Nemzeti Közszolgálati Egyetem
Közigazgatási Továbbképzési Intézet

Elektronikus információbiztonsági vezető szakirányú továbbképzési szak

Szakfelelős: Dr. Bányász Péter

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

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

4. A képzési idő félévekben meghatározva: 2 félév

5. A szakképzettség megszerzéséhez összegyűjtendő kreditek száma: 60 kredit

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

6.1. A képzés célja:
A képzés fő célja a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvényben meghatározott elektronikus információs rendszer biztonságáért felelős személyek feladatellátásához szükséges szakmai kompetenciák átadása és a biztonságtudatos szemléletmód kialakítása.

6.2. A szakmai kompetenciák:

A szakképzettség megnevezése: elektronikus információbiztonsági vezető

6.2.1. Tudás
- 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.

6.2.2. Képesség

- 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.

6.2.3. Attitűd

- 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.

6.2.4. Autonómia és felelősség

- 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.

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

7.1. Államtudományi, jogi és közigazgatás-szervezési ismeretek - 10-15 kredit,

7.2. Információbiztonsági és biztonságszervezési ismeretek - 25-35 kredit,

7.3. Alkalmazott infokommunikációs szakismeretek - 10-20 kredit

ELEKTRONIKUS INFORMÁCIÓBIZTONSÁGI VEZETŐ SZAKIRÁNYÚ TOVÁBBKÉPZÉSI SZAK AJÁNLOTT TANTERVE

Alkalmazandó:
a 2025/2026. tanévtől felmenő rendszerben

Budapest, 2025 július

Tartalomjegyzék

Tartalomjegyzék

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:

3.4. képzési terület szerinti besorolása: államtudományi képzési terület

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

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

4. A képzési idő félévekben meghatározva: 2 félév

5. A szakképzettség megszerzéséhez összegyűjtendő kreditek száma: 60 kredit

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

6.1. A képzés célja:
A képzés fő célja a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvényben meghatározott elektronikus információs rendszer biztonságáért felelős személyek feladatellátásához szükséges szakmai kompetenciák átadása és a biztonságtudatos szemléletmód kialakítása.

6.2. A szakmai kompetenciák:

A szakképzettség megnevezése: elektronikus információbiztonsági vezető

6.2.1. Tudás
- 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.

6.2.2. Képesség

- 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.

6.2.3. Attitűd

- 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.

6.2.4. Autonómia és felelősség

- 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.

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

7.4. Államtudományi, jogi és közigazgatás-szervezési ismeretek - 10-15 kredit,

7.5. Információbiztonsági és biztonságszervezési ismeretek - 25-35 kredit,

7.6. Alkalmazott infokommunikációs szakismeretek - 10-20 kredit

8. A képzés időtényezői
A képzési idő félévekben: 2 félév

A képzési idő részletezése:

A fokozat megszerzéséhez összegyűjtendő kreditek száma	60 kredit
Összes hallgatói tanulmányi munkaóra	285
Hallgatói munkamennyiség kreditben egy tanulmányi félévben:	átlagosan 30 kredit
Egy tanulmányi félévben a tanórák száma levelező munkarendben	átlagosan 140 tanóra

6. A képzés felépítése

6.1. a szakképzettséghez vezető tudományágak, szakterületek, amelyekből 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,

6.2. a szakdolgozat készítéséhez rendelt kreditérték: 0 kredit
6.3. a szabadon választható tantárgyakhoz rendelhető minimális kreditérték: 0 kredit

7. A tanóra-, kredit- és vizsgaterv
A tanóra-, kredit- és vizsgaterv tartalmazza oktatási időszakonkénti bontásban az összes tantárgy vonatkozásában

a) a tantárgyak Neptun-kódját,
b) a tantárgyak jellegét (kötelező, kötelezően választható, szabadon választható),
c) a meghirdetés féléveit,
d) a tantárgyak heti és félévi vagy félévi óraszámát a tanóra típusa szerinti bontásban,
e) a tantárgyakhoz rendelt krediteket,
f) a hallgatói teljesítmény értékelésének módját (számonkérés);
g) a tantárgyfelelős szervezeti egységet és a tantárgyfelelős személyét.

A tanóratípusok rövidítései:

- előadás: EA
- szeminárium: SZ
- gyakorlat: GY
- e-szeminárium: ESZ
- *további szükséges rövidítések*

A tanóra-, kredit- és vizsgatervet az 1. számú melléklet tartalmazza.

