenedzsmentet támogató módszerek (Project management tools);

12.14. Lean menedzsment alkalmazásának lehetősége és feltételei (Conditions of applying lean management).

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 tantárgy elfogadásához a tanórák legalább 80%-án jelen kell lennie a hallgatónak. A távollétet a hiányzást követő első foglalkozáson kell igazolnia. Hiányzás esetén a hallgató köteles az előadás anyagát beszerezni, abból önállóan felkészülni.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A félév során az egyes témakörökből tesztek megírására kerül sor, ezek pontozásra kerülnek. A megszerzett pontok beszámítanak a féléves értékelésbe. A tesztek időpontjáról az előadáson egyeztetettek szerint kerül sor, továbbá arról tájékoztatást kap a hallgató a Moodle rendszeren keresztül.

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

16.1. Az aláírás megszerzésének feltételei:

Aktív órai részvétel, kiadott feladatok határidőre történő elkészítése és a tesztek megírásában való részvétel.

16.2. Az értékelés:

A félév során az egyes témakörökből tesztek megírására kerül sor. Ezek összesített eredménye adja az évközi értékelés eredményét. A félév végén az eredmény javítására vagy pótlására van lehetőség. Az értékelés ötfokozatú, a maximális pontszám 0-60%-a elégtelen, 61-70%-a elégséges, 71-80%-a közepes, 81-90%-a jó, 91-100%-a jeles. Külföldi ösztöndíjas tanulmányok esetén az oktatóval egyeztett témakörben beadvány készítése kötelező.

16.3. A kreditek megszerzésének feltételei:

A kreditek megszerzésének feltétele az aláírás megszerzése és legalább elégséges évközi értékelés (ÉÉ).

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. Mintzberg, H., Golubeff, L. (2010): A menedzsment művészete. Budapest: Alinea. ISBN 9789639659445;
2. Csedő, Z., Zavarkó, M. (2019): Változásvezetés. Budapest: Akadémiai Kiadó. ISBN 9789630599573;
3. Sasvári P. (megjenelés alatt): Rendszerelmélet. Budapest: Ludovika Kiadó.

17.2. Ajánlott irodalom:

1. Edding, C., Schattenhofer, K. (2017): Bevezetés a teammunkába. Budapest: In Dynamics Consulting. ISBN 9789631246544;
2. Dobák, M. (2002): Szervezeti formák és vezetés. Budapest: KJK-Kerszöv. ISBN 0489005135144;
3. Bakacsi, Gy. (2004): Szervezeti magatartás és vezetés. Budapest: Aula. ISBN 9789639585492.

Budapest, 2021.01.05.

Dr. Sasvári Péter László, PhD,
egyetemi docens sk.

NEMZETI KÖZSZOLGÁLATI EGYETEM
Államtudományi és Nemzetközi Tanulmányok Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** ÁKINTM51
2. **A tantárgy megnevezése (magyarul):** Adatbányászat
3. **A tantárgy megnevezése (angolul):** Data Mining
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):** kiberbiztonsági MA , 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, adjunktus
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 célja az előtanulmányokból ismert relációs adatmodellen és az SQL nyelven alapuló hagyományos adatkezelésen túlmutató, nagyon nagy mennyiségű adat kezelési módjának megismerése. Ennek keretében a kurzus során ismertetésre kerülnek az adatok forrásai, a lehetséges adatmodellek és a feldolgozási technológiák. Emellett a big data és a dolgok internete (IoT) alapvető kérdéseivel is megismertetjük a hallgatókat. A tantárgy feltételezi az adatbáziskezelés elméletének ismeretét. A kurzus elvégzésével a hallgató kritikailag lesz képes értelmezni a big data fogalmát és az adatbányászat felhasználását, emellett betekintést nyer a közigazgatási adatkezelés problémáiba az elkövetkező évtizedben.

   A tantárgy szakmai tartalma (angolul) (Course description): The purpose of the course is to learn how to handle a very large amount of data beyond the relational data model known from pre-studies and traditional data management based on SQL. As part of this, the course introduces data sources, possible data models, and processing technologies. In addition, we also introduce students to the basics of big data and the Internet of Things (IoT). The subject assumes knowledge of database management theory. By completing this course, students will be able to critically understand the concept of big data and the use of data mining, as well as gain insight into the problems of administrative data management over the next decade.

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

Tudása: Ismeri a NoSQL adatbázisok fajtáit, működési logikáját, az adattárházak felépítését, az adatbányászat módszereit.

Képességei: Képes átlátni az adatbányászat felhasználási lehetőségeit, a nagy mennyiségű adatok kezelésének problémáit és azok megoldási lehetőségeit.

Attitűdje: Törekszik az adatok hatékony felhasználására.

