Nemzeti Közszolgálati Egyetem
Közigazgatási Továbbképzési Intézet

Elektronikus információbiztonsági vezető szakirányú továbbképzési szak

Képzési program

Szakfelelős: Dr. Bányász Péter

I.
ELEKTRONIKUS INFORMÁCIÓBIZTONSÁGI VEZETŐ SZAKIRÁNYÚ TOVÁBBKÉPZÉSI SZAK
KÉPZÉSI ÉS KIMENETI KÖVETELMÉNYEK

1. A szakirányú továbbképzés megnevezése: elektronikus információbiztonsági vezető szakirányú továbbképzési szak

A szakirányú továbbképzés megnevezése angolul: Electronic Information Security Manager postgraduate specialist training course

2. A szakirányú továbbképzésben szerezhető szakképzettség oklevélben szereplő megnevezése: elektronikus információbiztonsági vezető

A szakirányú továbbképzésben szerezhető szakképzettség oklevélben szereplő megnevezése angolul: Electronic Information Security Manager

3. A szakirányú továbbképzés besorolása:

3.1. képzési terület szerinti besorolása: államtudományi képzési terület

3.2. a végzettségi szint besorolása:
- ISCED 1997 szerint: 5A
- ISCED 2011 szerint: 6
- az európai keretrendszer szerint: 6
- a magyar képesítési keretrendszer szerint: 6

3.2. a szakképzettség képzési területek egységes osztályozási rendszere szerinti tanulmányi területi besorolása:
- ISCED 1997 szerint: 48
- ISCED-F 2013 szerint: 0610

4. A felvétel feltétele(i):
A képzésben legalább alapképzésben (korábban főiskolai szintű képzésben) szerzett oklevéllel rendelkezők vehetnek részt azok, akik angol nyelvű alapfokú komplex nyelvvizsgával, vagy ezzel egyenértékű bizonyítvánnyal, oklevéllel rendelkeznek.

5. A képzési idő félévekben meghatározva: 2 félév

6. A szakképzettség megszerzéséhez összegyűjtendő kreditek száma: 60 kredit

7. A képzés célja és a szakmai kompetenciák (tudás, képesség, attitűd, autonómia és felelősség):

7.1. A képzés célja:
A képzés fő célja az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott elektronikus információs rendszer biztonságáért felelős személyek feladatellátásához szükséges szakmai kompetenciák átadása és a biztonságtudatos szemléletmód kialakítása.

7.2. Szakmai kompetenciák:

A szakképzettség megnevezése: elektronikus információbiztonsági vezető

a) tudása
- Ismeri azokat a fontosabb előírásokat a szabályozásokból, amelyek a mindennapi munkáját befolyásolják.
- Átlátja, hogy milyen védelmi megoldások vannak a kibertámadás ellen.
- Ismeri a kibertámadás esetén alkalmazandó eljárásokat.
- Ismeri a létfontosságú rendszerelemek fogalmát.

- Átlátja a munkáltatók által meghatározott belső szabályzatok megalkotásának szükségességét az információs rendszerekben tárolt adatok sértetlensége és a rendelkezésre állás tekintetében.
- Tisztában van az emberi tényező szerepével a kibertámadások kivitelezése során.
- Ismeri a kártékony kódok fogalmát és hatásmechanizmusát.
- Tisztában van az állami kibervédelmi rendszerrel.
- Megérti a szervezeti feladatokat a kibervédelemben.

b) képességei

- Képes értelmezni a jogszabályokból eredő követelményeket.
- Képes megszerezni a szervezet vezetőinek támogatását a jogszabályi megfelelőség kiépítéséhez.
- Képes olyan védelmi intézkedések meghozatalára, amelyek segítik a humán fenyegetettségből eredő kockázatok csökkentését.
- Képes olyan technológiai védelmi intézkedések meghozatalára, amelyek a cyber kill chain egyes elemeihez kapcsolódnak.
- Képes felmérni a belső munkavállalók jelentette kiberbiztonsági kockázatokat.
- Képes olyan szabályzatok alkotására, amelyek a belső munkavállalók jelentette fenyegetések kezelésére vonatkoznak.
- Képes átlátni a kibertér aktuális fenyegetéseit.
- Képes támogatni szervezetét a kibervédelmi képességek kialakításában.
- Képes megfelelően támogatni szervezetét és a külső feleket egy kibertámadás kezelésében.

c) attitűdje

- Munkája során figyelembe veszi és alkalmazza a kiberbiztonsággal kapcsolatos jogszabályokat.
- A maga komplexitásában tervezi meg az információbiztonsági irányítási rendszert.
- Hatékony lépéseket tesz a kibertámadások megelőzése érdekében, így csökkentve a szervezete kitettségét.
- Kiemelt kockázatként kezeli a belső munkavállalókat, és ennek megfelelően tervezi meg az információbiztonsági folyamatokat.
- Partner abban, hogy se a szervezete, se ő maga ne váljon kibertámadás áldozatává.

d) autonómiája és felelőssége

- Tudatosan törekszik a kiberbiztonság sajátosságainak megfelelő, korszerű ismeretek hazai és nemzetközi szinten történő gyakorlati alkalmazására.
- 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.
- Vállalja a szakterület, a szakmai praxis módszertanának fejlesztéséhez szükséges elméleti, tudományos kutatási és gyakorlati információk beszerzésének, értékelésének és hasznosításának végrehajtását.
- Felelősséget vállal a kiberbiztonság összefüggő ismeretének és a meghatározó jogi, szabályozási és gazdasági összefüggések ismeretének alapján a szakmai javaslatok kidolgozásában.
- Önállóan és pontosan vesz részt a kiberbiztonsági fenyegetések technológiai, politikai és adminisztratív megoldásában.
- Vállalja a kiberbiztonsági fenyegetések kezelésének felelősségét.
- Kezdeményezőként dolgozik a technikai és operatív teendők stratégiai célokká való konvertálásában.
- Gyakorlatába beépíti és alkalmazza az e szakterületen folyó kutatások eredményeit.

8. A szakirányú továbbképzés szakmai jellemzői, a szakképzettséghez vezető szakterületek és azok kreditaránya, amelyből a szak felépül:

- Államtudományi, jogi és közigazgatás-szervezési ismeretek - 10-15 kredit,
- Információbiztonsági és biztonságszervezési ismeretek - 25-35 kredit,
- Alkalmazott infokommunikációs szakismeretek - 10-20 kredit

II.
ÉRTÉKELÉSI ÉS ELLENŐRZÉSI MÓDSZEREK, ELJÁRÁSOK

9. Az ismeretek ellenőrzési rendszere

A tananyag ismeretének ellenőrzése és értékelése történhet:

a) szorgalmi időszakban a tanórán tett írásbeli vagy szóbeli számonkéréssel, írásbeli (zárthelyi) dolgozattal, otthoni munkával készített feladat értékelésével vagy gyakorlati feladat-végrehajtás értékelésével félévközi jegy formájában;
b) a vizsgaidőszakban tett vizsgával;
c) a félévközi követelmények és a vizsga alapján együttesen.

A hallgató tanulmányait záróvizsgával fejezi be. A záróvizsga az oklevél megszerzéséhez szükséges ismeretek, készségek és képességek ellenőrzése és értékelése, amelynek során a hallgatónak arról is tanúságot kell tennie, hogy a tanult ismereteket alkalmazni tudja.

Az értékeléstípusok rövidítései:

- évközi értékelés: ÉÉ / évközi értékelés (((záróvizsga tárgy((ÉÉ(Z)))
- gyakorlati jegy: GYJ / gyakorlati jegy (((záróvizsga tárgy((GYJ(Z)))
- kollokvium: K / kollokvium (((záróvizsga tárgy((K(Z)))
- beszámoló: B
- záróvizsga: ZV

Az ismeretek ellenőrzésének rendjét részletesen a vonatkozó jogszabályokban, valamint a Tanulmányi és Vizsgaszabályzatban meghatározottak alapján:

- a jelen ajánlott tanterv részét képező tantárgyi programok, valamint
- a záróvizsga tekintetében a jelen fejezet 10. pontja

határozzák meg.

10. A záróvizsga

10.1. A záróvizsgára bocsátás feltételei

A záróvizsgára bocsátás feltételei:
- az abszolutórium (végbizonyítvány) megszerzése: az Egyetem annak a hallgatónak, aki a tantervben előírt tanulmányi és vizsgakövetelményeket teljesítette, és az előírt krediteket megszerezte, végbizonyítványt állít ki (abszolutórium), amely minősítés és értékelés nélkül tanúsítja, hogy a hallgató a tantervben előírt tanulmányi és vizsgakövetelménynek mindenben eleget tett,
- az absztrakt elkészítése.

10.2. A záróvizsga részei

A záróvizsga az oklevél megszerzéséhez szükséges ismeretek, készségek és képességek ellenőrzése és értékelése, amelynek során a hallgatónak arról is tanúságot kell tennie, hogy a tanult ismereteket alkalmazni tudja.

A záróvizsga több részből: az absztrakt elkészítéséből, a prezentáció bemutatásából, továbbá az írásbeli vizsgarészből áll. Az írásbeli záróvizsga során a hallgatók a szakirányú továbbképzés során elsajátított ismereteket alkalmazva oldanak meg egy elképzelt kiberbiztonsági incidenst. Az írásbeli záróvizsga legalább 3 nappal megelőzi a prezentáció bemutatását.

A záróvizsgára történő felkészülés során a hallgatónak prezentációt és (a prezentációban feldolgozandó témát bemutató) absztraktot szükséges készítenie. A hallgató a záróvizsga keretében egy jól felépített, problémafelvetéssel és megoldási javaslatokkal ellátott prezentációt mutat be. Az absztrakt témakörét alkotó esetkört a hallgató az Elektronikus információbiztonsági vezető szakirányú továbbképzési szak tantárgyaihoz illeszkedve, a választott tantárgy felelősével vagy oktatójával előzetesen egyeztetve szabadon választja.
A hallgató a prezentáció során tisztán elméleti megközelítés helyett a konkrét esetet, problémát, körülményt, mért/tapasztalt jellemzőket, saját észrevételeket, javaslatokat, logikus érvelés keretében, a szakmai fogalomkészlet segítségével ismerteti.
A prezentációt követően a záróvizsga-bizottság tagjai – a prezentáció témaköréhez illeszkedően – kérdéseket intézhetnek a hallgatóhoz.

10.3 A záróvizsga eredménye

A záróvizsga érdemjegyét a kapott osztályzatok számtani átlaga adja. Bármelyik elem vizsgatételére kapott elégtelen osztályzat esetében a záróvizsga értékelése elégtelen.
Az egyes elemeket (írásbeli záróvizsga, absztrakt elkészítése és prezentáció bemutatása) külön érdemjeggyel kell értékelni.
A záróvizsga eredményét a záróvizsga részeredményeinek egyszerű átlaga képezi, az alábbiak szerint: ZvÖ=(ZvAP + ZvÍ) / 2

11. Szakdolgozat

A TVSZ 5. mellékletének I./1. bekezdése lehetőséget ad arra, hogy a szakirányú továbbképzésben részt vevő hallgató a képzési programban meghatározottak szerint szakdolgozatot készít azzal, hogy a képzési program eltérhet a szakdolgozat a TVSZ. mellékletében meghatározott tartalmi és formai követelményektől.

Ezek alapján a hallgató a 10. pontban meghatározott prezentációt és (a prezentációban feldolgozandó témát bemutató) absztraktot készít.

12. Az oklevél

12.1. Az oklevél kiadásának feltétele

Az oklevél kiadásának feltétele:

- az eredményes záróvizsga, továbbá
- a 60 kredit megszerzése.

12.2. Az oklevél minősítésének megállapítása

Az oklevél minősítését az alábbiak egyszerű átlaga adja meg:

a) az absztrakt elkészítésére és a prezentáció bemutatására adott osztályzat;
b) a záróvizsga írásbeli részére adott osztályzat;
c) a teljesített félévek (két tizedesig kifejezett) súlyozott tanulmányi átlagainak átlaga:

(ZvAP + ZvÍ + (Á1+…+Án)/n) / 3

Az oklevél minősítésének megállapítása az alábbi határértékek figyelembevételével történik:

a) kitűnő, ha az átlag 5,00
b) jeles, ha az átlag 4,51-4,99
c) jó, ha az átlag 3,51-4,50
d) közepes, ha az átlag 2,51-3,50
e) elégséges, ha az átlag legalább 2,00 – de legfeljebb 2,50.

Kiváló eredménnyel végez az a hallgató, akinek oklevél-minősítése kitűnő. Kiváló eredménnyel végez továbbá az is, akié jeles, valamint az összes többi vizsgájának és gyakorlati jegyének átlaga legalább 4,51.

Budapest, 2021. március 1.