8. Az előtanulmányi rend
A tanterv határozza meg, hogy az egyes tantárgyak felvételéhez milyen más tantárgyak előzetes vagy egyidejű teljesítése szükséges (előtanulmányi rend).

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, szóbeli vizsgarészből, 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. A szóbeli záróvizsga részét képezi továbbá egy gyakorlati feladatmegoldás is, amelynek keretében a hallgatónak egy kiberbiztonsági problémára reflektálva kell bemutatnia, hogyan kommunikálná az adott eseményt a szervezeti vezetés felé. A hallgató feladata, hogy az eset kapcsán javaslatot tegyen a szükséges azonnali intézkedésekre, valamint ismertesse azokat a főbb lépéseket, amelyek a helyzet gyors és hatékony kezeléséhez szükségesek. A válasz során elvárás a

szakmai nyelvezet alkalmazása, a logikus érvelés, valamint a tantárgyak során elsajátított elméleti és gyakorlati ismeretek integrált felhasználása.

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. A 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, 2025. szeptember 16.

Dr. Bányász Péter sk.
egyetemi docens 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**			**145**	**100+45**	**30**		
1.1.	Kiberbiztonsági és adatvédelmi jogi keretrendszer	I.	kötelező	40	40+0	8	kollokvium	Dr. Bányász Péter
1.2.	Az információbiztonság alapjai	I.	kötelező	20	10+10	4	kollokvium	Dr. Bányász Péter
1.3.	Információs rendszerek és hálózatok biztonsága	I.	kötelező	20	20+0	4	kollokvium	Dr. Farkas Tibor
1.4.	Információbiztonsági szabványok	I.	kötelező	15	15+0	3	kollokvium	Dr. Szádeczky Tamás
1.5.	Kockázatértékelés, kockázatmenedzsment	I.	kötelező	30	15+15	7	kollokvium	Dr. Krasznay Csaba
1.6.	Kiberfenyegetettség elemzés	I.	kötelező	10	0+10	2	gyakorlati jegy	Dr. Magyar Sándor
1.7.	Mesterséges intelligencia és kibervédelem	I.	kötelező	10	0+10	2	gyakorlati jegy	Dr. Bányász Péter
2.	**II. félév**			**140**	**30+110**	**30**		
2.1.	Incidensmenedzsment	II.	kötelező	25	10+15	6	kollokvium	Dr. Krasznay Csaba
2.2.	Biztonsági tesztelés	II.	kötelező	15	0+15	3	gyakorlati jegy	Dr. Tóth András
2.3.	Információbiztonsági stratégia és vezetés	II.	kötelező	30	10+20	6	gyakorlati jegy	Dr. Kovács László
2.4.	Biztonsági műveleti központok kialakítása	II.	kötelező	15	0+15	3	gyakorlati jegy	Dr. Magyar Sándor
2.5.	Kríziskommunikáció	II.	kötelező	15	0+15	3	gyakorlati jegy	Dr. Kriskó Edina
2.6.	Kiberbiztonsági gyakorlatok	II.	kötelező	10	0+10	2	gyakorlati jegy	Dr. Magyar Sándor
2.7.	Információbiztonsági rendszerek auditja	II.	kötelező	20	10+10	5	gyakorlati jegy	Dr. Krasznay Csaba
2.8.	Hatósági megfelelés támogatása	II.	kötelező	10	0+10	2	gyakorlati jegy	Dr. Bányász Péter
	ÖSSZESEN			**285**	**130+155**	**60**		

A tantárgyi programok listája

I. Törzsanyag
Kiberbiztonsági és adatvédelmi jogi keretrendszer
Az információbiztonság alapjai
Információs rendszerek és hálózatok biztonsága
Információbiztonsági szabványok
Kockázatértékelés, kockázatmenedzsment
Kiberfenyegetettség elemzés
Mesterséges intelligencia és kibervédelem
Incidensmenedzsment
Biztonsági tesztelés
Információbiztonsági stratégia és vezetés
Biztonsági műveleti központok kialakítása
Kríziskommunikáció
Kibergyakorlatok
Információbiztonsági rendszerek auditja
Hatósági megfelelés támogatása

II. Szakdolgozat

III. Szabadon választható tantárgyak

List of Course Programs

I. Core curriculum

Legal framework for cybersecurity and data protection
Basics of Information Security
Security of Information Systems and Networks
Information Security Standards
Risk Assessment, Risk Management
Cyber Threat Intelligence
Artificial intelligence and cyber defence
Incident management
Security Testing
Information Security Strategy and Leadership
Designing Security Operation Centres
Crisis communication
Cyberdefence exercises
Audit of information security systems
Assistance for compliance with public authorities