Autonómiája és felelőssége: Az adatforrások ismeretében megszervezi az elemzési folyamatokat.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: Is familiar with the types of NoSQL databases, logic of operation, structure of data warehouses, methods of data mining.

Capabilities: Able to understand the uses of data mining, the problems of managing large amount of data and how to solve them.

Attitude: Striving for efficient use of data.

Autonomy and responsibility: Organizes the analysis process knowing the data sources.

11. Előtanulmányi követelmények: -

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

12.1. Adatbáziskezelés alapok: relációs adatmodell (Database management: Relational data model);

12.2. Adatbáziskezelés alapok: Normálformára rendezés (Database management: Normal forms);

12.3. Adatbáziskezelés alapok: SQL (Database management: SQL);

12.4. Adatbáziskezelés gyakorlat DML (Database management excercise DML);

12.5. Adatbáziskezelés gyakorlat DDL,DCL,TCL (Database management excercise DDL,DCL,TCL);

12.6. NoSQL (NoSQL);

12.7. Adattárházak (Data warehouses);

12.8. Adatbányászati elvek (Theories of data mining);

12.9. Adatbányászati példák (Examples of data mining).

12.10. Big Data elvei (Big Data theories);

12.11. Esettanulmány (Case Study);

12.12. Esettanulmány (Case Study);

12.13. Összefoglalás (Summary);

12.14. Zárthelyi dolgozat (Exam).

13. A tantárgy meghirdetésének gyakorisága/a tantervben történő félévi elhelyezkedése: őszi/tavaszi 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 esettanulmányt kell kidolgozni, mely ötfokozatú skálán kerül értékelésre. Nappali munkarendben a félév utolsó előtti, levelező munkarendben az utolsó előadásán kerül sor a kidolgozott esettanulmány előadására („pitchelésére"), melynek értékelése ötfokozatú skálán történik. A nem megfelelt értékelésű feladatot vagy előadást (csak az egyiket) az elméleti ismereteket összefoglaló ZH-val, egy alkalommal lehet javítani, nappali munkarendben az utolsó előadáson, levelező munkarendben egyeztetett időpontban.

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 az előadás eredményes teljesítése.

16.2. Az értékelés:

Gyakorlati jegy, ötfokozatú értékelés. A gyakorlati jegyet a félévi feladat és az előadás 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. Szádeczky Tamás: Big Data a közigazgatásban. In: Szádeczky Tamás (szerk.) et al.: Digitális Állam modul tankönyve. NKE (megjelenés alatt)
2. Tan, Pang-Ning, Steinbach, Michael, Kumar, Vipin: Bevezetés az adatbányászatba. Budapest: Panem, 2011. ISBN 978-963-545-535-5

17.2. Ajánlott irodalom:

1. Reynolds, Vince: Big Data For Beginners: Understanding SMART Big Data, Data Mining & Data Analytics For improved Business Performance, Life Decisions & More! CreateSpace Independent Publishing Platform, 2016. ISBN 9781530412044

Budapest, 2021.01.05.

Dr. Bányász Péter, PhD,
adjunktus sk.

NEMZETI KÖZSZOLGÁLATI EGYETEM
Államtudományi és Nemzetközi Tanulmányok Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** ÁKINTM52
2. **A tantárgy megnevezése (magyarul):** Adatvédelem a gyakorlatban
3. **A tantárgy megnevezése (angolul):** Data protection in the practice
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):** kiberbiztonsági MA , 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. Péterfalvi Attila, PhD, egyetemi docens
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 hallgatók a már megszerzett ismeretekre alapozva megismerkednek a hazai és nemzetközi joggyakorlattal. A tantárgyhoz kapcsolódó jogesetek feldolgozása.

   A tantárgy szakmai tartalma (angolul) (Course description): Students will become familiar - based on the already acquired knowledge - with the Hungarian and international case-law. Processing of legal cases related to the subject.

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

Tudása: Az adatvédelem, és a köz és magánszféra adatkezelése területén felmerülő jogi problémák felismerése, azonosítása, a jogi helyzet rögzítése, a problémás helyzet áttekintése, elemzése, rendszerezése, illetve megoldása, megoldási alternatívák felvázolása és az érintettek képviselete.

Képességei: Az adatvédelem, és a köz- és magánszféra adatkezelése területén felmerülő jogi problémákat felismeri és képes kialakítani megoldási javaslatokat, illetve alkalmas a megfelelő jogi megoldás kiválasztására.

Attitűdje: Törekszik az adatvédelmi tudatosítás minél szélesebb körű megvalósítására.

Autonómiája és felelőssége: A megfelelő irányítás mellett képes a feladatok önálló végzésére, önellenőrzésre képes, javaslatokat tesz, mások munkáját értékeli.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: The recognition and identification legal problems arising from data protection, and public and private data processing, determining the legal situation, reviewing, analysing, systematizing, and solving the problematic situation, outlining alternative solutions, and representing data subjects.