Dr. Bányász Péter sk.
adjunktus, NKE ÁNTK

ELEKTRONIKUS INFORMÁCIÓBIZTONSÁGI VEZETŐ SZAKIRÁNYÚ TOVÁBBKÉPZÉSI SZAK
TANTERVE

Sorszám	Tantárgy neve	Félév	Típus	Óraszámok összesen	Óraszámok (elmélet+ gyakorlat)	Kreditérték	Számonkérés módja	Tantárgyfelelős
1.	**I. félév**			**150**	**116+34**	**30**		
1.1.	Információbiztonsági és adatvédelmi szabályozás	I.	kötelező	25	25+0	5	kollokvium	Dr. Péterfalvi Attila
1.2.	Az információbiztonság alapjai	I.	kötelező	25	15+10	5	kollokvium	Dr. Muha Lajos
1.3.	Információs rendszerek és hálózatok biztonsága 1.	I.	kötelező	15	15+0	3	kollokvium	Dr. Farkas Tibor
1.4.	Információbiztonsági szabványok	I.	kötelező	25	25+0	5	kollokvium	Dr. Muha Lajos
1.5.	Kockázatértékelés, kockázatmenedzsment	I.	kötelező	30	15+15	6	kollokvium	Dr. Tiszolczi Balázs Gergely
1.6.	Biztonságtechnika	I.	kötelező	10	10+0	2	gyakorlati jegy	Dr. László Gábor
1.7.	Biztonságpolitika	I.	kötelező	10	5+5	2	gyakorlati jegy	Dr. Kovács László
1.8.	Vezetéselmélet	I.	kötelező	10	6+4	2	gyakorlati jegy	Dr. Kovács Gábor
2.	**II. félév**			**130**	**70+60**	**30**		
2.1.	Incidensmenedzsment	II.	kötelező	30	15+15	6	kollokvium	Dr. Krasznay Csaba
2.2.	Biztonsági tesztelés	II.	kötelező	15	0+15	4	gyakorlati jegy	Dr. Tóth András
2.3.	Információbiztonsági stratégia és vezetés	II.	kötelező	25	10+15	6	gyakorlati jegy	Dr. Bányász Péter
2.4.	Kiberbiztonsági szabályozás Európában	II.	kötelező	25	25+0	6	kollokvium	Dr. Gyaraki Réka Eszter
2.5.	Válságmenedzsment és kommunikáció	II.	kötelező	15	0+15	4	gyakorlati jegy	Dr. Kriskó Edina
2.6.	Információs rendszerek és hálózatok biztonsága 2.	II.	kötelező	20	20+0	4	kollokvium	Dr. Farkas Tibor
	ÖSSZESEN			**280**	**186+94**	**60**		

ELEKTRONIKUS INFORMÁCIÓBIZTONSÁGI VEZETŐ SZAKIRÁNYÚ TOVÁBBKÉPZÉSI SZAK
TANTÁRGYI PROGRAMOK

1. TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** KVTIS634
2. **A tantárgy megnevezése (magyarul):** Információbiztonsági és adatvédelmi szabályozás
3. **A tantárgy megnevezése (angolul):** Legislation on Information Security and Data Protection
4. **Kreditérték és képzési karakter:**
   4.1. 5 kredit
   4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 0% gyakorlat, 100% elmélet
5. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** NKE KTI
6. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Péterfalvi Attila, egyetemi docens, NKE ÁNTK
7. **A tanórák száma és típusa:**
   7.1. összes óraszám/félév: 25 óra
   7.2. levelező munkarend: 25 óra (25 EA (vagy 25 óra online előadás, amennyiben az évfolyam létszáma indokolja) + 0 SZ + 0 GY)
8. **A tantárgy szakmai tartalma (magyarul):**

   A tantárgy célja, hogy a hallgató megismerje az információbiztonsági és az adatvédelmi szabályozás alapjait és összefüggéseit. Az elektronikus információbiztonság területén zajlott stratégiaalkotás bemutatása nemzeti és Európai Uniós szinten. A jogok és kötelezettségek elsajátítása és gyakorlati alkalmazása, a felelősségi szabályok megismerése. Az adatvédelem szükségességének erősítése, tudatosítása. Az információbiztonság és az adatvédelem szervezetei a nemzeti közigazgatásban.

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

   The purpose of the subject is to make the student aware of the basics and context of information security and data protection regulations. Presentation of strategy work in the field of electronic information security at national and European Union level. Mastering and practical application of rights and obligations, learning about liability rules. Strengthening and raising awareness of the need for data protection. Information security and data protection organizations in national administrations.
9. **Elérendő kompetenciák (magyarul):**

   Tudása:

   - Ismeri azokat a fontosabb előírásokat a szabályozásokból, amelyek a mindennapi munkáját befolyásolják.
   - Ismeri a kibertámadás esetén alkalmazandó eljárásokat.
   - Tisztában van az állami kibervédelmi rendszerrel.
   - Megérti a szervezeti feladatokat a kibervédelemben.

   Képességei:

   - Képes értelmezni a jogszabályokból eredő követelményeket.
   - Képes megszerezni a szervezet vezetőinek támogatását a jogszabályi megfelelőség kiépítéséhez.

   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.
- Kezdeményezőként dolgozik a technikai és operatív teendők stratégiai célokká való konvertálásában.

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 the procedures applicable in case of a cyberattack.
- He/She is familiar with the cybersecurity system of the state.
- He/She is familiar with organisational tasks in cyber security.

Capabilities:

- He/She is capable of interpreting legal requirements.
- He/She is capable of obtaining the support of leaders of the organisation in establishing regulatory compliance.

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:

- He/She is responsible for making professional proposals based on comprehensive knowledge of cyber security and dominant legal, regulatory and economical processes.
- He/She is an initiator to take the initiative to convert technical and operative tasks into strategic targets.

10. Előtanulmányi követelmények: -

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

11.1. Az elektronikus információbiztonság szabályozási környezete.
11.2. Az információbiztonság szervezetrendszere a nemzeti közigazgatásban és a kapcsolódó Uniós szervezetek.
11.3. Az adatvédelemi szabályozás alapjai.

11.1. Regulatory environment for electronic information security.
11.2. The organization of information security in national administrations and related EU organizations.
11.3. Fundamentals of data protection regulation and freedom of information.

12. A tantárgy meghirdetésének gyakorisága/a tantervben történő félévi elhelyezkedése: I. félév

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

Követelmény a tanórákon történő részvétel. A hallgató köteles a foglalkozások legalább 75%-án részt venni. Az elfogadható hiányzások mértéke 25%, az e feletti távolmaradás esetén a tantárgy oktatója által meghatározott feladatot szükséges teljesíteni.

14. Félévközi feladatok, ismeretek ellenőrzésének rendje: -

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

15.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele a 13. pontban meghatározott arányú részvétel a foglalkozásokon.

15.2. Az értékelés:

A félév végi számonkérés módja és formája: kollokvium, szóbeli vizsga, amelynek során a kötelező irodalom és a foglalkozások anyagának ismerete a követelmény.

15.3. A kreditek megszerzésének feltételei:

A kreditek megszerzésének feltétele az aláírás megszerzése és a legalább elégséges vizsgajegy.

16. Irodalomjegyzék:

16.1. Kötelező irodalom:

- Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat
- Magyarország hálózati és információs rendszerek biztonságára vonatkozó stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozat
- a kormányzati stratégiai irányításról szóló 38/2012. (III. 12.) Korm. rendelet
- az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény
- a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról szóló 38/2011. (III. 22.) Korm. rendelet
- az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet
- az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól szóló 271/2018. (XII. 20.) Korm. rendelet
- az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről szóló 270/2018. (XII. 20.) Korm. rendelet
- a központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről szóló 186/2015. (VII. 13.) Korm. rendelet
- a Kormányzati Adatközpont működéséről szóló 467/2017. (XII. 28.) Korm. rendelet
- a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről szóló 484/2013. (XII. 17.) Korm. rendelet
- az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, továbbá a biztonsági osztályba és a biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet
- az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról szóló 26/2013. (X. 21.) KIM rendelet
- a létfontosságú rendszerek és létesítmények védelmi szabályozását biztosító, a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény
- a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló 65/2013. (III. 8.) Korm. rendelet és az ágazati rendeletek
- az Európai Parlament és a Tanács 2016. július 6-i 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről
- a Tanács 2019. május 17-i 2019/796 rendelete az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről
- 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)
- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény
- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény
- a 29. cikk alapján létrehozott adatvédelmi munkacsoport és az Adatvédelmi Testület iránymutatásai

16.2. Ajánlott irodalom:

- Deák Veronika (szerk.): *Célzott kibertámadások. Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára 2018.* NKE, Budapest, 2019. ISBN: 978 963 498 062 9
- Deák Veronika (szerk.): *Kritikus információs infrastruktúrák védelme. Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára 2019*. NKE, Budapest, 2019. ISBN 978 963 498 239 5

Budapest, 2021. március 1.

Dr. Péterfalvi Attila sk.
egyetemi docens, NKE ÁNTK

2. TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** KVTIS635
2. **A tantárgy megnevezése (magyarul):** Az információbiztonság alapjai
3. **A tantárgy megnevezése (angolul):** Basics of Information Security
4. **Kreditérték és képzési karakter:**
   4.1. 5 kredit
   4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 40% gyakorlat, 60% elmélet
5. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** NKE KTI
6. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Muha Lajos, egyetemi docens, NKE RTK
7. **A tanórák száma és típusa:**
   7.1. összes óraszám/félév: 25 óra
   7.2. levelező munkarend: 25 óra (15 EA (vagy 15 óra online előadás, amennyiben az évfolyam létszáma indokolja)+ 0 SZ + 10 GY (vagy 10 óra online gyakorlat, amennyiben az évfolyam létszáma indokolja))
8. **A tantárgy szakmai tartalma (magyarul):**

   Az információs rendszerek fenyegetéseinek és védelmének fejlődése. Az információbiztonság alapvető fogalmai. Kapcsolódó szakterületek: a kibernetika, a játékelmélet, a kockázatelemzés és a számítógép védelmi modellek bemutatása. A kiberműveletek (kiberhadviselés) és a „kiberháborúk”, a kiberhidegháború. A kritikus információs infrastruktúrák védelme. A kiberbűnözés.

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

   The evolution of threats and protection of information systems. Basic definitions of information security. Related areas: the Cybernetics, the Game Theory, the Risk Analysis and the Computer Security Models. The Cyberoperations (cyberwarfare) and "cyberwars", Cybercoldwar. Critical Information Infrastructures Protection. Cybercrime.
9. **Elérendő kompetenciák (magyarul):**

   Tudása:

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

   Képességei:

   - 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.

   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.

Capabilities:

- He/She is capable of understanding the current threats 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:

- His/Her autonomy and responsibility are to implement advanced knowledge characterising cyber security on a national and international level.

10. Előtanulmányi követelmények: -

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

11.1. Az információs rendszerek fenyegetéseinek és védelmének fejlődése.
11.2. Az információbiztonság alapvető fogalmai.
11.3. Kapcsolódó szakterületek: a kibernetika, a játékelmélet, a kockázatelemzés és a számítógép védelmi modellek bemutatása.
11.4. A kiberműveletek (kiberhadviselés) és a „kiberháborúk", a kiberhidegháború.
11.5. A kiberterrorizmus, a kritikus információs infrastruktúrák védelme.
11.6. A kiberbűnözés.

11.1. The evolution of threats and protection of information systems.
11.2. Basic definitions of information security.
11.3. Related areas: the Cybernetics, the Game Theory, the Risk Analysis and the Computer Security Models.
11.4. The Cyberoperations (cyberwarfare) and "cyberwars", Cybercoldwar.
11.5. The Cyberterrorism, the Critical Information Infrastructures Protection.
11.6. The Cybercrime.

12. A tantárgy meghirdetésének gyakorisága/a tantervben történő félévi elhelyezkedése: I. félév

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

Követelmény a tanórákon történő részvétel. A hallgató köteles a foglalkozások legalább 75%-án részt venni. Az elfogadható hiányzások mértéke 25%, az e feletti távolmaradás esetén a tantárgy oktatója által meghatározott feladatot szükséges teljesíteni.

14. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A hallgató értékelése a szorgalmi időszakban a 11. pontban meghatározott, 11.3., a 11.4 vagy 11.6. témakörökhöz köthető, 15-20 perces kiselőadás megtartása alapján történik. Amennyiben az évfolyam létszáma nem teszi lehetővé a kiselőadások megtartását, az oktató írásban is bekérheti a kidolgozott témákat.

Az értékelés ötfokozatú: elégtelen (60% alatt), elégséges (61%-70%), közepes (71%-80%), jó (81%-90%), jeles (91%-100%). Pótlás, illetve 61% alatti eredmény esetén, javítási lehetőséget kell biztosítani a szorgalmi időszakban, egy alkalommal.