II. Thesis

III. Optional Subjects

ELEKTRONIKUS INFORMÁCIÓBIZTONSÁGI VEZETŐ SZAKIRÁNYÚ TOVÁBBKÉPZÉSI SZAK TANTÁRGYI PROGRAMOK

ELECTRONIC INFORMATION SECURITY MANAGER POSTGRADUATE SPECIALIST TRAINING COURSE COURSE PROGRAMS

1. TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** KVTIS1192
2. **A tantárgy megnevezése (magyarul):** Kiberbiztonsági és adatvédelmi jogi keretrendszer
3. **A tantárgy megnevezése (angolul):** Legal framework for cybersecurity and data protection
4. **Kreditérték és képzési karakter:**
   - 4.1. 8 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. Bányász Péter, egyetemi docens, PhD.
7. **A tanórák száma és típusa:**
   - 7.1. össz óraszám/félév / total number of lectures: 40
   - 7.2. levelező munkarend / correspondence training: 40 EA (vagy 40 óra online előadás, amennyiben az évfolyam létszáma indokolja) + 0 SZ + 0 GY
8. **A tantárgy szakmai tartalma (magyarul):**

   A tárgy elsődleges célja az adatok, és az adatok kezelésére, tárolására, továbbítására alkalmas elektronikus információs rendszerek védelmét szolgáló európai uniós és hazai szabályozási keretrendszer elsajátítása. A hallgatók megismerik a nemzetközi és hazai jogszabályi környezet fejlődését, az aktuális hatály szerinti szervezeti- és feladatrendszert, felelősségi és hatásköröket, valamint az adatvédelemi és információbiztonsági követelményeket, amelyeket az érintett szervezetek teljesítenek. Betekintést nyernek emellett a védelmi tevékenységekhez köthető tervezési, dokumentációs, hatósági és ellenőrzési, illetve információbiztonsági feladatellátásba is. A tárgy foglalkozik a definíciós környezet evolúciójával a kétezres évektől napjainkig, nemzetközi és hazai viszonylatban. Bemutatja továbbá az információbiztonsághoz kapcsolódó egyéb szabályozóeszközöket, amelyek a keretrendszeren túl a biztonság magasabb szintjének eléréhez hozzájárulhatnak.

   A tantárgy szakmai tartalma (angolul):

   The primary aim of the subject is to master the European Union and domestic regulatory framework that protects data and electronic information systems suitable for managing, storing, and transmitting data. Students will learn about the development of the international and domestic legal environment, the current organizational and task system, responsibilities, and competencies, as well as the data protection and information security requirements that the relevant organizations must meet. Additionally, they will gain insight into planning, documentation, regulatory and control activities, and information security tasks related to protective activities. The subject also deals with the evolution of the definitional environment from the 2000s to the present, both internationally and domestically. Furthermore, it presents other regulatory tools related to information security that can contribute to achieving a higher level of security beyond the framework.

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 (magyarul, angolul - English):

11.1. Jogi alapok a kiberbiztonságban és adatvédelemben (Legal foundations of cybersecurity and data protection);

11.2. Nemzetközi kitekintés: az EU biztonsági és kiberbiztonsági stratégiái, az adatvédelmi és információbiztonsági kérdések jelentőségének változása az elmúlt 20 évben. Nemzetközi intézményrendszer bemutatása, ENISA jelentősége és szerepe (International outlook: EU security and cybersecurity strategies; changes in the significance of data protection and information security over the past 20 years; overview of the international institutional framework and the role and relevance of ENISA);

11.3. Az Európai Parlament és a Tanács 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről (Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [GDPR]);

11.4. Adatvédelmi fogalomrendszer: alapvető definíciók és az adatvédelem célja, rendeltetése, a GDPR-ból fakadó alapelvek és kötelezettségek a hazai szabályozási környezetben (Data protection terminology: basic definitions and the purpose of data protection, principles and obligations arising from the GDPR in the domestic regulatory environment);

11.5. Adatvédelem Magyarországon: hazai szabályozással és gyakorlattal kapcsolatos tapasztalatok (Data protection in Hungary: experiences with national regulations and their practical implementation);