Capabilities: Recognizing legal issues in the areas of data protection, and data management in the public and private sphere, and coming up with solutions and choosing the appropriate legal solution.

Attitude: Striving to achieve a high level of privacy awareness.

Autonomy and responsibility: Under proper direction, carrying out tasks independently and self-monitoring. He/she can make recommendations and evaluate the work of others.

11. Előtanulmányi követelmények: Adatvédelem [ÁKINTM08]

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

12.1. A Nemzeti Adatvédelmi és Információszabadság Hatóság bemutatása (Introduction of the Hungarian National Authority for Data Protection and Freedom of Information (NAIH));

12.2. A Nemzeti Adatvédelmi és Információszabadság Hatóság eljárásai 1. – hazai szabályok (The proceedures of the Hungarian National Authority for Data Protection and Freedom of Information 1. – national rules);

12.3. A Nemzeti Adatvédelmi és Információszabadság Hatóság eljárásai 2. – eljárások az Európai Unión belül (The proceedures of the Hungarian National Authority for Data Protection and Freedom of Information 2. - procedures in the European Union);

12.4. Nyilvántartások és nyilvántartási feladatok a GDPR alapján (Records and registration tasks under the GDPR);

12.5. Az adatvédelmi incidens kezelésének gyakorlati kérdései (Practical aspects of managing personal data breaches);

12.6. Gyakorlati jogesetek ismertetése az adatvédelmi incidensek bejelentésével és kezelésével kapcsolatosan 1. (Presenting practical legal cases for notifying and managing personal data breaches 1.);

12.7. Gyakorlati jogesetek ismertetése az adatvédelmi incidensek bejelentésével és kezelésével kapcsolatosan 2. (Presenting practical legal cases for notifying and managing personal data breaches 2.);

12.8. Az adatvédelmi hatásvizsgálatok elkészítésére használható gyakorlati iránymutatások és eszközök használata (Use of practical guidelines and tools for preparing data protection impact assessments);

12.9. Adatvédelmi hatásvizsgálat készítése a gyakorlatban 1. (Making a data protection impact assessment / in practice 1.);

12.10. Adatvédelmi hatásvizsgálat készítése a gyakorlatban 2. (Making a data protection impact assessment / in practice 2.);

12.11. Akkreditáció és tanúsítás a gyakorlatban (Accreditation and certification in practice);

12.12. Adatvédelem – bírósági tárgyaláson részvétel (Data Protection - attend a court trial);

12.13. Adatvédelem – bírósági tárgyaláson részvétel (Data Protection - attend a court trial);

12.14. Összefoglalás (Summary).

13. A tantárgy meghirdetésének gyakorisága/a tantervben történő félévi elhelyezkedése: őszi/tavaszi 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 egy 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 szemeszterben egy 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. Magyarázat a GDPR-ról, Wolters Kluwer Hungary Kft., Budapest, 2018. ISBN 978 963 295 761 6;
2. Árvay Viktor György et.al.: Az elszámoltathatóság alapelve és az adatkezelői kötelezettségek, NKE, Budapest, 2018;
3. Sziklay Júlia – Bendik Tamás: Az adatvédelem hazai és európai uniós szabályozása és alapintézményei, NKE, Budapest, 2019;
4. Balogh Gyöngyi et.al.: Az adatvédelmi jog alapelvei, fogalmai, szereplői, profilalkotás, a személyes adatok különleges kategóriái, bűnügyi személyes adatok, NKE, Budapest, 2019
5. Magyar Közlöny Lap- és Könyvkiadó Kft. kiadásában: A Nemzeti Adatvédelmi és Információszabadság Hatóság általános adatvédelmi rendelettel kapcsolatos állásfoglalásai, Budapest, 2018. ISBN 978-615-5710-64-3.

17.2. Ajánlott irodalom:

1. Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) hatályos szövege;
2. Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény;
3. Az Európai Adatvédelmi Testület (EDPB) véleményei, iránymutatásai;
4. A Nemzeti Adatvédelmi és Információszabadság Hatóság beszámolói; kapcsolódó bírósági határozatok; a korábbi adatvédelmi biztos beszámolói;
5. A 29. cikk alapján létrehozott adatvédelmi munkacsoport véleményei és iránymutatásai;

Budapest, 2021.01.05.

Dr. Péterfalvi Attila, PhD,
egyetemi docens sk.