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

15.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele a 13. pontban meghatározott arányú részvétel a foglalkozásokon, valamint a 14. pontban meghatározott félévközi feladat legalább elégséges teljesítése.

15.2. Az értékelés:

A félév végi számonkérés módja és formája: kollokvium, az évfolyam létszámától függően írásbeli vagy szóbeli vizsga, amelynek során a kötelező irodalom és a foglalkozások anyagának ismerete a követelmény.

15.3. A kreditek megszerzésének feltételei:

A kreditek megszerzésének feltétele az aláírás megszerzése és a legalább elégséges vizsgajegy.

16. Irodalomjegyzék:

16.1. Kötelező irodalom:

- Muha Lajos – Krasznay Csaba: *Az elektronikus információs rendszerek biztonságának menedzselése*. NKE, Budapest, 2018. ISBN: 978 615 5870 27 9 (elektronikus)

16.2. Ajánlott irodalom:

- Kovács László: *A kibertér védelme.* Dialóg Campus Kiadó, Budapest, 2018. ISBN 978 615 5889 63 9 (nyomtatott) ISBN 978 615 5889 64 6 (elektronikus)
- Az Európai Parlament, a Tanács, az Európai Gazdasági és Szociális Bizottság és a Régiók Bizottsága Közös Közleménye – Az Európai Unió kiberbiztonsági stratégiája, 2013. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52013JC0001
- Europol's EC3: Internet Organised Crime Threat Assessment (IOCTA), 2019. https://extranet.ebf.eu/CorGovFinCri/AntMonLauAntFraCom/CyberSec/Documents/Draft/iocta_2019.pdf 2019. november 10.
- Singer, Peter W. – Friedman, Allan: *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, USA, 2014. ISBN: 978 019 991 811 9
- Brown, Lawrie - Stallings, William: *Computer Security: Principles and Practice, Pearson*. Pearson, 2018. (4. kiadás). ISBN-13: 978 013 479 410 5
- Gordon, Lawrence A. - Loeb, Martin P.: *The economics of information security investment*. In: ACM Transactions on Information and System Security (TISSEC), 2002. november.

Budapest, 2021. március 1.

Dr. Muha Lajos sk.
egyetemi docens, NKE RTK

3. TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** KVTIS636
2. **A tantárgy megnevezése (magyarul):** Információs rendszerek és hálózatok biztonsága 1.
3. **A tantárgy megnevezése (angolul):** Security of Information Systems and Networks 1.
4. **Kreditérték és képzési karakter:**
   4.1. 3 kredit
   4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 0% gyakorlat, 100% elmélet
5. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** NKE KTI
6. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Farkas Tibor, egyetemi docens, NKE HHK
7. **A tanórák száma és típusa:**
   7.1. összes óraszám/félév: 15 óra
   7.2. levelező munkarend: 15 óra (15 EA (vagy 15 óra online előadás, amennyiben az évfolyam létszáma indokolja)+ 0 SZ + 0 GY)
8. **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, előnyeinek meghatározása, a virtuális magánhálózatok (VPN) működésének leírása.

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

   Tudása:

   - Átlátja, hogy milyen védelmi megoldások vannak a kibertámadás ellen.

- Ismeri a kártékony kódok fogalmát és hatásmechanizmusát.

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:

- 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:

- He/She is familiar with defence solutions against cyberattacks.
- He/She is familiar with the concept and mode of action of malware codes.

Capabilities:

- He/She is capable of taking technological defensive measures related to elements of the cyber kill chain.
- He/She 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 cyberattacks, by this means reducing the exposure of his/her organisation.

Autonomy and responsibility:

- His/Her autonomy and responsibility are to take part in providing technological, political and administrative solutions to cyber threats.
- His/Her autonomy and responsibility are to take the initiative to convert technical and operative tasks into strategic targets.

10. Előtanulmányi követelmények: -

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

11.1. Korszerű számítógépek felépítése, működése.
11.2. Operációs rendszerek funkciói, működési elvei.
11.3. Hálózati protokollok és kommunikáció, Ethernet szabvány.
11.4. Hálózati és szállítási réteg.
11.5. Alkalmazási réteg.
11.6. Kapcsolt hálózatok, a kapcsolás beállításainak alapjai.
11.7. VLAN-ok.
11.8. A forgalomirányítás alapjai.
11.9. Statikus, dinamikus forgalomirányítás.
11.10. Hozzáférés vezérlési listák, DHCP, IPv4 hálózati címfordítás.
11.11. WAN technológiák jellemzői.
11.12. Virtuális magánhálózatok (VPN) működése.

11.1. Construction and operation of modern computers.
11.2. Functions and principles of operating systems.
11.3. Network protocols and communications, Ethernet standard.
11.4. Network and Transport Layer.

11.5. Application layer.
11.6. Switched networks, basics of switching settings.
11.7. VLANs.
11.8. The basics of routing.
11.9. Static and dynamic routing.
11.10. Access control lists, DHCP, IPv4 network address translation.
11.11. Features of WAN technologies.
11.12. Operation of virtual private networks (VPNs).

12. A tantárgy meghirdetésének gyakorisága/a tantervben történő félévi elhelyezkedése: I. félév

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

Követelmény a tanórákon történő részvétel. A hallgató köteles a foglalkozások legalább 75%-án részt venni. Az elfogadható hiányzások mértéke 25%, az e feletti távolmaradás esetén a tantárgy oktatója által meghatározott feladatot szükséges teljesíteni.

14. Félévközi feladatok, ismeretek ellenőrzésének rendje: -

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

15.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele a 13. pontban meghatározott arányú részvétel a foglalkozásokon.

15.2. Az értékelés:

A félév végi számonkérés módja és formája: kollokvium, írásbeli vizsga, amelynek során a kötelező irodalom és a foglalkozások anyagának ismerete a követelmény.

15.3. A kreditek megszerzésének feltételei:

A kreditek megszerzésének feltétele az aláírás megszerzése és a legalább elégséges vizsgajegy.

16. Irodalomjegyzék:

16.1. Kötelező irodalom:

- Tanenbaum, Andrew S. – Wetherall, David J.: *Számítógép-hálózatok*. Panem Kft., Budapest, 2013. ISBN: 978 963 545 529 4
- Tanenbaum, Andrew S.: *Számítógép-architektúrák*. Panem Kft., Budapest, 2007. ISBN: 978 963 545 457 0
- Petrényi József: *TCP/IP – alapok I. és II. kötet.* 2009. http://mek.oszk.hu/08300/08374/
- Dr. Kónya László: *Számítógép-hálózatok.* LSI Oktatóközpont, Budapest. ISBN: 963 577 22 X
- Kurose, James F. – Ross, Keith W.: *Számítógép-hálózatok működése*. Panem Kft., Budapest, 2009. ISBN 978 963 545 498 3

16.2. Ajánlott irodalom:

- Brown, Lawrie - Stallings, William: *Computer Security: Principles and Practice, Pearson*. Pearson, 2018. (4. kiadás). ISBN-13: 978 013 479 410 5
- Borbély Balázs: *Otthoni és irodai hálózatok zsebkönyve.* Jedlik Oktatási Stúdió, Budapest, 2018. ISBN: 978 615 501 231 0
- Casad, Joe: *Tanuljuk meg a TCP/IP használatát 24 óra alatt*. Kiskapu Kiadó, Budapest, 2010. ISBN: 978 963 963 768 9
- Rusen, Ciprian Adrian: *Számítógépes eszközök hálózatba kötése - Lépésről lépésre.* Szak Kiadó, Budapest, 2011. ISBN: 978 963 986 321 7

- Gál Tamás - Szabó Levente - Szerényi László: *Rendszerfelügyelet rendszergazdáknak*. Szak Kiadó, Budapest, 2007. ISBN 978 963 913 198 9

Budapest, 2021. március 1.

Dr. Farkas Tibor sk.
egyetemi docens, NKE HHK

4. TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** KVTIS637
2. **A tantárgy megnevezése (magyarul):** Információbiztonsági szabványok
3. **A tantárgy megnevezése (angolul):** Information Security Standards
4. **Kreditérték és képzési karakter:**
   4.1. 5 kredit
   4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 0% gyakorlat, 100% elmélet
5. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** NKE KTI
6. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Muha Lajos, egyetemi docens, NKE RTK
7. **A tanórák száma és típusa:**
   7.1. összes óraszám/félév: 25 óra
   7.2. levelező munkarend: 25 óra (25 EA (vagy 25 óra online előadás, amennyiben az évfolyam létszáma indokolja)+ 0 SZ + 0 GY)
8. **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 cybersecurity regulators and key standards.
9. **Elérendő kompetenciák (magyarul):**

   Tudása:

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

   Képességei:

   - Képes támogatni szervezetét a kibervédelmi képességek kialakításában.

   Attitűdje:

   - Munkája során figyelembe veszi és alkalmazza a kiberbiztonsággal kapcsolatos jogszabályokat.

   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:

   - He/She is familiar with the specifications of regulations that have an immediate impact on his/her daily work.

   Capabilities:

   - He/She is capable of supporting his/her organisation in developing cyber security skills.

Attitude:

- His/Her personal attitude is characterized by an attention to and application of laws of cybersecurity in his/her work.

Autonomy and responsibility:

- His/Her 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.

10. Előtanulmányi követelmények: -

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

11.1. A szabványok fogalma, az információbiztonsági szabványok összefüggései és felhasználási lehetőségeik.
11.2. Az ISO/IEC 27xxx sorozat.
11.3. Az ISO/IEC 27001 szabvány szerinti Információbiztonsági Irányítási Rendszer és tanúsítása.
11.4. ISO 19011:2011 – Guidelines for auditing management systems.
11.5. A NIST SP 800 sorozat és az SP 800-53.
11.6. Common Criteria.
11.7. COBIT.
11.8. ITIL.
11.9. Enterprise Information Security Architecture (EISA).
11.10. Payment Card Industry Data Security Standard.

11.1. Concept of standards, relations between information security standards and their potential usage.
11.2. The ISO/IEC 27xxx series.
11.3. The ISO/IEC 27001 standard based Information Security Management System and its certification.
11.4. ISO 19011:2011 – Guidelines for auditing management systems.
11.5. NIST SP 800 series and SP 800-53.
11.6. Common Criteria.
11.7. COBIT.
11.8. ITIL.
11.9. Enterprise Information Security Architecture (EISA).
11.10. Payment Card Industry Data Security Standard (PCI DSS).

12. A tantárgy meghirdetésének gyakorisága/a tantervben történő félévi elhelyezkedése: I. félév

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

Követelmény a tanórákon történő részvétel. A hallgató köteles a foglalkozások legalább 75%-án részt venni. Az elfogadható hiányzások mértéke 25%, az e feletti távolmaradás esetén a tantárgy oktatója által meghatározott feladatot szükséges teljesíteni.

14. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A hallgató értékelése a szorgalmi időszakban, a 11. pontban meghatározott, 11.3. témakörhöz köthető, 5000 leütést tartalmazó beadandó dolgozat alapján történik.

Az értékelés ötfokozatú: elégtelen (60% alatt), elégséges (61%-70%), közepes (71%-80%), jó (81%-90%), jeles (91%-100%). Pótlás, illetve 61% alatti eredmény esetén, javítási lehetőséget kell biztosítani a szorgalmi időszakban, egy alkalommal.

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

15.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele a 13. pontban meghatározott arányú részvétel a

foglalkozásokon, valamint a 14. pontban meghatározott félévközi feladat legalább elégséges teljesítése.

15.2. Az értékelés:

A félév végi számonkérés módja és formája: kollokvium, az évfolyam létszámától függően írásbeli vagy szóbeli vizsga, amelynek során a kötelező irodalom és a foglalkozások anyagának ismerete a követelmény.

15.3. A kreditek megszerzésének feltételei:

A kreditek megszerzésének feltétele az aláírás megszerzése és a legalább elégséges vizsgajegy.

16. Irodalomjegyzék:

16.1. Kötelező irodalom:

- Szádeczky Tamás: *Információbiztonsági szabványok.* NKE, Budapest, 2014., egyetemi jegyzet.

16.2. Ajánlott irodalom:

- Muha Lajos – Krasznay Csaba: *Az elektronikus információs rendszerek biztonságának menedzselése*. NKE, Budapest, 2018. ISBN: 978 615 5870 27 9 (elektronikus)
- Magyar Informatikai Biztonsági Ajánlások (MIBA) – KIB 25. számú ajánlás, Budapest, 2008.

Budapest, 2021. március 1.