11.6. Információbiztonsági fogalomrendszer: aktuális nemzetközi és hazai szakmai terminológia, az információbiztonsági kötelezettségek célkitűzései, a kapcsolódó szervezeti és tagállami szintű stratégia alkotás jelentősége (Information security terminology: current international and domestic professional terminology, objectives of information security obligations, and the importance of developing related organizational and national-level strategies);

11.7. Új megközelítések az információbiztonsági szabályozásban: az Európai Parlament És A Tanács (EU) 2022/2555 Irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről, a NIS 2 irányelvből fakadó tagállami kötelezettségek és szervezetekkel szembeni elvárások értelmezése (New approaches in information security regulation: Directive (EU) 2022/2555 of the European Parliament and the Council on measures for a high common level of cybersecurity across the Union, as well as amendments to regulation (EU) 910/2014 and directive (EU) 2018/1972, and the repeal of directive (EU) 2016/1148, interpretation of member state obligations and expectations from organizations arising from the NIS 2 Directive);

11.8. Magyarország kiberbiztonsági szabályozása: a NIS 2 irányelv implementációja, valamint a kialakított jogi környezet (kiberbiztonsági stratégia, kiberbiztonságáról szóló törvény és végrehajtási rendelete, követelmények a miniszteri rendeletekben, auditok és felügyeleti díj rendje az SZTFH rendeletek alapján), az érintett szervezetrendszer felépítése és feladatai, a személyi hatály alá tartozó szervezetek és kötelezettségeik (Cybersecurity regulation in Hungary: implementation of the NIS 2 Directive, and the established legal environment (Cybersecurity Strategy, Cybersecurity Act and its Implementing Decrees, requirements in Ministerial Decrees, audit and supervision fee regulations based on SZTFH Decrees), structure and tasks of the relevant organizational system, and obligations of entities subject to personal scope);

11.9. Információbiztonsági érettség fejlesztése: információbiztonsági követelmények értelmezése a szervezetek szintjén, szervezeti szerepkörök a kiberbiztonságban és az adatvédelemben, a kiberreziliencia, mint megközelítés és a tudatosság, mint attitűd (Developing information security maturity: interpreting information security requirements at the organizational level; organizational roles in cybersecurity and data protection; cyber resilience as an approach; and awareness as an attitude);

11.10. Kapcsolódó EU-s törekvések: kiberbiztonsági tanúsítási keretrendszer, kiberreziliencia fokozása, pénzügyi szektor digitális ellenállóképességének erősítés, kritikus szervezetek védelmének hatékonyabbá tétele, mesterséges intelligencia fejlesztésének és alkalmazásának felelős előmozdítása (Cybersecurity Act, Cyber Resilience Act, DORA, CER, AI Act);

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:

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

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 tanórákon való 70 %-os részvétel.

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 legalább elégséges vizsgajegy.

16. Irodalomjegyzék:

16.1. Kötelező irodalom:

- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról és kapcsolódó végrehajtási rendeletei;
- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről;
- Sziklay Júlia – Bendik Tamás: Az adatvédelem hazai és európai uniós szabályozása és alapintézményei. Negyedik, hatályosított kiadás, Nemzeti Közszolgálati Egyetem, Budapest, 2018. ISBN: 978-615-5870-98-9;

16.2. Ajánlott irodalom:

- Európai Adatvédelmi Hatóság: Iránymutatás az adatvédelmi incidensek GDPR-rendelet szerinti bejelentéséről – 2.0 verzió. URL: https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202209_personal_data_breach_notification_v2.0_hu.pdf (Online tananyag);
- Krasznay Csaba: A NIS2 irányelv kihívásai és gyakorlati alkalmazása. In Védelem Tudomány a Katasztrófavédelem Online Szakmai, tudományos folyóirata, 9 kszm, ISSN: 2498-6194;
- Európai adatvédelmi jogi kézikönyv. Az Európai Unió Kiadóhivatala, Luxembourg, 2014. ISBN: 978-92-871-9944-7;

Budapest, 2025. szeptember 16.