NEMZETI KÖZSZOLGÁLATI EGYETEM
Államtudományi és Nemzetközi Tanulmányok Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** ÁKINTM53
2. **A tantárgy megnevezése (magyarul):** Kiberbiztonsági akkreditáció és tanúsítás
3. **A tantárgy megnevezése (angolul):** Cybersecurity accreditation and certification
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):** kiberbiztonsági MA , 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. Krasznay Csaba, PhD, egyetemi docens
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 kurzus célja a megfelelőségértékelés alapjainak, a jogszabályi és szabvány környezetnek, valamint az akkreditálás hazai és európai gyakorlatának bemutatása. A hallgató megismeri a megfelelőségértékelés szabályozott területén a jogszabályi és szabványkörnyezet, a notifikációs eljárások, a szektorális programok, az IKT területspecifikus akkreditálás gyakorlati ismeretanyagát. Az előadás részletesen foglalkozik az információbiztonság területén használt folyamat- és terméktanúsítások kérdéskörével, különös tekintettel az Európai Unió és tagországai elvárásaira.

   A tantárgy szakmai tartalma (angolul) (Course description): The aim of the course is to introduce the basics of conformity assessment, the legal and standard environment, and the national and European practice of accreditation. Students will become familiar with the practical knowledge of the regulatory and standard environment, notification procedures, sectoral programs, and specific ICT accreditation in the field of regulated conformity assessment. The lecture deals in detail with the process and product certification used in the field of information security, with particular attention to the requirements of the European Union and its member states.

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

Tudása: Ismeri azokat a fontosabb előírásokat a szabályozásokból, amelyek a mindennapi munkáját befolyásolják. Tisztában van az állami kibervédelmi rendszerrel.

Képességei: Képes értelmezni a jogszabályokból eredő követelményeket. Képes átlátni a kibertér aktuális fenyegetéseit.

Attitűdje: Munkája során figyelembe veszi és alkalmazza a kiberbiztonsággal kapcsolatos jogszabályokat.

Autonómiája és felelőssége: Tudatosan törekszik a kiberbiztonság sajátosságainak megfelelő,

korszerű ismeretek hazai és nemzetközi szinten történő gyakorlati alkalmazására. Kezdeményező módon lép fel az alternatív, eredeti megoldások kidolgozásában, bemutatásában és a bonyolult, nem tipikus helyzetekben történő adekvát döntések meghozatalában. Vállalja a szakterület, a szakmai praxis módszertanának fejlesztéséhez szükséges elméleti, tudományos kutatási és gyakorlati információk beszerzésének, értékelésének és hasznosításának végrehajtását.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: Is familiar with specifications of regulations that have an immediate impact on his/her daily work. Is familiar with the cyber security system of the state.

Capabilities: Is capable of interpreting legal requirements. Is capable of understanding the current threats of cyber space.

Attitude: His/her personal attitude is characterized by an attention to and application of laws of cyber security in his/her work.

Autonomy and responsibility: Autonomy and responsibility are to implement advanced knowledge characterising cyber security on a national and international level. Autonomy and responsibility are to initiate and introduce alternative and original solutions and appropriate decision making in complex, atypical contexts. Autonomy and responsibility are to obtain, evaluate and utilize theoretical, scientific and practical information necessary for the improvement of the field and the methodology of professional practice.

11. Előtanulmányi követelmények: -

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

12.1. A megfelelőségértékelés használata a szabályozási gyakorlatban (Use of conformity assessment in regulatory practice);

12.2. Az Új Jogalkotási Keret európai gyakorlata (The European practice of the New Legislative Framework);

12.3. Megfelelőségértékelési modulok (Modules for conformity assessment);

12.4. Bejelentési eljárások (Notification procedures);

12.5. Az akkreditálás, mint a kormányzati célkitűzések támogatásának eszköze (Accreditation as a means of supporting government objectives);

12.6. Szakpolitikák támogatása, egységes digitális piac (Supporting policies, digital single market);

12.7. Ágazati akkreditálási rendszerek (Sectoral accreditation systems);

12.8. Felügyeleti tevékenységek (Surveillance activities);

12.9. IKT termékek és szolgáltatások közbeszerzési megfelelőségértékelési követelményei (Public procurement conformity assessment requirements for ICT products and services);

12.10. Európai és hazai IKT megfelelőségértékelési szabványok, jogszabályok (European and national ICT conformity assessment standards, legislation);

12.11. IKT termékek és rendszerek hazai akkreditálása (Domestic accreditation of ICT products and systems);

12.12. Az információbiztonsági tanúsítás az IKT környezetben (Information security certification in the ICT environment);

12.13. Az IKT laboratóriumok működésének áttekintése (Overview of the operation of ICT laboratories);

12.14. Az IKT-termékek és -szolgáltatások kiberbiztonsági tanúsítása (Cybersecurity certification framework for ICT products and services).

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

-

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.

16.2. Az értékelés:

Írásbeli kollokvium, ötfokozatú értékelés. A kollokvium a félév folyamán átadott elméleti ismeretek számonkérését tartalmazza.