Dr. Muha Lajos sk.
egyetemi docens, NKE RTK

5. TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** KVTIS638
2. **A tantárgy megnevezése (magyarul):** Kockázatértékelés, kockázatmenedzsment
3. **A tantárgy megnevezése (angolul):** Risk Assessment, Risk Management
4. **Kreditérték és képzési karakter:**
   4.1. 6 kredit
   4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 50% gyakorlat, 50% elmélet
5. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** NKE KTI
6. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Tiszolczi Balázs Gergely, adjunktus, NKE RTK
7. **A tanórák száma és típusa:**
   7.1. összes óraszám/félév: 30 óra
   7.2. levelező munkarend: 30 óra (15 EA (vagy 15 óra online előadás, amennyiben az évfolyam létszáma indokolja)+ 0 SZ + 15 GY (vagy 15 óra online gyakorlat, amennyiben az évfolyam létszáma indokolja))
8. **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 COBIT2019, ITILv4, 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 COBIT2019, ITILv4, 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.
9. **Elérendő kompetenciák (magyarul):**

   Tudása:

   - Ismeri azokat a fontosabb előírásokat a szabályozásokból, amelyek a mindennapi munkáját befolyásolják.
   - Átlátja a munkáltatók által meghatározott belső szabályzatok megalkotásának szükségességét az információs rendszerekben tárolt adatok sértetlensége és a rendelkezésre állás tekintetében.

Képességei:

- Képes megszerezni a szervezet vezetőinek támogatását a jogszabályi megfelelőség kiépítéséhez.
- Képes olyan védelmi intézkedések meghozatalára, amelyek segítik a humán fenyegetettségből eredő kockázatok csökkentését.
- Képes felmérni a belső munkavállalók jelentette kiberbiztonsági kockázatokat.
- Képes olyan szabályzatok alkotására, amelyek a belső munkavállalók jelentette fenyegetések kezelésére vonatkoznak.
- Képes átlátni a kibertér aktuális fenyegetéseit.

Attitűdje:

- Hatékony lépéseket tesz a kibertámadások megelőzése érdekében, így csökkentve a szervezete kitettségét.
- Kiemelt kockázatként kezeli a belső munkavállalókat, és ennek megfelelően tervezi meg az információbiztonsági folyamatokat.

Autonómiája és felelőssége:

- Önállóan dolgozza fel az új és összetett információkat, problémákat, illetve jelenségeket, rendszerszerű és kritikus módon.
- 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 the need for introducing internal regulations defined by employers in order to maintain integrity and availability of the data stored in information systems.

Capabilities:

- He/She is capable of obtaining the support of leaders of the organisation in establishing regulatory compliance.
- He/She is capable of taking defensive measures that ensure the reduction of risk resulting from threat against humans.
- 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 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 cyberattacks, 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:

- His/Her autonomy and responsibility are to process new and complex information, problems and phenomena in a systematic and critical way.
- His/Her autonomy and responsibility are to handle cyber security threats.

10. Előtanulmányi követelmények: -

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

11.1. Bevezetés: a 2013. évi L. tv. és a CISM alapú kockázatmenedzsment.
11.2. Alapfogalmak „ISO-s” alapokon.
11.3. Egy kis kitérő: ISO alapú szabványosítás.

11.4. Az ISO 27000-es szabványcsalád és a kockázatelemzés szabványa.
11.5. Kockázatkezelési opciók ISO 27005 alapon.
11.6. Kockázatértékelés és ISO 27001:2013.
11.7. A kockázatértékelés áttekintő algoritmusa.
11.8. Kockázatértékelési esettanulmányok.
11.9. Szabályozott kockázatmenedzsment (Áttekintés: COBIT2019, ITILv4, Octave, ISO 73, ISO/IEC 31000, ISO 13335, NIST 800).
11.10. Kockázatmenedzsment a 2013. évi L. törvényben és a 41/2015 BM rendeletben.
11.11. A kockázatértékelési folyamat (azonosítás, elemzés, kiértékelés).
11.12. Kockázati forgatókönyv.
11.13. Általánosítható következtetések.
11.14. Kockázatmenedzsment ISO 27005:2018 mentén.
11.15. Általános kockázatmenedzsment – ISO 31000:2018.
11.16. Kockázatmenedzsment – kockázatkezelési terv.
11.17. Lehetséges intézkedések meghatározása és értékelése.
11.18. Az információvédelmi intézkedések területei.
11.19. A kockázatértékelés karbantartása (megismétlése).
11.20. Vagyonleltár és sebezhetőség vizsgálat.
11.21. Kockázatbecslés (kvantitatív, kvalitatív, szemikvantitatív).

11.1. Introduction: risk assessment based on the Act L of 2103 and CISM.
11.2. Definitions based on ISO.
11.3. ISO based standardisation.
11.4. ISO 27000 standard family and its risk assessment standard (ISO 27005).
11.5. Risk management options based on ISO 27005.
11.6. Risk assessment and ISO 27001:2013.
11.7. Review algorithm of risk assessment.
11.8. Risk assessment case studies.
11.9. Regulated risk management (Review: COBIT2019, ITILv4, Octave, ISO 73, ISO/IEC 31000, ISO 13335, NIST 800).
11.10. Risk assessment in the Act L of 2013 and Decree 41/2015.
11.11. Risk assessment process (identification, analysis, evaluation).
11.12. Risk scenario.
11.13. Generalizable conclusions.
11.14. Risk management according to ISO 27005:2018.
11.15. General risk management – ISO 31000:2018.
11.16. Risk management plan.
11.17. Identification and evaluation of potential countermeasures.
11.18. Areas of countermeasures in information security.
11.19. Review (repeat) of risk assessment.
11.20. Asset and vulnerability assessment.
11.21. Risk estimation (quantitative, qualitative, semi-quantitative).

12. A tantárgy meghirdetésének gyakorisága/a tantervben történő félévi elhelyezkedése: I. félév

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

Követelmény a tanórákon történő részvétel. A hallgató köteles a foglalkozások legalább 75%-án részt venni. Az elfogadható hiányzások mértéke 25%, az e feletti távolmaradás esetén a tantárgy oktatója által meghatározott feladatot szükséges teljesíteni.

14. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A hallgató értékelése a szorgalmi időszakban a 11. pontban meghatározott témakörökhöz köthető, 5000 leütést tartalmazó beadandó dolgozat alapján történik.

Az értékelés ötfokozatú: elégtelen (60% alatt), elégséges (61%-70%), közepes (71%-80%), jó (81%-90%), jeles (91%-100%). Pótlás, illetve 61% alatti eredmény esetén, javítási lehetőséget kell biztosítani a szorgalmi időszakban, egy alkalommal.

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

15.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele a 13. pontban meghatározott arányú részvétel a foglalkozásokon, valamint a 14. pontban meghatározott félévközi feladat legalább elégséges teljesítése.

15.2. Az értékelés:

A félév végi számonkérés módja és formája: kollokvium, írásbeli vizsga, amelynek során a kötelező irodalom és a foglalkozások anyagának ismerete a követelmény.

15.3. A kreditek megszerzésének feltételei:

A kreditek megszerzésének feltétele az aláírás megszerzése és a legalább elégséges vizsgajegy.

16. Irodalomjegyzék:

16.1. Kötelező irodalom:

- László Gábor: *Kockázatértékelés, kockázatmenedzsment.* NKE, Budapest, 2014., egyetemi jegyzet
- Som Zoltán: *Kockázatmenedzsment gyakorlat.* NKE, Budapest, 2014. ISBN: 978 615 505 755 7

16.2. Ajánlott irodalom:

- Wheeler, Evan: *Security Risk Management: Building an Information Security Risk Management Program from the Ground Up.* Syngress, 2011. ISBN 978 159 749 615 5
- Talabis, Mark: *Information Security Risk Assessment Toolkit.* Syngress, 2012. ISBN: 978 159 749 735 0

Budapest, 2021. március 1.

Dr. Tiszolczi Balázs Gergely sk.
adjunktus, NKE RTK

6. TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** KVTIS639
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: 0% gyakorlat, 100% elmélet
5. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** NKE KTI
6. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. László Gábor, adjunktus, NKE ÁNTK
7. **A tanórák száma és típusa:**
   7.1. összes óraszám/félév: 10 óra
   7.2. levelező munkarend: 10 óra (10 EA (vagy 10 óra online előadás, amennyiben az évfolyam létszáma indokolja)+ 0 SZ + 0 GY)
8. **A tantárgy szakmai tartalma (magyarul):**

   A hallgatók megismerik a komplex vagyonvédelem fogalmát, felépítését, összetevőit, valamint az elemeinek egymásra épülését. Ezen belül bemutatásra kerülnek a mechanikai védelem elemei és eszközei (falazat, nyílászárók, zárak, rácsok, kerítések). Részletesen foglalkoznak az elektronikus vagyonvédelem területeivel és az integrált vagyonvédelem kialakításával, így a behatolásjelző 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 a 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 (e.g. 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 entry control systems.
9. **Elérendő kompetenciák (magyarul):**

   Tudása:

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

   Képességei:

   - Képes támogatni szervezetét a kibervédelmi képességek kialakításában.

   Attitűdje:

   - A maga komplexitásában tervezi meg az információbiztonsági irányítási rendszert.

Autonómiája és felelőssége:

- Kezdeményezőként dolgozik a technikai és operatív teendők stratégiai célokká való konvertálásában.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge:

- He/She is familiar with specifications of regulations that have an immediate impact on his/her daily work.

Capabilities:

- He/She is capable of supporting his/her organisation in developing cyber security skills.

Attitude:

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

Autonomy and responsibility:

- His/Her autonomy and responsibility are to take the initiative to convert technical and operative tasks into strategic targets.

10. Előtanulmányi követelmények: -

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

11.1. A komplex vagyonvédelem fogalma, felépítése, összetevői, egymásra épülésük.
11.2. Mechanikai védelem elemei.
11.3. Az elektronikus vagyonvédelem területei. Integrált vagyonvédelem.
11.4. Behatolásjelző rendszerek felépítése.
11.5. Video felügyeleti (CCTV) rendszerek alkalmazási területei, jogi hátterük, felépítésük, eszközeik.
11.6. Tűzjelző rendszerek felépítése, funkciói, fajtái. Tűzjelző érzékelők.
11.7. Beléptető rendszerek és paramétereik.

11.1. The concept, structure, components and complexity of physical security.
11.2. Elements of mechanical protection.
11.3. Areas of electronic security. Integrated protection.
11.4. Construction of intrusion detection systems.
11.5. Applications of video surveillance (CCTV) systems, legal background, structure, tools.
11.6. Structure, functions and types of fire alarm systems. Fire detectors.
11.7. Access control systems and their parameters.

12. A tantárgy meghirdetésének gyakorisága/a tantervben történő félévi elhelyezkedése: I. félév

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

Követelmény a tanórákon történő részvétel. A hallgató köteles a foglalkozások legalább 75%-án részt venni. Az elfogadható hiányzások mértéke 25%, az e feletti távolmaradás esetén a tantárgy oktatója által meghatározott feladatot szükséges teljesíteni.

14. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A hallgató értékelése a szorgalmi időszak során egy zárthelyi dolgozat sikeres teljesítése alapján történik, amelynek követelménye a foglalkozásokon elhangzott ismeretanyag.

Az értékelés ötfokozatú: elégtelen (60% alatt), elégséges (61%-70%), közepes (71%-80%), jó (81%-90%), jeles (91%-100%). Pótlás, illetve 61% alatti eredmény esetén, javítási lehetőséget kell biztosítani a szorgalmi időszakban, egy alkalommal.

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

15.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele a 13. pontban meghatározott arányú részvétel a foglalkozásokon, valamint a 14. pontban meghatározott félévközi feladat legalább elégséges teljesítése.

15.2. Az értékelés:

A félévközi számonkérés módja és formája: gyakorlati jegy, amely a félévközi feladat sikeres teljesítéséből, valamint az órai teljesítmény értékeléséből áll (50-50%-os arányban).

15.3. A kreditek megszerzésének feltételei:

A kreditek megszerzésének feltétele az aláírás megszerzése és a legalább elégséges félévközi jegy.

16. Irodalomjegyzék:

16.1. Kötelező irodalom:

- Berek Lajos: *Biztonságtechnika.* NKE, Budapest, 2014. ISBN 978 615 549 151 1

16.2. Ajánlott irodalom:

- Knoke, Michael E. - Peterson, Kevin E. (eds.): *Physical Security Principles.* ASIS International, 2015. ISBN-13: 978 193 490 461 9

Budapest, 2021. március 1.