Dr. Bányász Péter sk.
egyetemi docens, NKE ÁNTK

2. TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** KVTIS1193
2. **A tantárgy megnevezése (magyarul):** Az információbiztonság alapjai
3. **A tantárgy megnevezése (angolul):** Basics of Information Security
4. **Kreditérték és képzési karakter:**
   - 4.1. 4 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. Bányász Péter, egyetemi docens, PhD.
7. **A tanórák száma és típusa:**
   - 7.1. összes óraszám/félév: 20 óra
   - 7.2. levelező munkarend: 20 óra (10 EA (vagy 10 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):**

A tantárgy célja, hogy a hallgatók alapvető ismereteket szerezzenek az információbiztonság elméleti és gyakorlati alapjairól, különös tekintettel a kibertérrel összefüggő társadalmi, technológiai és biztonsági kérdésekre. A kurzus bevezet a digitális társadalom biztonsági dilemmáiba, bemutatja a kiberbiztonság történeti fejlődését és a kibertér fogalmi kereteit. A hallgatók megismerik az információbiztonság alapfogalmait, a kibertér szereplőit és motivációikat, valamint a digitális adatok és kritikus infrastruktúrák védelmének alapvető szempontjait. A tantárgy áttekinti a leggyakoribb kibertéri fenyegetéstípusokat, példákkal illusztrálva, valamint felhívja a figyelmet a jövő technológiai trendjeiben rejlő újabb kockázatokra. A tárgy megalapozza a hallgatók további információbiztonsági tanulmányait, miközben fejleszti biztonságtudatosságukat és rendszerszintű gondolkodásukat.

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

The aim of the course is to provide students with basic knowledge of the theoretical and practical foundations of information security, with a particular focus on social, technological, and security issues related to cyberspace. The course introduces the security dilemmas of the digital society, presents the historical development of cybersecurity and the conceptual framework of cyberspace. Students will learn the basic concepts of information security, the actors and motivations in cyberspace, and the fundamental aspects of protecting digital data and critical infrastructure. The course reviews the most common types of cyber threats, illustrated with examples, and draws attention to new risks inherent in future technology trends. The course lays the foundation for students' further studies in information security, while developing their security awareness and systems thinking.

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 társadalom biztonsági dilemmái (The security dilemmas of the information society);
11.2. A kiberbiztonság fejlődéstörténete és mérföldkövei (The history and milestones of cybersecurity);
11.3. A kibertér értelmezése (Understanding cyberspace)
11.4. Az információbiztonság alapvető fogalmai (Basic concepts of information security);
11.5. A kibertér szereplői és motivációik (The actors in cyberspace and their motivations);
11.6. Digitális adatok és kritikus infrastruktúrák védelme (Protection of digital data and critical infrastructure);
11.7. Kibertéri fenyegetések típusai és példái (Types and examples of cyber threats)
11.8. Jövőbeni kihívások és technológiai trendek (Future challenges and technological trends);

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 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 írásbeli és 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 (Online tananyag);
- Gyaraki Réka (szerk.): Az információbiztonság alapjai. NKE RTK, 2023., URL: https://rtk.uni-nke.hu/document/rtk-uni-nke-hu/az_informaciobiztonsag_alapjai_konyv_kesz_2.pdf (Online tananyag);

16.2. Ajánlott irodalom:

- Bonnyai Tünde – Kiss Adrienn – Tóth András (szerk.): Nagyvállalati biztonságtudatosság és nyílt forrású információszerzés: Kiber- és információbiztonsági tanulmányok. Ludovika Egyetemi Kiadó, Budapest, 2023., ISBN: 9786156598691
- Kovács László: A kibertér védelme. Dialóg Campus Kiadó, Budapest, 2018. ISBN 978 615 5889 63 9 (nyomtatott) ISBN 978 615 5889 64 6 (Online tananyag);

Budapest, 2025. szeptember 16.

Dr. Bányász Péter sk.
egyetemi docens, NKE ÁNTK

3. TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** KVTIS1194
2. **A tantárgy megnevezése (magyarul):** Információs rendszerek és hálózatok biztonsága
3. **A tantárgy megnevezése (angolul):** Security of Information Systems and Networks
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, habilitált egyetemi docens, PhD.
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 tantárgy célja, hogy átfogó ismereteket nyújtson az informatikai rendszerek működéséről, különös tekintettel a hálózati infrastruktúrára és az ahhoz kapcsolódó technológiai alapokra. A hallgatók megismerkednek a hálózati architektúrák felépítésével, a hálózati protokollokkal és a kommunikációs mechanizmusokkal, különös hangsúlyt fektetve az OSI és TCP/IP modellekre. A tárgy bemutatja az információbiztonság technikai kontrollcsaládját, valamint annak szerepét és jelentőségét a szervezeti biztonsági architektúrában. A kurzus során példákon keresztül kerül bemutatásra az alapvető információbiztonsági alapelvek – mint az AAA (azonosítás, hitelesítés, jogosultságkezelés) és a BSR (bizalmasság, sértetlenség, rendelkezésre állás) – gyakorlati alkalmazása technikai kontrollok segítségével. Kiemelt figyelmet kap az elektronikus információbiztonsági vezető szerepe a technikai kontrollok kialakításában, működtetésében és fenntartásában, valamint a kontrollok közötti technológiai függőségek és azok rendszerszintű kezelése. A kurzus célja a hallgatók biztonságtudatos és rendszerszemléletű gondolkodásának megalapozása a kiberbiztonság technikai dimenzióiban.