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. EA, ILAC, IAF terület specifikus dokumentumok
2. Jogszabályok: 768/2008/EK határozat, 2009. évi CXXXIII. törvény, 315/2009. (XII. 28.) Korm. rendelet, IKT specifikus EU jogszabályok, állásfoglalások
3. IKT specifikus szabványok (ISO, ETSI)

17.2. Ajánlott irodalom:

1. NAH szabályzatok

Budapest, 2021.01.05.

Dr. Krasznay Csaba, PhD,
egyetemi docens sk.

NEMZETI KÖZSZOLGÁLATI EGYETEM
Államtudományi és Nemzetközi Tanulmányok Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** ÁKINTM54
2. **A tantárgy megnevezése (magyarul):** Kiberbiztonsági innováció
3. **A tantárgy megnevezése (angolul):** Cybersecurity innovation
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):** kiberbiztonsági MA , 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. Krasznay Csaba, PhD, egyetemi docens
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 kurzus célja bemutatni a kutatás-fejlesztés-innováció lehetőségeit a kiberbiztonsági szakterületen. A hallgatók megismerhetik a hazai és európai szakpolitikai irányokat, betekintést kapnak az innováció folyamatába nagyvállalati, akadémiai és startup környezetben. Ismereteket szereznek a speciális szakterületek (pl. rendészet, honvédelem) innovációs igényeivel kapcsolatban is. A kurzus esettanulmányokon keresztül mutatja be, milyen módszerekkel lehet sikerre vinni egy kiberbiztonsági termék vagy szolgáltatás ötletét, mind üzleti, mind pedig technológiai aspektusból.

   A tantárgy szakmai tartalma (angolul) (Course description): The aim of the course is to demonstrate the possibilities of research, development and innovation in the field of cybersecurity. Students will learn about national and European policies and get an insight into the process of innovation in a large enterprise, academic and startup environment. They also gain knowledge of the innovation needs of special areas (e.g. law enforcement, military). The course introduces case studies on how to succeed an idea of a cybersecurity product or service, both from a business and a technology perspective.

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

Tudása: Átlátja, hogy milyen védelmi megoldások vannak a kibertámadás ellen. Tisztában van az állami kibervédelmi rendszerrel. Megérti a szervezeti feladatokat a kibervédelemben.

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

Attitűdje: Hatékony lépéseket tesz a kibertámadások megelőzése érdekében, így csökkentve a szervezete kitettségét.

Autonómiája és felelőssége: Tudatosan törekszik a kiberbiztonság sajátosságainak megfelelő,

korszerű ismeretek hazai és nemzetközi szinten történő gyakorlati alkalmazására. Kezdeményező módon lép fel az alternatív, eredeti megoldások kidolgozásában, bemutatásában és a bonyolult, nem tipikus helyzetekben történő adekvát döntések meghozatalában. Vállalja a szakterület, a szakmai praxis módszertanának fejlesztéséhez szükséges elméleti, tudományos kutatási és gyakorlati információk beszerzésének, értékelésének és hasznosításának végrehajtását.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: Is familiar with defence solutions against cyber attacks. Is familiar with the cyber security system of the state. Is familiar with the organisational tasks in cyber security.

Capabilities: Is capable of taking technological defensive measures related to elements of the cyber kill chain. Is capable of understanding the current threats of cyber space.

Attitude: 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.

Autonomy and responsibility: Autonomy and responsibility are to implement advanced knowledge characterising cyber security on a national and international level. Autonomy and responsibility are to initiate and introduce alternative and original solutions and appropriate decision making in complex, atypical contexts. Autonomy and responsibility are to obtain, evaluate and utilize theoretical, scientific and practical information necessary for the improvement of the field and the methodology of professional practice.

11. Előtanulmányi követelmények: -

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

12.1. Az innováció fogalma (Concept of innovation);

12.2. Kiberbiztonsági K+F+I stratégiák Magyarországon és Európában (Cybersecurity R&D&I strategies in Hungary and Europe);

12.3. Ügyfelek, piaci igények (Customers and market needs);

12.4. Különleges innovációs igények (Special innovation requirements);

12.5. Kiberbiztonsági innováció akadémiai környezetben (Cybersecurity innovation in academic environment);

12.6. Nagyvállalati innováció (Enterprise innovation);

12.7. A startup ökoszisztéma (Startup ecosystem);

12.8. Ötlettől a megvalósításig (From the idea to the delivery);