Dr. László Gábor sk.
adjunktus, NKE ÁNTK

7. TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** KVTIS640
2. **A tantárgy megnevezése (magyarul):** Biztonságpolitika
3. **A tantárgy megnevezése (angolul):** Security Policy
4. **Kreditérték és képzési karakter:**
   4.1. 2 kredit
   4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 50% gyakorlat, 50% elmélet
5. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** NKE KTI
6. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Kovács László, egyetemi tanár, NKE HHK
7. **A tanórák száma és típusa:**
   7.1. összes óraszám/félév: 10 óra
   7.2. levelező munkarend: 10 óra (5 EA (vagy 5 óra online előadás, amennyiben az évfolyam létszáma indokolja)+ 0 SZ + 5 GY (vagy 5 óra online gyakorlat, amennyiben az évfolyam létszáma indokolja))
8. **A tantárgy szakmai tartalma (magyarul):**

   A tantárgy oktatása során bemutatásra kerül a biztonságpolitika fogalma és tárgya. Biztonságpolitika Magyarországon, valamint biztonság és biztonságpolitika a kibertérben. A biztonságpolitika változása és a megváltozott környezet mellett az információtechnológia biztonságpolitikára és hadügyre gyakorolt hatása. Kiberműveletek és kiberhadviselés. Kína, Oroszország és az USA, mint globális (kiber) biztonságpolitikai tényezők. Terrorizmus, mint biztonságpolitikai kihívás a kibertérben. Az Európai Unió és a NATO kibervédelmi politikája és stratégiája. Nemzeti kibervédelmi stratégiák: Magyarország, Lengyelország, Cseh Köztársaság, Szlovák Köztársaság.

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

   The course introduces the concept and subject matter of security policy. Security policy in Hungary and security and safety policy in cyberspace. The change of security policy and the changed environment, the impact of information technology on security policy and warfare. Cyber operations and cyber warfare. China, Russia and the US as global (cyber) security policy actors. Terrorism as a Security Policy Challenge in Cyberspace. European Union and NATO cyber defense policy and strategy. National cyber defense strategies: Hungary, Poland, Czech Republic, Slovak Republic.

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

   Tudása:

   - Tisztában van az állami kibervédelmi rendszerrel.

   Képességei:

   - Képes átlátni a kibertér aktuális fenyegetéseit.

   Attitűdje:

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

   Autonómiája és felelőssége:

   - Önállóan dolgozza fel az új és összetett információkat, problémákat, illetve jelenségeket, rendszerszerű és kritikus módon.
   - Önállóan és pontosan vesz részt a kiberbiztonsági fenyegetések technológiai, politikai és adminisztratív megoldásában.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge:

- He/She is familiar with the cyber security system of the state.

Capabilities:

- He/She is capable of understanding the current threats of cyber space.

Attitude:

- His/Her personal attitude is characterized by a cooperation in preventing his/her organisation and him/herself from becoming a victim of a cyberattack.

Autonomy and responsibility:

- His/Her autonomy and responsibility are to process new and complex information, problems and phenomena in a systematic and critical way.
- His/Her autonomy and responsibility are to take part in providing technological, political and administrative solutions to cyber threats.

10. Előtanulmányi követelmények: -

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

11.1. A biztonságpolitika fogalma és tárgya.
11.2. Biztonságpolitika Magyarországon.
11.3. Biztonság és biztonságpolitika a kibertérben.
11.4. A biztonságpolitika változása, a megváltozott környezet és az információtechnológia biztonságpolitikára és hadügyre gyakorolt hatása.
11.5. Kiberműveletek és kiberhadviselés.
11.6. Kína, Oroszország és az USA, mint globális (kiber) biztonságpolitikai tényezők.
11.7. Terrorizmus, mint biztonságpolitikai kihívás a kibertérben.
11.8. Az Európai Unió és a NATO kibervédelmi politikája és stratégiája.
11.9. Nemzeti kibervédelmi stratégiák: Magyarország, Lengyelország, Cseh Köztársaság, Szlovák Köztársaság.

11.1. The concept and subject of security policy.
11.2. Security Policy in Hungary.
11.3. Security and security policy in cyberspace.
11.4. Change in security policy, changed environment, the impact of information technology on security policy and warfare.
11.5. Cyber operations and cyber warfare.
11.6. China, Russia and USA ass global [cyber] security policy actors.
11.7. Terrorism as a security policy challenge in cyberspace.
11.8. Cyber Defense Policy and Strategy of the European Union and NATO.
11.9. National cyber defense strategies: Hungary, Poland, Czech Republic, Slovak Republic.

12. A tantárgy meghirdetésének gyakorisága/a tantervben történő félévi elhelyezkedése: I. félév

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

Követelmény a tanórákon történő részvétel. A hallgató köteles a foglalkozások legalább 75%-án részt venni. Az elfogadható hiányzások mértéke 25%, az e feletti távolmaradás esetén a tantárgy oktatója által meghatározott feladatot szükséges teljesíteni.

14. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A hallgató értékelése a szorgalmi időszakban a 11. pontban meghatározott témakörökhöz köthető gyakorlati feladat kidolgozása, valamint annak 10-15 perces kiselőadás formájában történő ismertetése alapján zajlik. Amennyiben az évfolyam létszáma nem teszi lehetővé a kiselőadások megtartását, az oktató írásban is bekérheti a kidolgozott témákat.

Az értékelés ötfokozatú: elégtelen (60% alatt), elégséges (61%-70%), közepes (71%-80%), jó (81%-90%), jeles (91%-100%). Pótlás, illetve 61% alatti eredmény esetén, javítási lehetőséget kell biztosítani a szorgalmi időszakban, egy alkalommal.

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

15.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele a 13. pontban meghatározott arányú részvétel a foglalkozásokon, valamint a 14. pontban meghatározott félévközi feladat legalább elégséges teljesítése.

15.2. Az értékelés:

A félévközi számonkérés módja és formája: gyakorlati jegy, amely az oktató által adott gyakorlati feladat sikeres teljesítéséből, valamint az órai teljesítmény értékeléséből áll (50-50%-os arányban).

15.3. A kreditek megszerzésének feltételei:

A kreditek megszerzésének feltétele az aláírás megszerzése és a legalább elégséges félévközi jegy.

16. Irodalomjegyzék:

16.1. Kötelező irodalom:

- Kovács László: *Biztonságpolitika*. NKE, Budapest, 2014., egyetemi jegyzet
- Kovács László (2018): *Kiberbiztonság és -stratégia.* Dialóg Campus Kiadó, Budapest, 2018. ISBN 978 615 592 092 9 (nyomtatott), ISBN 978 615 592 093 6 (elektronikus)

16.2. Ajánlott irodalom:

- Kovács László: *A kibertér védelme.* Dialóg Campus Kiadó, Budapest, 2018. ISBN 978 615 588 963 9 (nyomtatott), ISBN 978 615 588 964 6 (elektronikus)

Budapest, 2021. március 1.

Dr. Kovács László sk.
egyetemi tanár, NKE HHK

8. TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** KVTIS641
2. **A tantárgy megnevezése (magyarul):** Vezetéselmélet
3. **A tantárgy megnevezése (angolul):** Theory of Leadership and Management
4. **Kreditérték és képzési karakter:**
   4.1. 2 kredit
   4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 40% gyakorlat, 60% elmélet
5. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** NKE KTI
6. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Kovács Gábor, egyetemi tanár, NKE RTK
7. **A tanórák száma és típusa:**
   7.1. összes óraszám/félév: 10 óra
   7.2. levelező munkarend: 10 óra (6 EA (vagy 6 óra online előadás, amennyiben az évfolyam létszáma indokolja) + 0 SZ + 4 GY (vagy 4 óra online gyakorlat, amennyiben az évfolyam létszáma indokolja))
8. **A tantárgy szakmai tartalma (magyarul):**

   Az előadás bemutatja a vezetés és vezetők szerepét, a vezetési folyamatot, a vezetési rendszer elemeit. Foglalkozik továbbá a szervezettel és környezetével, a célkitűzéssel és stratégiaalkotással. Bemutatja a szervezetek diagnosztizálását, a munkaszervezést és feladattervezést, valamint az emberierőforrás-gazdálkodást. A hallgatók megismerhetik a motiváció, a vezetési stílus és a kommunikáció fontosságát. Végül kitér a szervezetben lévő csoportokra, a szervezeti konfliktusokra és változásokra, a változásirányításra, ezen keresztül pedig a szervezetfejlesztésre.

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

   The course introduces the role of leadership and management, the leadership process and the elements of the management system. It deals with the organization and environment and the objectives and strategy development. Introduces the diagnostics of organizations, work organization and task planning, and Human Resource Management. Students can learn about the importance of motivation, management style and communication. At last, it discusses groups in the organization, organizational conflict, organizational change, change management and organizational development.
9. **Elérendő kompetenciák (magyarul):**

   Tudása:

   - Megérti a szervezeti feladatokat a kibervédelemben.

   Képességei:

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

   Attitűdje:

   - A maga komplexitásában tervezi meg az információbiztonsági irányítási rendszert.
   - Hatékony lépéseket tesz a kibertámadások megelőzése érdekében, így csökkentve a szervezete kitettségét.

Autonómiája és felelőssége:

- Önállóan és pontosan vesz részt a kiberbiztonsági fenyegetések technológiai, politikai és adminisztratív megoldásában.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge:

- He/She is familiar with the organisational tasks in cyber security.

Capabilities:

- He/She is capable of taking defensive measures that ensure the reduction of risk resulting from threat against humans.
- He/She is capable of supporting his/her organisation and external parties in handling a cyberattack.

Attitude:

- His/Her personal attitude is characterized by an effort to design the cybersecurity management system in its own complexity.
- His/Her personal attitude is characterized by an effort to take effective measures in order to prevent cyberattacks, by this means reducing the exposure of his/her organisation.

Autonomy and responsibility:

- His/Her autonomy and responsibility are to take part in providing technological, political and administrative solutions to cyber threats.

10. Előtanulmányi követelmények: -

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

11.1. A vezetéselmélet fő iskolái és irányzatai, a vezető és a vezetés, a szervezet és környezete.
11.2. A vezetési folyamat elemei, a munkaszervezés, a feladattervezés, a vezetési stílus.
11.3. Szervezetek fejlesztése, változásvezetés, motiváció, csoportok a szervezetben, projektmenedzsment.
11.4. Zárthelyi dolgozat.

11.1. The main schools of management, the leader and the management, the organizations.
11.2. The element of the leadership process.
11.3. Diagnosis and development of the organizations, motivation, change management and project management.
11.4. Written examination.

12. A tantárgy meghirdetésének gyakorisága/a tantervben történő félévi elhelyezkedése: I. félév

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

Követelmény a tanórákon történő részvétel. A hallgató köteles a foglalkozások legalább 75%-án részt venni. Az elfogadható hiányzások mértéke 25%, az e feletti távolmaradás esetén a tantárgy oktatója által meghatározott feladatot szükséges teljesíteni.

14. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A hallgató értékelése a szorgalmi időszakban a 11. pontban meghatározott témakörökhöz köthető, 15-20 perces kiselőadás megtartása (az értékelés 50%-át adja), továbbá az utolsó órán egy zárthelyi dolgozat sikeres teljesítése a foglalkozásokon elhangzott ismeretanyagból (az értékelés 50%-át adja). Amennyiben az évfolyam létszáma nem teszi lehetővé a kiselőadások megtartását, az oktató írásban is bekérheti a kidolgozott témákat.

Az értékelés ötfokozatú: elégtelen (60% alatt), elégséges (61%-70%), közepes (71%-80%), jó (81%-90%), jeles (91%-100%). Pótlás, illetve 61% alatti eredmény esetén, javítási lehetőséget kell biztosítani a szorgalmi időszakban, egy alkalommal.

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

15.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele a 13. pontban meghatározott arányú részvétel a foglalkozásokon, valamint a 14. pontban meghatározott félévközi feladat legalább elégséges teljesítése.

15.2. Az értékelés:

A félévközi számonkérés módja és formája: gyakorlati jegy, amely a gyakorlati feladat sikeres teljesítéséből (kiselőadás vagy esszé, az évfolyam létszámától függően), valamint a zárthelyi dolgozat értékeléséből áll (50-50%-os arányban).

15.3. A kreditek megszerzésének feltételei:

A kreditek megszerzésének feltétele az aláírás megszerzése és a legalább elégséges félévközi jegy.

16. Irodalomjegyzék:

16.1. Kötelező irodalom:

- Czuprák Ottó – Kovács Gábor: *A szervezetvezetés elmélete.* Dialóg Campus Kiadó, Budapest 2017. ISBN 978 615 576 442 4 (nyomtatott), ISBN 978 615 576 443 1 (elektronikus)
- Kovács Gábor (szerk.): *Közszolgálati műveletirányítási rendszerek.* Dialóg Campus Kiadó, Budapest, 2017. ISBN: 978 615 584 529 1 (nyomtatott), ISBN: 978 615 584 530 7 (elektronikus)

16.2. Ajánlott irodalom:

- Horváth József - Kovács Gábor (szerk.): *Pályakezdő Rendőrtisztek Kézikönyve.* NKE, Budapest, 2016. ISBN: 978 615 552 795 1
- Kovács Gábor (szerk.): *Vezetőktől a gyakorlati vezetéstudományról.* Dialóg Campus Kiadó, Budapest, 2017. ISBN: 978 615 568 029 8
- Horváth József – Kovács Gábor (szerk.): *A rendészeti szervek vezetés és szervezéselmélete.* NKTK Kiadó, Budapest, 2014. ISBN: 978 615 530 541 2

Budapest, 2021. március 1.