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

   The aim of the course is to provide comprehensive knowledge of the functioning of information systems, with a particular focus on network infrastructures and communication protocols. Students will gain an understanding of basic network architectures, methods of network connectivity, and the layered operations defined by the OSI and TCP/IP models. The course offers an overview of information security controls, with emphasis on the family of technical controls and their role in organizational security implementation.

   Key information security principles—such as AAA (authentication, authorization, and accounting) and CIA (confidentiality, integrity, and availability)—are presented through practical examples demonstrating their enforcement via technical controls. Special attention is given to the role of the Chief Information Security Officer (CISO, in Hungarian: EIV) in the design, implementation, and maintenance of technical safeguards, as well as in managing technological dependencies between controls. The course aims to develop students' security awareness and systemic thinking within the technical dimensions of cybersecurity.
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 (Structure and operation of modern computers);
11.2. Operációs rendszerek funkciói, működési elvei (Functions and operating principles of operating systems);
11.3. Hálózati protokollok és kommunikáció, Ethernet szabvány (Network protocols and communication, Ethernet standard);
11.4. Hálózati és szállítási réteg (Network and transport layer);
11.5. Alkalmazási réteg (Application layer);
11.6. Kapcsolt hálózatok, a kapcsolás beállításainak alapjai (Switched networks, basics of switching configuration);
11.7. VLAN-ok (VLANs);
11.8. A forgalomirányítás alapjai (Basics of routing);
11.9. Statikus, dinamikus forgalomirányítás (Static and dynamic routing);
11.10. Hozzáférés vezérlési listák, DHCP, IPv4 hálózati címfordítás (Access Control Lists, DHCP, IPv4 Network Address Translation);
11.11. WAN technológiák jellemzői (Characteristics of WAN technologies);
11.12. Virtuális magánhálózatok (VPN) működése (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.
  - URL: http://mek.oszk.hu/08300/08374/;
- 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, 2025. szeptember 16.

Dr. Farkas Tibor sk.
habilitált egyetemi docens, NKE HHK

4. TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** KVTIS1195
2. **A tantárgy megnevezése (magyarul):** Információbiztonsági szabványok
3. **A tantárgy megnevezése (angolul):** Information Security Standards
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. Szádeczky Tamás, egyetemi tanár, PhD.
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):**

   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:

   - 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.

   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 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.

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 (The concept of standards, the context of information security standards and their uses);
11.2. Az ISO/IEC 27000 sorozat felépítése, főbb elemei (Structure and main elements of the ISO/IEC 27000 series);
11.3. Az ISO/IEC 27001 szabvány szerinti Információbiztonsági Irányítási Rendszer (IBIR) követelményei (Requirements of the Information Security Management System (IBIR) according to ISO/IEC 27001);
11.4. IBIR kontrollok az ISO/IEC 27002 alapján (IBIR controls based on ISO/IEC 27002);
11.5. Belső és külső audit az ISO 19011 és az ISO/IEC 27006 figyelembe vételével (Internal and external auditing in the light of ISO 19011 and ISO/IEC 27006);
11.6. A NIST SP 800 sorozat és az SP 800-53 (NIST SP 800 series and SP 800-53);
11.7. IT terméktanúsítás és Common Criteria (IT product certification and Common Criteria);
11.8. További szabványok áttekintése: COBIT, ITIL, Enterprise Information Security Architecture (EISA), Payment Card Industry Data Security Standard (Overview of other standards: COBIT, ITIL, Enterprise Information Security Architecture (EISA), Payment Card Industry Data Security Standard);

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 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, írásbeli és 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 (Online tananyag);
- MSZ ISO/IEC 27001:2023 Információbiztonság, kiberbiztonság és a magánélet védelme. Információbiztonság-irányítási rendszerek. Követelmények;
- MSZ EN ISO/IEC 27002:2023 Információbiztonság, kiberbiztonság és a magánélet védelme. Információbiztonsági kontrollok/intézkedések;

Budapest, 2025. szeptember 16.