12.9. A cégépítés rejtelmei (Mysteries of company building);

12.10. A megfelelő csapat (The right team);

12.11. Business Model Canvas (Business model canvas);

12.12. PR, marketing, sales (PR, marketing, sales);

12.13. Tárgyalás a befektetővel és az ügyféllel (Negotiation with the investor and the customer);

12.14. Esettanulmány (Case study).

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 feladatot szükséges teljesíteni, mely a

témához kapcsolódó házidolgozat elkészítését jelenti.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A félév folyamán egy, a félév elején kiadott esettanulmányt kell kidolgozni, mely ötfokozatú skálán kerül értékelésre. Nappali munkarendben a félév utolsó előtti, levelező munkarendben az utolsó előadásán kerül sor a kidolgozott esettanulmány előadására („pitchelésére"), melynek értékelése ötfokozatú skálán történik. A nem megfelelt értékelésű feladatot vagy előadást (csak az egyiket) az elméleti ismereteket összefoglaló ZH-val, egy alkalommal lehet javítani, nappali munkarendben az utolsó előadáson, levelező munkarendben egyeztetett időpontban.

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 az előadás eredményes teljesítése.

16.2. Az értékelés:

Gyakorlati jegy, ötfokozatú értékelés. A gyakorlati jegyet a félévi feladat és az előadás 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. Szabó, K. (2012): Az invenciótól az innovációig. In: Hámori, B. és Szabó, K. (2012): Innovációs verseny: esélyek és korlátok. Aula, Budapest, pp.21-44.
2. Makó, C., Illéssy, M. (2017). Innováció menedzsment in Vezetés a közjó szolgálatában. Közpénzügyi gazdálkodás és menedzsment. Szerk. Bábosik Mária, Állami Számvevőszék – Typotex Kiadó, Budapest
3. Inzelt, A., & Bajmócy, Z. (2013). Innovációs rendszerek: Szereplők, kapcsolatok és intézmények.

17.2. Ajánlott irodalom:

1. Porkoláb, I. (2016). Az innováció hatása a hadviselésre. HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA, 26(1-2), 19-28.
2. Carlota Perez, Technological revolutions, paradigm shifts and socio-institutional change, in E.Reinert, ed. Globalization, Economic Development and Inequality, An Alternative Perspective, Elgar, 2004. pp. 217-242.
3. Dosi, G. (1983). Technological paradigms and technological trajectories. Research Policy, 11(3).
4. Makó, C., Illéssy, M., & Heidrich, B. (2019). When will alpha and omega collide? In search of the theoretical relevance of EU innovation policies. Vezetéstudomány-Budapest Management Review, 50(11), 66-73.
5. Mazzucato, M. (2016). From market fixing to market-creating: a new framework for innovation policy. Industry and Innovation, 23(2), 140-156.

Budapest, 2021.01.05.

Dr. Krasznay Csaba, PhD,
egyetemi docens sk.

NEMZETI KÖZSZOLGÁLATI EGYETEM
Államtudományi és Nemzetközi Tanulmányok Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** ÁKINTM55
2. **A tantárgy megnevezése (magyarul):** Pénzintézeti információs rendszerek védelme
3. **A tantárgy megnevezése (angolul):** Protection of financial institution information systems
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):** kiberbiztonsági MA , 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. Krasznay Csaba, PhD, egyetemi docens
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 kurzus célja a magyar és európai pénzügyi rendszer, mint kritikus infrastruktúra, valamint az ezeket működtető elektronikus információs rendszerek ismertetése. A tárgy részletesen foglalkozik pénzintézetek információbiztonsági követelményrendszerével a hazai, európai és globális szabályrendszerének tükrében. Bemutatja a fontosabb globális hazai és nemzetközi pénzügyi információs rendszereket, végigvezeti a hallgatókat a fontosabb pénzügyi folyamatokat támogató háttérrendszereken. Ismerteti az új típusú, bankrendszeren kívüli pénzügyi megoldásokat, mint a kriptovaluták és a fintech megoldások, valamint ezek kiberbiztonsági kockázatait.

   A tantárgy szakmai tartalma (angolul) (Course description): The aim of the course is to introduce the Hungarian and European financial systems as critical infrastructure and the electronic information systems that operate them. The subject deals in detail with the information security requirements of financial institutions in the light of their national, European and global rules. It introduces the major global domestic and international financial information systems, and guides students through the background systems supporting major financial processes. It introduces new types of non-banking financial solutions, such as cryptocurrencies and fintech solutions, and their cyber security risks.

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

Tudása: Ismeri a pénzügyi folyamtok biztonsági jellemzőit.

Képességei: Képes átlátni a gazdasági-pénzügyi rendszereket.

Attitűdje: A pénzügyi folyamatokban is meglátja a biztonsági kihívásokat.

Autonómiája és felelőssége: Pénzügyi szakember mellett képes ellátni a biztonsági felelős szerepét.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: Knowledge of financial security features.

Capabilities: Ability to understand economic-financial systems.

Attitude: Also sees security challenges in financial processes.