Dr. Kovács Gábor sk.
egyetemi tanár, NKE RTK

9. TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** KVTIS642
2. **A tantárgy megnevezése (magyarul):** Incidensmenedzsment
3. **A tantárgy megnevezése (angolul):** Incident management
4. **Kreditérték és képzési karakter:**
   4.1. 6 kredit
   4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 50% gyakorlat, 50% elmélet
5. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** NKE KTI
6. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Krasznay Csaba, egyetemi docens, NKE ÁNTK
7. **A tanórák száma és típusa:**
   7.1. összes óraszám/félév: 30 óra
   7.2. levelező munkarend: 30 óra (15 EA (vagy 15 óra online előadás, amennyiben az évfolyam létszáma indokolja)+ 0 SZ + 15 GY (vagy 15 óra online gyakorlat, amennyiben az évfolyam létszáma indokolja))
8. **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 üzletmenet-folytonosság tervezési kérdéseire is. Az előadás tárgyalja az incidensekkel kapcsolatos információk megosztásának módját a hivatalos és az iparági szereplőkkel. A gyakorlati foglalkozások során bemutatásra kerülnek az incidensmenedzsment folyamat technikai eszközei, melyek 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.
9. **Elérendő kompetenciák (magyarul):**

   Tudása:

   - Ismeri azokat a fontosabb előírásokat a szabályozásokból, amelyek a mindennapi munkáját befolyásolják.
   - Átlátja, hogy milyen védelmi megoldások vannak a kibertámadás ellen.
   - Ismeri a kibertámadás esetén alkalmazandó eljárásokat.
   - Tisztában van az állami kibervédelmi rendszerrel.
   - Megérti a szervezeti feladatokat a kibervédelemben.

   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.

Attitűdje:

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

- 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 cyberattacks.
- He/She is familiar with procedures applicable in case of a cyberattack.
- He/She is familiar with the cyber security system of the state.
- He/She is familiar with organisational tasks in cybersecurity.

Capabilities:

- He/She is capable of understanding the current threats of cyberspace.
- He/She is capable of supporting his/her organisation in developing cybersecurity skills.
- He/She is capable of supporting his/her organisation and external parties in handling a cyberattack.

Attitude:

- His/Her personal attitude is characterized by an attention to and application of laws of cybersecurity in his/her work.
- His/Her personal attitude is characterized by an effort to take effective measures in order to prevent cyberattacks, by this means reducing the exposure of his/her organisation.

Autonomy and responsibility:

- His/Her autonomy and responsibility are to handle cyber security threats.

10. Előtanulmányi követelmények: -

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

11.1. Az incidenskezelés elmélete.
11.2. Az incidenskezelés jogi háttere.
11.3. Az incidenskezelés szervezeti háttere Magyarországon és a nemzetközi térben, CERT/CSIRT szervezetek.
11.4. A Biztonsági Műveleti Központok.
11.5. Az incidenskezelés műszaki eszköztára.
11.6. Incidenssel kapcsolatos információk megosztása.
11.7. Üzletmenet-folytonosság tervezése.
11.8. Esemény, probléma, incidens fogalmának meghatározása, gyakorlati példák bemutatása.
11.9. Incidens esettanulmányok.
11.10. Incidenskezelő csapat létrehozása.
11.11. Az incidenskezelés folyamata a gyakorlatban.

11.1. Theory of incident management.
11.2. Legal background of incident management.
11.3. Organizational background of incident management in Hungary and internationally, CERT/CSIRT).
11.4. Security Operation Centers.
11.5. Technical tools of incident management.

11.6. Incident information sharing.
11.7. Business continuity planning.
11.8. Definition of security event, problem and incident, practical examples.
11.9. Incident related case studies.
11.10. Setup of an incident management team.
11.11. Incident management in practice.

12. A tantárgy meghirdetésének gyakorisága/a tantervben történő félévi elhelyezkedése: II. félév

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

Követelmény a tanórákon történő részvétel. A hallgató köteles a foglalkozások legalább 75%-án részt venni. Az elfogadható hiányzások mértéke 25%, az e feletti távolmaradás esetén a tantárgy oktatója által meghatározott feladatot szükséges teljesíteni.

14. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A hallgató értékelése a szorgalmi időszakban egy zárthelyi dolgozat sikeres teljesítése alapján történik, amelynek követelménye a foglalkozásokon elhangzott ismeretanyag.

Az értékelés ötfokozatú: elégtelen (60% alatt), elégséges (61%-70%), közepes (71%-80%), jó (81%-90%), jeles (91%-100%). Pótlás, illetve 61% alatti eredmény esetén, javítási lehetőséget kell biztosítani a szorgalmi időszakban, egy alkalommal.

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

15.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele a 13. pontban meghatározott arányú részvétel a foglalkozásokon, valamint a 14. pontban meghatározott félévközi feladat legalább elégséges teljesítése.

15.2. Az értékelés:

A félév végi számonkérés módja és formája: kollokvium, írásbeli vizsga, amelynek során egy elképzelt kiberbiztonsági incidens különböző szempontú megoldására kell javaslatot tennie a vizsgázónak, felhasználva az elméleti és gyakorlati foglalkozásokon elsajátított ismereteket.

15.3. A kreditek megszerzésének feltételei:

A kreditek megszerzésének feltétele az aláírás megszerzése és a legalább elégséges vizsgajegy.

16. Irodalomjegyzék:

16.1. Kötelező irodalom:

- Berzsenyi Dániel – Zámbó Nóra: *Incidensmenedzsment. Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára 2017.* Dialóg Campus Kiadó, Budapest, 2019. ISBN: 978 615 576 499 8

16.2. Ajánlott irodalom:

- Luttgens, Jason - Pepe, Matthew - Mandia, Kevin: *Incident Response & Computer Forensics, Third Edition.* McGraw-Hill Education, 2014. ISBN-13: 978 007 179 868 6
- Thomas, Arun E.: *Security Operations Center - SIEM Use Cases and Cyber Threat Intelligence.* CreateSpace Independent Publishing Platform, 2018. ISBN-13: 978 198 686 201 1

Budapest, 2021. március 1.

Dr. Krasznay Csaba sk.
egyetemi docens, NKE ÁNTK

10. TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** KVTIS734
2. **A tantárgy megnevezése (magyarul):** Biztonsági tesztelés
3. **A tantárgy megnevezése (angolul):** Security Testing
4. **Kreditérték és képzési karakter:**
   4.1. 4 kredit
   4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 100% gyakorlat, 0% elmélet
5. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** NKE KTI
6. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Tóth András, egyetemi docens, NKE HHK
7. **A tanórák száma és típusa:**
   7.1. összes óraszám/félév: 15 óra
   7.2. levelező munkarend: 15 óra (0 EA + 0 SZ + 15 GY (vagy 15 óra online gyakorlat, amennyiben az évfolyam létszáma indokolja))
8. **A tantárgy szakmai tartalma (magyarul):**

   A tantárgy célja az informatikai rendszerek biztonsági tesztelése tervezésének, végrehajtásának és a vizsgálatok dokumentálásának ismertetése a hallgatókkal. 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 módszerei), 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 vezeték nélküli 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, e-learning 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. 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, e-learning materials, certificates, CTFs, cyber security exercises).

9. 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:

- He/She is familiar with the procedures applicable in case of a cyberattack.

Capabilities:

- He/She 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 cyberattacks, by this means reducing the exposure of his/her organisation.

Autonomy and responsibility:

- His/Her autonomy and responsibility are to put the results of scientific research in the field into his/her practice.

10. Előtanulmányi követelmények: -

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

11.1. Biztonsági tesztlabor tervezésének és kialakításának lépései.
11.2. IT rendszerek biztonsági tesztelésének különböző módszertanai.
11.3. Biztonságtesztelő módszerek fő típusai.
11.4. Biztonsági eszközök vizsgálatának lehetőségei.
11.5. Biztonsági funkcionális tesztelés.
11.6. Sérülékenység-vizsgálat.
11.7. Behatolás tesztelés.
11.8. Helyi és távoli sérülékenység keresés és kihasználás.
11.9. Alkalmazások és szolgáltatások tesztelésének lehetőségei.
11.10. Webszolgáltatások és adatbázisok biztonsági tesztelése.
11.11. Felhasználói biztonságtudatossági vizsgálatok.

11.12. Vezeték nélküli rendszerek tesztelésének módszertana.
11.13. Mobil eszközök (okos eszközök) tesztelésének lehetőségei.
11.14. Beágyazott rendszerek vizsgálatának lehetőségei.
11.15. Továbbképzés és önképzés egyéni és csoportos lehetőségei.

11.1. Steps to design and build a security test laboratory.
11.2. Different methodologies for security testing of IT systems.
11.3. Main types of security testing methods.
11.4. Possibilities for testing security devices.
11.5. Security functional testing.
11.6. Vulnerability assessment.
11.7. Penetration testing.
11.8. Local and remote vulnerability scanning and exploitation.
11.9. Possibilities for testing applications and services.
11.10. Security testing of web services and databases.
11.11. Social engineering tests.
11.12. Methodology of wireless testing.
11.13. Mobile (smart) device testing.
11.14. Possibilities of embedded systems' security testing.
11.15. Possibilities of self and group learning.

12. A tantárgy meghirdetésének gyakorisága/a tantervben történő félévi elhelyezkedése: II. félév

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

Követelmény a tanórákon történő részvétel. A hallgató köteles a foglalkozások legalább 75%-án részt venni. Az elfogadható hiányzások mértéke 25%, az e feletti távolmaradás esetén a tantárgy oktatója által meghatározott feladatot szükséges teljesíteni.

14. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A hallgató értékelése a szorgalmi időszakban az oktató által adott, a 11. pontban meghatározott témakörökhöz köthető gyakorlati feladat megoldása alapján történik.

Az értékelés ötfokozatú: elégtelen (60% alatt), elégséges (61%-70%), közepes (71%-80%), jó (81%-90%), jeles (91%-100%). Pótlás, illetve 61% alatti eredmény esetén, javítási lehetőséget kell biztosítani a szorgalmi időszakban, egy alkalommal.

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

15.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele a 13. pontban meghatározott arányú részvétel a foglalkozásokon, valamint a 14. pontban meghatározott félévközi feladat legalább elégséges teljesítése.

15.2. Az értékelés:

A félévközi számonkérés módja és formája: gyakorlati jegy, amely az oktató által adott gyakorlati feladat sikeres teljesítéséből, valamint az órai teljesítmény értékeléséből áll (50-50%-os arányban).

15.3. A kreditek megszerzésének feltételei:

A kreditek megszerzésének feltétele az aláírás megszerzése és a legalább elégséges félévközi jegy.

16. Irodalomjegyzék:

16.1. Kötelező irodalom:

- Frész Ferenc - Kálovics Tamás - Puha Gábor: *Hálózatok Biztonsága.* NKE, Budapest, 2014., egyetemi jegyzet
- Tihanyi Norbert - Vargha Gergely - Frész Ferenc: *Biztonsági tesztelés a gyakorlatban.* NKE, Budapest, 2014. ISBN: 978 615 549 159 7

- Open Source Security Testing Methodology Manual – OSSTMM, Online elérése: http://www.isecom.org/mirror/OSSTMM.3.pdf.

16.2. Ajánlott irodalom:

- Hertzog, Raphael - O'Gorman, Jim: *Kali Linux Revealed: Mastering the Penetration Testing Distribution.* Offsec Press, 2017. ISBN-13: 978 099 761 560 9
- Kim, Peter: *The Hacker Playbook 3: Practical Guide To Penetration Testing.* Independently, 2018. ISBN-13: 978 198 090 175 4
- OWASP ajánlás, online elérése:https://www.owasp.org/images/1/19/OTGv4.pdf
- RTFM - Red Team Field Manual, online elérése:https://github.com/droberson/rtfm
- Sérülékenység keresési link gyűjtemények: https://github.com/enaqx/awesome-pentest, és http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html

Budapest, 2021. március 1.