Dr. Szádeczky Tamás sk.
egyetemi tanár, NKE ÁNTK

5. TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** KVTIS1196
2. **A tantárgy megnevezése (magyarul):** Kockázatértékelés, kockázatmenedzsment
3. **A tantárgy megnevezése (angolul):** Risk Assessment, Risk Management
4. **Kreditérték és képzési karakter:**
   - 4.1. 7 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, habilitált egyetemi docens, PhD.
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 az 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, az Octave, az ISO NIST SP 800-53, illetve részletesen elemzésre kerül a 2024. évi LXIX. tv. és végrehajtási rendeletei 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 aim of the course is to introduce information security risk analysis and risk management. In this context, students will learn about the conceptual tools used in standards, in particular the ISO 31000 and 27005 standards, i.e. the general and information security risk management standards. They will master quantitative, qualitative and semi-quantitative risk assessment solutions. Risk assessment options and algorithms will be reviewed. The lecture presents risk management frameworks such as COBIT2019, Octave, ISO NIST SP 800-53, and provides a detailed analysis of Act LXIX of 2024 and its implementing decrees. During the practical part of the course, risk assessment case studies will be developed, risk scenarios will be compiled by the students, and risk management plans will be prepared, including asset inventories and vulnerability assessments.

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 2024. évi LXIX. tv. és a kockázatkezelés alapjai (Introduction: the Act LXIX of 2024 and the basics of risk management);

11.2. Kockázatmenedzsment a 2024. évi LXIX. törvényben és a 7/2024 MK rendeletben

(Risk assessment in the Act LXIX of 2024 and Decree 7/2024);

11.3. Az ISO 31000:2018 és az ISO/IEC 27000-es szabványcsalád kockázatkezelési szabványa, az ISO/IEC 27005:2022 (The ISO 31000:2018 standard and the risk management standard of the ISO/IEC 27000 standard family, the ISO/IEC 27005:2022);

11.4. Kockázatértékelés és az ISO/IEC 27001:2022 szabvány (Risk assessment and the ISO/IEC 27001:2022 standard);

11.5. Kockázatkezelés az ISO/IEC 27005:2022 mentén (Risk management according to the ISO/IEC 27005:2022);

11.6. Szabályozott kockázatkezelés (Áttekintés: COBIT2019 - RiskIT, ITILv4, Octave, NIST SP 800-53) (Regulated risk management (Review: COBIT2019 - RiskIT, ITILv4, Octave, NIST SP 800-53);

11.7. Vagyonleltár és sebezhetőség vizsgálat (Asset and vulnerability assessment);

11.8. Kockázati forgatókönyv (Risk scenario);

11.9. A kockázatértékelési folyamat (azonosítás, elemzés, kiértékelés) (Risk assessment process (identification, analysis, evaluation);

11.10. Kockázatbecslés (kvantitatív, kvalitatív, szemikvantitatív) (Risk estimation (quantitative, qualitative, semi-quantitative);

11.11. Kockázatmenedzsment – kockázatkezelési terv (Risk management plan);

11.12. Az információvédelmi intézkedések területei (Areas of countermeasures in information security);

11.13. Lehetséges intézkedések meghatározása és értékelése (Identification and evaluation of potential countermeasures);

11.14. A kockázatértékelés karbantartása (megismétlése) (Review (repeat) of risk assessment);

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:

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

14. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A hallgatók a félév folyamán kiscsoportos foglalkozás során egy fiktív kockázatelemzést készítenek el, a félév során megadott információkat követve. Az értékelés ötfokozatú: elégtelen (60% alatt), elégséges (61%-70%), közepes (71%-80%), jó (81%-90%), jeles (91%-100%).

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, 2025. szeptember 16.