Autonomy and responsibility: Able to act as a security officer alongside a financial professional.

11. Előtanulmányi követelmények: -

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

12.1. Hazai jogi előírások (Hpt, Bszt) (Domestic legal regulations);

12.2. Uniós jogi előírások (PSD2) (EU Legal Requirements);

12.3. MNB elvárások (Requirements of the central bank);

12.4. Kártyatársasági elvárások (PCI DSS) (Payment card industry requirements);

12.5. Pénzintézetek informatikai rendszerei (IT systems of financial institutions);

12.6. Bankkártyás fizetés informatikája (IT background of credit card payment);

12.7. Pénzügyi információs rendszerek (Financial information systems);

12.8. Speciális biztonsági követelmények (Special security requirements);

12.9. Csalásfelderítés (Fraud detection);

12.10. Incidenskezelés specifikumai (Specialties in incident management);

12.11. Esettanulmány (Case Study);

12.12. Esettanulmány (Case Study);

12.13. Összefoglalás (Summary);

12.14. Zárthelyi dolgozat (Exam).

13. A tantárgy meghirdetésének gyakorisága/a tantervben történő félévi elhelyezkedése: őszi/tavaszi 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 esettanulmányt kell kidolgozni, mely ötfokozatú skálán kerül értékelésre. Nappali munkarendben a félév utolsó előtti, levelező munkarendben az utolsó előadásán kerül sor a kidolgozott esettanulmány előadására („pitchelésére"), melynek értékelése ötfokozatú skálán történik. A nem megfelelt értékelésű feladatot vagy előadást (csak az egyiket) az elméleti ismereteket összefoglaló ZH-val, egy alkalommal lehet javítani, nappali munkarendben az utolsó előadáson, levelező munkarendben egyeztetett időpontban.

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 az előadás eredményes teljesítése.

16.2. Az értékelés:

Gyakorlati jegy, ötfokozatú értékelés. A gyakorlati jegyet a félévi feladat és az előadás 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. Muha Lajos - Tóth Georgina Nóra: A bankbiztonság vizsgálata kockázatelemzéssel, Hadmérnök, VI. Évfolyam 4. szám - 2011. december
2. Kovács Levente - Marsi Erika (szerk.): Bankmenedzsment – Banküzemtan, Alapítvány a Pénzügyi Kultúra Fejlesztéséért, 2019
3. Hetyei József (szerk.): Pénzintézetek és állami intézmények információs rendszerei Magyarországon. Computerbooks, 2002.

17.2. Ajánlott irodalom:

1. Duran, Randall E. (2017): Financial Services Technology: Processes, Architecture, and Solutions, 2nd Edition. Cengage Asia, ISBN 978-9814780865
2. Williams, Branden R., Chuvakin, Anton: PCI Compliance: Understand and Implement Effective PCI Data Security Standard Compliance. Syngress, ISBN 978-0128015797

Budapest, 2021.01.05.

Dr. Krasznay Csaba, PhD,
egyetemi docens sk.

NEMZETI KÖZSZOLGÁLATI EGYETEM
Államtudományi és Nemzetközi Tanulmányok Kar

TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** ÁKINTM56
2. **A tantárgy megnevezése (magyarul):** Villamosenergia-rendszerek kibervédelme
3. **A tantárgy megnevezése (angolul):** Cybersecurity of electricity systems
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):** kiberbiztonsági MA , 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. Krasznay Csaba, PhD, egyetemi docens
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):** Az előadás a villamosenergia szektor, mint kritikus infrastruktúra terület felépítésével és műszaki alapismereteivel foglalkozik. A hallgatók megismerik a villamosenergia ellátás alapjait, infrastruktúráját, a magyar villamosenergia-rendszer működését. A kurzus foglalkozik a villamosenergia-rendszer irányítástechnikai, védelmi, automatikai és kommunikációs rendszereivel. Bevezeti az IoT és az IIoT fogalmakat, valamint ismerteti a Smart Energy és a háztartási villamosenergia rendszereket és a kapcsolódó informatikai megoldásokat. A kibervédelem területén az ismert, villamosenergetika területét érintő kihívásokat is megtárgyalja, valamint foglalkozik a védelmi lehetőségekkel az OT/IT területen, illetve azokkal a megfelelőségi követelményekkel, melyek a szektorra vonatkoznak.

   A tantárgy szakmai tartalma (angolul) (Course description): The course deals with the structure and basic technical knowledge of the electricity sector as a critical infrastructure. Students get acquainted with the basics of electricity supply, the infrastructure and the operation of the Hungarian electricity system. The course deals with power system control, protection, automation and communication systems. It introduces IoT, IIoT, Smart Energy, Home Power Systems and related IT solutions. It also discusses known challenges of electrical power from the cybersecurity perspective, as well as protection options in the OT / IT field and compliance requirements for the sector.