Dr. Tóth András sk.
egyetemi docens, NKE HHK

11. TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** KVTIS735
2. **A tantárgy megnevezése (magyarul):** Információbiztonsági stratégia és vezetés
3. **A tantárgy megnevezése (angolul):** Information Security Strategy and Leadership
4. **Kreditérték és képzési karakter:**
   4.1. 6 kredit
   4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 60% gyakorlat, 40% elmélet
5. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** NKE KTI
6. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Bányász Péter, adjunktus, NKE ÁNTK
7. **A tanórák száma és típusa:**
   7.1. összes óraszám/félév: 25 óra
   7.2. levelező munkarend: 25 óra (10 EA (vagy 10 óra online előadás, amennyiben az évfolyam létszáma indokolja)+ 0 SZ + 15 GY (vagy 15 óra online gyakorlat, amennyiben az évfolyam létszáma indokolja))
8. **A tantárgy szakmai tartalma (magyarul):**

   A tantárgy célja az információbiztonsági stratégia kialakítása és megvalósítása lépéseinek bemutatása, a monitorozási és riportolási lehetőségek vizsgálata, valamint a biztonságtudatossági alapok megteremtése a szervezeten belül. Az információbiztonsági stratégia kialakítása során a biztonságtudatosság fejlesztésének példáján keresztül ismerik meg a hallgatók a gyakorlati alkalmazás módját. A tantárgy teljesítésével a hallgatók képesek lesznek az információbiztonsági stratégia kialakítására és nyomon követésére, valamint biztonságtudatossági program menedzselésére.

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

   The aim of the course is to introduce the steps of designing and implementing an information security strategy, discuss monitoring and reporting opportunities, and establish security awareness basics within the organization. During the development of the information security strategy, students will learn how to apply it in practice through the example of developing security awareness. By completing the course, students will be able to develop and monitor an information security strategy and manage a security awareness program.
9. **Elérendő kompetenciák (magyarul):**

   Tudása:

   - Átlátja a munkáltatók által meghatározott belső szabályzatok megalkotásának szükségességét az információs rendszerekben tárolt adatok sértetlensége és a rendelkezésre állás tekintetében.
   - Tisztában van az emberi tényező szerepével a kibertámadások kivitelezése során.

   Képességei:

   - Képes megszerezni a szervezet vezetőinek támogatását a jogszabályi megfelelőség kiépítéséhez.
   - Képes olyan védelmi intézkedések meghozatalára, amelyek segítik a humán fenyegetettségből eredő kockázatok csökkentését.
   - Képes felmérni a belső munkavállalók jelentette kiberbiztonsági kockázatokat.

   Attitűdje:

   - A maga komplexitásában tervezi meg az információbiztonsági irányítási rendszert.

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

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:

- 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 the role of human factors in the execution of cyberattacks.

Capabilities:

- He/She is capable of obtaining the support of leaders of the organisation in establishing regulatory compliance.
- He/She is capable of taking defensive measures that ensure the reduction of risk resulting from threat against humans.
- He/She is capable of assessing cybersecurity risk posed by internal employees.

Attitude:

- 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 ability to treat internal employees as high risk and plans information security processes accordingly.

Autonomy and responsibility:

- His/Her autonomy and responsibility are to take responsibility for making professional proposals based on comprehensive knowledge of cyber security and dominant legal, regulatory and economical processes.

10. Előtanulmányi követelmények: -

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

11.1. Információbiztonsági irányítási rendszer alapjai.
11.2. Információbiztonsági stratégia készítése – biztonságtudatossági példával szemléltetve.
11.3. Az információbiztonsági stratégia megvalósítása, módosítása.
11.4. Visszamérés – biztonságtudatossági példával szemléltetve.
11.5. Biztonságtudatossági alapok.
11.6. A biztonságtudatosság fejlesztésének lehetőségei.

11.1. Foundations of the Information Security Management System.
11.2. Creating an Information Security Strategy - Illustrated by an example of security awareness.
11.3. Implementation and modification of the information security strategy.
11.4. Feedback - illustrated with an example of security awareness.
11.5. Security Awareness Basics.
11.6. Opportunities for developing security awareness.

12. A tantárgy meghirdetésének gyakorisága/a tantervben történő félévi elhelyezkedése: II. félév

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

Követelmény a tanórákon történő részvétel. A hallgató köteles a foglalkozások legalább

75%-án részt venni. Az elfogadható hiányzások mértéke 25%, az e feletti távolmaradás esetén a tantárgy oktatója által meghatározott feladatot szükséges teljesíteni.

14. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A hallgató értékelése a szorgalmi időszakban az oktató által adott, a 11. pontban meghatározott témakörökhöz köthető gyakorlati feladatokban történő részvétel alapján zajlik.

Az értékelés ötfokozatú: elégtelen (60% alatt), elégséges (61%-70%), közepes (71%-80%), jó (81%-90%), jeles (91%-100%). Pótlás, illetve 61% alatti eredmény esetén, javítási lehetőséget kell biztosítani a szorgalmi időszakban, egy alkalommal, az oktató által megadott témában írt beadandó formájában.

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

15.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele a 13. pontban meghatározott arányú részvétel a foglalkozásokon, valamint a 14. pontban meghatározott félévközi feladat legalább elégséges teljesítése.

15.2. Az értékelés:

A félévközi számonkérés módja és formája: gyakorlati jegy, amely az oktató által meghatározott gyakorlati feladat sikeres teljesítéséből, valamint az órai teljesítmény értékeléséből áll (50-50%-os arányban).

15.3. A kreditek megszerzésének feltételei:

A kreditek megszerzésének feltétele az aláírás megszerzése és a legalább elégséges félévközi jegy.

16. Irodalomjegyzék:

16.1. Kötelező irodalom:

- Oroszi Eszter Diána (2014): *Információbiztonsági stratégia és vezetés.* NKE, Budapest, 2014., egyetemi jegyzet

16.2. Ajánlott irodalom:

- ISACA: *CISM Review Manual, 15th Edition.* 2016. ISBN-13: 978 160 420 508 4

Budapest, 2021. március 1.

Dr. Bányász Péter sk.
adjunktus, NKE ÁNTK

12. TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** KVTIS736
2. **A tantárgy megnevezése (magyarul):** Kiberbiztonsági szabályozás Európában
3. **A tantárgy megnevezése (angolul):** Cybersecurity Legislation in Europe
4. **Kreditérték és képzési karakter:**
   4.1. 6 kredit
   4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 0% gyakorlat, 100% elmélet
5. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** NKE KTI
6. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Gyaraki Réka Eszter, tanársegéd, NKE RTK
7. **A tanórák száma és típusa:**
   7.1. összes óraszám/félév: 25 óra
   7.2. levelező munkarend: 25 óra (25 EA (vagy 25 óra online előadás, amennyiben az évfolyam létszáma indokolja)+ 0 SZ + 0 GY)
8. **A tantárgy szakmai tartalma (magyarul):**

   A tantárgy a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló EU irányelv rendelkezéseire, tagállami kötelezettségeire és azok megvalósítási lehetőségeire fókuszál. Az ismeretanyag kiterjed az Irányelv kialakításához vezető mérföldkövek bemutatására a kétezres évek elejétől kezdve napjainkig. Tartalmazza továbbá az Irányelvhez közvetlenül vagy közvetetten kapcsolódó egyéb EU norma bemutatását. Bemutatja továbbá az EU Kiberbiztonsági Jogszabályának (Cybersecurity Act) követelményeit, kiemelve a kiberbiztonsági tanúsításra vonatkozó részleteket.

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

   The course focuses on the provisions of the EU Directive on measures for a high common level of security of network and information systems across the Union, on the obligations of Member States and on how to implement them. It covers milestones which led to the development of the Directive from the early 2000s to present days. It also includes a description of other EU norms that are directly or indirectly related to the Directive. It introduces the requirements of EU Cybersecurity Act, highlighting the details in connection with cybersecurity certification.

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

   Tudása:

   - Ismeri azokat a fontosabb előírásokat a szabályozásokból, amelyek a mindennapi munkáját befolyásolják.
   - Ismeri a létfontosságú rendszerelemek fogalmát.
   - Tisztában van az állami kibervédelmi rendszerrel.

   Képességei:

   - Képes értelmezni a jogszabályokból eredő követelményeket.
   - Képes megszerezni a szervezet vezetőinek támogatását a jogszabályi megfelelőség kiépítéséhez.
   - Képes támogatni szervezetét a kibervédelmi képességek kialakításában.

   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.
- Vállalja a szakterület, a szakmai praxis módszertanának fejlesztéséhez szükséges elméleti, tudományos kutatási és gyakorlati információk beszerzésének, értékelésének és hasznosításának végrehajtását.
- Felelősséget vállal a kiberbiztonság összefüggő ismeretének és a meghatározó jogi, szabályozási és gazdasági összefüggések ismeretének alapján a szakmai javaslatok kidolgozásában.
- Gyakorlatába beépíti és alkalmazza az e szakterületen folyó kutatások eredményeit.

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 concept of critical infrastructure protection.
- He/She is familiar with the cybersecurity system of the state.

Capabilities:

- He/She is capable of interpreting legal requirements.
- He/She is capable of obtaining the support of leaders of the organisation in establishing regulatory compliance.
- He/She is capable of supporting his/her organisation in developing cyber security skills.

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:

- His/Her autonomy and responsibility are to implement advanced knowledge characterising cyber security on a national and international level.
- His/Her 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.
- His/Her autonomy and responsibility are to take responsibility for making professional proposals based on comprehensive knowledge of cyber security and dominant legal, regulatory and economical processes.
- His/Her autonomy and responsibility are to put the results of scientific research in the field into his/her practice.

10. Előtanulmányi követelmények: -

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

11.1. Európai Uniós törekvések a XX. században a biztonság erősítésére.
11.2. Az ENISA szerepe az EU-ban.
11.3. Kritikus információs infrastruktúra védelem.
11.4. A NIS irányelv.
11.5. Kiberbiztonsági jogszabály.
11.6. Kiberbiztonsági tanúsítások.

11.1. Intentions in the EU for strengthening security in the 20th Century.
11.2. The role of ENISA in the EU.
11.3. Critical Information Infrastructure Protection.
11.4. The NIS Directive.
11.5. Cybersecurity Act.
11.6. Cybersecurity certifications.

12. A tantárgy meghirdetésének gyakorisága/a tantervben történő félévi elhelyezkedése: II. félév

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

Követelmény a tanórákon történő részvétel. A hallgató köteles a foglalkozások legalább 75%-án részt venni. Az elfogadható hiányzások mértéke 25%, az e feletti távolmaradás esetén a tantárgy oktatója által meghatározott feladatot szükséges teljesíteni.

14. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A hallgató értékelése a szorgalmi időszak során egy zárthelyi dolgozat sikeres teljesítése alapján történik, amelynek követelménye a foglalkozásokon elhangzott ismeretanyag.

Az értékelés ötfokozatú: elégtelen (60% alatt), elégséges (61%-70%), közepes (71%-80%), jó (81%-90%), jeles (91%-100%). Pótlás, illetve 61% alatti eredmény esetén, javítási lehetőséget kell biztosítani a szorgalmi időszakban, egy alkalommal. A zárthelyi dolgozattal elért 90% feletti eredmény esetén a tantárgy megajánlott jeggyel teljesíthető.

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

15.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele a 13. pontban meghatározott arányú részvétel a foglalkozásokon, valamint a 14. pontban meghatározott félévközi feladat legalább elégséges teljesítése.

15.2. Az értékelés:

A félév végi számonkérés módja és formája: kollokvium, írásbeli vizsga, amelynek során a kötelező irodalom és a foglalkozások anyagának ismerete a követelmény.

15.3. A kreditek megszerzésének feltételei:

A kreditek megszerzésének feltétele az aláírás megszerzése és a legalább elégséges vizsgajegy.

16. Irodalomjegyzék:

16.1. Kötelező irodalom:

- 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 – 2019.* NKE, Budapest, 2019. ISBN: 978 963 498 240 1

16.2. Ajánlott irodalom:

- Bognár Balázs - Bonnyai Tünde - Vámosi Zoltán: *Kritikus infrastruktúrák védelme I.* Dialóg Campus Kiadó, Budapest, 2019. ISBN: 978 615 592 036 3 (nyomtatott), ISBN: 978 615 594 528 1 (elektronikus)

Budapest, 2021. március 1.

Dr. Gyaraki Réka Eszter sk.
tanársegéd, NKE RTK

13. TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** KVTIS737
2. **A tantárgy megnevezése (magyarul):** Válságmenedzsment és kommunikáció
3. **A tantárgy megnevezése (angolul):** Crisis Management and Communication
4. **Kreditérték és képzési karakter:**
   4.1. 4 kredit
   4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 100% gyakorlat, 0% elmélet
5. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** NKE KTI
6. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Kriskó Edina, adjunktus, NKE ÁNTK
7. **A tanórák száma és típusa:**
   7.1. összes óraszám/félév: 15 óra
   7.2. levelező munkarend: 15 óra (0 EA + 0 SZ + 15 GY (vagy 15 óra online gyakorlat, amennyiben az évfolyam létszáma indokolja))
8. **A tantárgy szakmai tartalma (magyarul):**

   A tárgy célja a hallgatók felkészítése különböző szintű, méretű, típusú válságok felismerésére és elemzésére, az okok beazonosítására, a következmények felmérésére, a válságra figyelmeztető jelzőrendszerek működési mechanizmusainak átlátására. A kurzus során a hallgatók megismerkednek az adekvát kommunikációs stratégiának a válságok megelőzésében betöltött szerepével, eszközeivel, az esetleges krízisre felkészítő, szakszerűen megtervezett kommunikáció forgatókönyvével, illetve a már kialakult válság kezelésére szolgáló, a pánikot megelőző kommunikáció professzionális megtervezésének lehetőségével, eszköztárával, a válságkommunikáció szabályaival.

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

   The aim of the course is to prepare students to recognize and analyze crises of different levels, sizes, types, identify causes, assess consequences, and understand the mechanisms of crisis alert systems. During the course students will be introduced to the role and tools of an adequate communication strategy in crisis prevention, the scenario of professionally prepared communication in preparation for a possible crisis, and the possibility of professionally planning the planning of pre-panic communication and management of an existing crisis.
9. **Elérendő kompetenciák (magyarul):**

   Tudása:

   - Megérti a szervezeti feladatokat a kibervédelemben.

   Képességei:

   - Képes támogatni szervezetét a kibervédelmi képességek kialakításában.
   - Képes megfelelően támogatni szervezetét és a külső feleket egy kibertámadás kezelésében.

   Attitűdje:

   - A maga komplexitásában tervezi meg az információbiztonsági irányítási rendszert.
   - Partner abban, hogy se a szervezete, se ő maga ne váljon kibertámadás áldozatává.

   Autonómiája és felelőssége:

   - 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.
- Vállalja a kiberbiztonsági fenyegetések kezelésének felelősségét.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge:

- He/She is familiar with organisational tasks in cyber security.

Capabilities:

- He/She is capable of supporting his/her organisation in developing cyber security skills.
- He/She is capable of supporting his/her organisation and external parties in handling a cyberattack.

Attitude:

- 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 cooperation in preventing his/her organisation and him/herself from becoming a victim of a cyberattack.

Autonomy and responsibility:

- His/Her autonomy and responsibility are to initiate and introduce alternative and original solutions and appropriate decision making in complex, atypical contexts.
- His/Her autonomy and responsibility are to take part in providing technological, political and administrative solutions to cyber threats.
- His/Her autonomy and responsibility are to handle cyber security threats.

10. Előtanulmányi követelmények: -

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

11.1. A válságkommunikáció kompetenciaterülete, elméleti háttere, alapelvei.
11.2. A kiberincidensek, a közvélemény és a média.
11.3. A kiberbiztonság téma kommunikációjának kontextusa (nemzeti, ágazati és szervezeti sajátosságok, kiber témák a közigazgatásban és a politikai kommunikációban).
11.4. A preventív kommunikáció jelentősége és lehetőségei.
11.5. Kommunikáció a kiberválságok aktív szakaszában, retorikai és esemény-közzétételi stratégiák.
11.6. A helyreállítás folyamatainak és eredményeinek kommunikációja.
11.7. A kommunikáció tervezésének szempontjai speciális területeken.
11.8. Esettanulmányok.

11.1. The competence of crisis communication, the theoretical background and principles.
11.2. Cyber incidents, the public opinion and the media.
11.3. The context of communication on the topic of cyber security (national, sectoral and organizational characteristic, cyber security issues in public administration and in the politics).
11.4. The importance and possibilities of preventive communication (pre crisis communication).
11.5. Responding, rhetorical and incidents-disclosure strategies.
11.6. Communication on processes and results of the recovery.
11.7. Aspects of communication planning.
11.8. Case studies.

12. A tantárgy meghirdetésének gyakorisága/a tantervben történő félévi elhelyezkedése: II. félév

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

Követelmény a tanórákon történő részvétel. A hallgató köteles a foglalkozások legalább 75%-án részt venni. Az elfogadható hiányzások mértéke 25%, az e feletti távolmaradás esetén a tantárgy oktatója által meghatározott feladatot szükséges teljesíteni.

14. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A hallgató értékelése a szorgalmi időszakban a 11. pontban meghatározott témakörökhöz köthető, 10-12.000 karaktert tartalmazó házi dolgozat elkészítése alapján történik. A dolgozatokat legkésőbb a szorgalmi időszak végét megelőző 7. napon szükséges leadni.

Az értékelés ötfokozatú: elégtelen (60% alatt), elégséges (61%-70%), közepes (71%-80%), jó (81%-90%), jeles (91%-100%). Pótlás, illetve 61% alatti eredmény esetén, javítási lehetőséget kell biztosítani a szorgalmi időszakban, egy alkalommal, szóbeli beszámoló formájában.

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

15.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele a 13. pontban meghatározott arányú részvétel a foglalkozásokon, valamint a 14. pontban meghatározott félévközi feladat legalább elégséges teljesítése.

15.2. Az értékelés:

A félévközi számonkérés módja és formája: gyakorlati jegy, amely a félévközi feladat sikeres teljesítéséből, valamint az órai teljesítmény értékeléséből áll (50-50%-os arányban).

15.3. A kreditek megszerzésének feltételei:

A kreditek megszerzésének feltétele az aláírás megszerzése és a legalább elégséges félévközi jegy.

16. Irodalomjegyzék:

16.1. Kötelező irodalom:

- 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 – 2019.* NKE, Budapest, 2019. ISBN: 978 963 498 240 1
- Anthonissen, Peter Frans: *Kríziskommunikáció. A válságkezelés és reputációmenedzsment PR-stratégiái.* HVG Könyvek, Budapest, 2009. ISBN 978 963 968 691 5

16.2. Ajánlott irodalom:

- Coombs, Timothy W.: *Ongoing Crisis Communication. Planning, Managing and Responding.* SAGE, Thausend Oaks, California, 2012. ISBN-13: 978 141 298 310 5
- Kulikova, Olga – Heil, Ronald – Berg, Jan van den – Pieters, Wolter: 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
- Lange-Ionatamishvili, Elina – Sveotka, Sanda: *Strategic Communications and Social Media in the Russia Ukraine Conflict.* In: Kenneth Geers (Ed.): *Cyber War in Perspective: Russian Aggression against Ukraine, NATO CCD COE Publications*. CCDCOE, Tallinn, 2015. 103–111. o.

Budapest, 2021. március 1.

Dr. Kriskó Edina sk.
adjunktus, NKE ÁNTK

14. TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** KVTIS647
2. **A tantárgy megnevezése (magyarul):** Információs rendszerek és hálózatok biztonsága 2.
3. **A tantárgy megnevezése (angolul):** Security of Information Systems and Networks 2.
4. **Kreditérték és képzési karakter:**
   4.1. 4 kredit
   4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 0% gyakorlat, 100% elmélet
5. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** NKE KTI
6. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Farkas Tibor, egyetemi docens, NKE HHK
7. **A tanórák száma és típusa:**
   7.1. összes óraszám/félév: 20 óra
   7.2. levelező munkarend: 20 óra (20 EA (vagy 20 óra online előadás, amennyiben az évfolyam létszáma indokolja)+ 0 SZ + 0 GY)
8. **A tantárgy szakmai tartalma (magyarul):**

   A kurzus célja 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 vezeték nélküli hálózatok működése vizsgálatának, az Ethernet szabványok összehasonlító mérésének, a hálózati eszközök (HUB, switch, router, tűzfal, proxy) működésének protokoll analizátor segítségével végzett vizsgálatának, a hálózati eszközök terheléses vizsgálatának és a hálózati eszközök funkcionális vizsgálatának lehetőségeinek megismerése. IP forgalom titkosítási lehetőségeinek (hálózati, szállítási, alkalmazás rétegbeli lehetőségek) bemutatása. Tűzfalak típusainak és funkcióinak gyakorlati vizsgálata. Végponti és hálózati támadások, különös tekintettel a kártékony kódokra.

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

   Aim of this course is to 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. Endpoint and network attacks, with a special focus on malware.
9. **Elérendő kompetenciák (magyarul):**

   Tudása:

   - Átlátja, hogy milyen védelmi megoldások vannak a kibertámadás ellen.
   - Ismeri a kártékony kódok fogalmát és hatásmechanizmusát.

   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:

- 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:

- He/She is familiar with defence solutions against cyberattacks.
- He/She is familiar with the concept and mode of action of malware codes.

Capabilities:

- He/She is capable of taking technological defensive measures related to elements of the cyber kill chain.
- He/She 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 cyberattacks, by this means reducing the exposure of his/her organisation.

Autonomy and responsibility:

- His/Her autonomy and responsibility are to take part in providing technological, political and administrative solutions to cyber threats.
- His/Her autonomy and responsibility are to take the initiative to convert technical and operative tasks into strategic targets.

10. Előtanulmányi követelmények: -

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

11.1. Hálózati diagnosztika, a hitelesítési és titkosítási protokollok alapjai.
11.2. A hálózat monitorozása, hálózati hibaelhárítás.
11.3. Tűzfalak típusainak és funkcióinak gyakorlati vizsgálata.
11.4. Végponti és hálózati támadások.
11.5. Kártékony kódok.
11.6. Informatikai rendszerek felépítése, komplexitása.
11.7. Nem PC alapú rendszerek specifikumai (mobileszközök, ipari vezérlés, IoT).

11.1. Network diagnostics, basics of authentication and encryption protocols.
11.2. Network monitoring, network troubleshooting.
11.3. Practical study of firewall types and functions.
11.4. Endpoint and network attacks.
11.5. Malicious codes.
11.6. Structure and complexity of IT systems.
11.7. Specifications for non-PC based systems (mobile devices, industrial control, IoT).

12. A tantárgy meghirdetésének gyakorisága/a tantervben történő félévi elhelyezkedése: II. félév

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

Követelmény a tanórákon történő részvétel. A hallgató köteles a foglalkozások legalább

75%-án részt venni. Az elfogadható hiányzások mértéke 25%, az e feletti távolmaradás esetén a tantárgy oktatója által meghatározott feladatot szükséges teljesíteni.

14. Félévközi feladatok, ismeretek ellenőrzésének rendje: -

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

15.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele a 13. pontban meghatározott arányú részvétel a foglalkozásokon.

15.2. Az értékelés:

A félév végi számonkérés módja és formája: kollokvium, írásbeli vizsga, amelynek során a kötelező irodalom és a foglalkozások anyagának ismerete a követelmény.

15.3. A kreditek megszerzésének feltételei:

A kreditek megszerzésének feltétele az aláírás megszerzése és a legalább elégséges vizsgajegy.

16. Irodalomjegyzék:

16.1. Kötelező irodalom:

- Tanenbaum, Andrew S. – Wetherall, David J.: *Számítógép-hálózatok*. Panem Kft., Budapest, 2013. ISBN: 978 963 545 529 4
- Tanenbaum, Andrew S.: *Számítógép-architektúrák*. Panem Kft., Budapest, 2007. ISBN: 978 963 545 457 0
- Petrényi József: *TCP/IP – alapok I. és II. kötet.* 2009. http://mek.oszk.hu/08300/08374/
- Dr. Kónya László: *Számítógép-hálózatok.* LSI Oktatóközpont, Budaoest. ISBN: 963 577 22 X
- Kurose, James F. – Ross, Keith W.: *Számítógép-hálózatok működése*. Panem Kft., Budapest, 2009. ISBN 978 963 545 498 3

16.2. Ajánlott irodalom:

- Brown, Lawrie - Stallings, William: *Computer Security: Principles and Practice, Pearson*. Pearson, 2018. (4. kiadás). ISBN-13: 978 013 479 410 5
- Borbély Balázs: *Otthoni és irodai hálózatok zsebkönyve.* Jedlik Oktatási Stúdió, Budapest, 2018. ISBN: 978 615 501 231 0
- Casad, Joe: *Tanuljuk meg a TCP/IP használatát 24 óra alatt*. Kiskapu Kiadó, Budapest, 2010. ISBN: 978 963 963 768 9
- Rusen, Ciprian Adrian: *Számítógépes eszközök hálózatba kötése - Lépésről lépésre.* Szak Kiadó, Budapest, 2011. ISBN: 978 963 986 321 7
- Gál Tamás - Szabó Levente - Szerényi László: *Rendszerfelügyelet rendszergazdáknak*. Szak Kiadó, Budapest, 2007. ISBN 978 963 913 198 9

Budapest, 2021. március 1.

Dr. Farkas Tibor sk.
egyetemi docens, NKE HHK