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

Tudása: Átlátja, hogy milyen védelmi megoldások vannak a kibertámadás ellen. Ismeri a létfontosságú rendszerelemek fogalmát. Ismeri a kártékony kódok fogalmát és hatásmechanizmusát.

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

Attitűdje: Hatékony lépéseket tesz a kibertámadások megelőzése érdekében, így csökkentve a szervezete kitettségét.

Autonómiája és felelőssége: Tudatosan törekszik a kiberbiztonság sajátosságainak megfelelő, korszerű ismeretek hazai és nemzetközi szinten történő gyakorlati alkalmazására. Kezdeményező módon lép fel az alternatív, eredeti megoldások kidolgozásában, bemutatásában és a bonyolult, nem tipikus helyzetekben történő adekvát döntések meghozatalában. Vállalja a szakterület, a szakmai praxis módszertanának fejlesztéséhez szükséges elméleti, tudományos kutatási és gyakorlati információk beszerzésének, értékelésének és hasznosításának végrehajtását.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge: Is familiar with defence solutions against cyber attacks. Is familiar with the concept of vital system components. Is familiar with the concept and mode of action of malware codes.

Capabilities: Is capable of taking technological defensive measures related to elements of the cyber kill chain. Is capable of understanding the current threats of cyber space.

Attitude: 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.

Autonomy and responsibility: Autonomy and responsibility are to implement advanced knowledge characterising cyber security on a national and international level. Autonomy and responsibility are to initiate and introduce alternative and original solutions and appropriate decision making in complex, atypical contexts. Autonomy and responsibility are to obtain, evaluate and utilize theoretical, scientific and practical information necessary for the improvement of the field and the methodology of professional practice.

11. Előtanulmányi követelmények: -

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

12.1. A villamosenergia ellátás alapjai (Basics of electricity supply);

12.2. A villamosenergia ellátás infrastruktúrája (Electricity supply infrastructure);

12.3. A magyar villamosenergia-rendszer áttekintése (Overview of the Hungarian electricity system);

12.4. A villamosenergia-rendszer irányítástechnikai rendszerei (Control systems of the electricity system);

12.5. A villamosenergia-rendszer védelmi rendszerei (Protection of electricity systems);

12.6. A villamosenergia-rendszer automatika rendszerei (Automation systems of electricity system);

12.7. A villamosenergia-rendszer kommunikációs rendszere (Communication systems of electricity system);

12.8. IoT/IIoT a villamosenergetikában (IoT/IIoT in electricity systems);

12.9. Smart Energy – okos megoldások a villamosenergetikában (Smart Energy - smart solutions in electricity);

12.10. Háztartási villamosenergia rendszerek és informatikai rendszereik (Household electricity systems and IT systems);

12.11. Ismert sebezhetőségek a villamosenergetikai környezet informatikai rendszereiben (Known vulnerabilities in IT systems of the electrical energy environment);

12.12. IT és OT védelem kibertámadások ellen (IT and OT defense against cyberattacks);

12.13. Kiberbiztonsági műszaki megfelelőségi követelmények villamosenergia környezetben (Cybersecurity technical compliance requirements in an electricity environment);

12.14. Konkrét kibertámadások és azok tanulságai (Specific cyberattacks and their lessons learnt);

12.15. Villamosenergia-irányító rendszerek kibertámadásának hálózati és informatikai következményei, teendői (Network and IT consequences of cyberattacks in Power Management Systems).

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 feladatot szükséges teljesíteni, mely a témához kapcsolódó házidolgozat elkészítését jelenti.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje:

-

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.

16.2. Az értékelés:

Írásbeli kollokvium, ötfokozatú értékelés. A kollokvium a félév folyamán átadott elméleti ismeretek számonkérését tartalmazza.

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. Deák Veronika (szerk) (2019): Kritikus információs infrastruktúrák védelme - Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára – 2019. Nemzeti Közszolgálati Egyetem, ISBN 978-963-498-240-1
2. Deák Veronika (szerk) (2019): Kritikus információs infrastruktúrák védelme - Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára 2019. Nemzeti Közszolgálati Egyetem, ISBN 978-963-498-239-5

17.2. Ajánlott irodalom:

1. Knapp, Eric D., Samani, Raj (2013): Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure. Syngress, ISBN 978-1597499989
2. Ackerman, Pascal (2017): Industrial Cybersecurity: Efficiently secure critical infrastructure systems. Packt, ISBN 978-1788395151
3. Knapp, Eric D., Langill, Joel Thomas (2014): Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. Syngress, ISBN 978-0124201149

Budapest, 2021.01.05.

Dr. Krasznay Csaba, PhD,
egyetemi docens sk.