Dr. Krasznay Csaba sk.
habilitált egyetemi docens, NKE ÁNTK

6. TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** KVTIS1197
2. **A tantárgy megnevezése (magyarul):** Kiberfenyegetettség elemzés
3. **A tantárgy megnevezése (angolul):** Cyber Threat Intelligence
4. **Kreditérték és képzési karakter:**
   4.1. 2 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. Magyar Sándor, tanszékvezető, egyetemi docens, PhD.
7. **A tanórák száma és típusa:**
   7.1. össz óraszám/félév /: 10 óra
   7.2. levelező munkarend: 10 óra (0 EA/L + 0 SZ/S + 10 GY/P (vagy 10 óra online gyakorlat, amennyiben az évfolyam létszáma indokolja))
8. **A tantárgy szakmai tartalma (magyarul):**

   A tantárgy keretében a hallgatók megismerik Cyber Threat Intelligence (CTI) tevékenységet és annak szerepét a kibertérből érkező fenyegetésekkel szembeni ellenállóképesség erősítése területén. A tantárgyi ismeretek átadása során bemutatásra kerül CTI életciklusa és a szintjei. A hallgatók megismerik, hogy a különböző forrásokból milyen adatokat és információkat gyűjtenek és elemeznek a tevékenység során. A tantárgy során bemutatásra kerülnek az információ megosztó platformok főbb jellemzői. A tantárgy esetében célként fogalmazódik meg a gyakorlati ismeretek elsajátítása is annak érdekében, hogy a hallgatók rendelkezzenek olyan tudással, amelyet képesek a gyakorlatba hatékonyan átültetni.

   A tantárgy szakmai tartalma (angolul):

   The course will provide students with an understanding of Cyber Threat Intelligence (CTI) and its contribution to strengthening resilience to threats that emerge from cyberspace. The life cycle of CTI will be introduced. Students will be familiarised in detail with the levels of CTI. Students will learn how data and information from different sources are collected and analysed during the activity. The main features of information sharing platforms will be introduced. The course also aims to provide students with the practical skills they need to be able to put their knowledge into practice effectively.

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

   Tudása

   - Átlátja, hogy milyen védelmi megoldások vannak a kibertámadás ellen.
   - Ismeri a kibertámadás esetén alkalmazandó eljárásokat.
   - Ismeri a kártékony kódok fogalmát és hatásmechanizmusát.
   - Megérti a szervezeti feladatokat a kibervédelemben.

   Képességei

   - Képes olyan technológiai védelmi intézkedések meghozatalára, amelyek a Cyber Kill Chain egyes elemeihez kapcsolódnak.
   - Képes átlátni a kibertér aktuális fenyegetéseit.
   - 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.
- Partner abban, hogy se a szervezete, se ő maga ne váljon kibertámadás áldozatává.

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.
- 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.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge:

- He/She is familiar with defence solutions against cyberattacks.
- He/She is familiar with procedures applicable in case of a cyberattack.
- He/She is capable of taking technological defensive measures related to elements
- He/She is familiar with organisational tasks in cybersecurity.

Capabilities:

- He/She is capable of taking technological defensive measures related to elements of the cyber kill chain.
- He/She is capable of understanding the current threats of cyberspace.
- 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 attention to and application of laws of cyber security in his/her work.
- His/Her personal attitude is characterized by an effort to take effective measures in order to prevent cyberattacks, by this means reducing the exposure of his/her organisation.
- 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 implement advanced knowledge characterising cyber security on a national and international level.
- His/Her autonomy and responsibility are to process new and complex information, problems and phenomena in a systematic and critical way.
- His/Her personal attitude is characterized by an effort to design the cyber security management system in its own complexity.
- 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.
- 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(magyarul, angolul - English):

11.1. Cyber Threat Intelligence (CTI) tevékenysége és annak szerepét a kibertérből érkező fenyegetésekkel szembeni ellenállóképesség erősítése területén. (Cyber Threat Intelligence (CTI) and its contribution to strengthening resilience to threats that emerge from cyberspace);

11.2. CTI életciklusa és szintjei (The life cycle and the levels of CTI);

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

11.4. A CTI elemzésének módszerei (Methods of CTI analysis);

11.5. Az információmegosztás szerepe, előnyei, kockázatai. A CTI platformok (The role, benefits, and risks of information sharing. CTI platforms.).

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:

A hallgató köteles a foglalkozások legalább 70 %-án részt venni. A távollétet a hiányzást követő első foglalkozáson kell igazolnia. Hiányzás esetén a hallgató köteles a foglalkozások anyagát beszerezni, abból önállóan felkészülni.

14. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A tanulmányi munka alapja a szemináriumok látogatása, az előírt olvasmányok ismerete. A hallgató a félév során egy feleletválasztós tesztet ír. A szorgalmi időszak végén egy vizsgafeladat gyakorlati megvalósítása. A félévközi feladatok összesítéséből áll a gyakorlati jegy. A TVSZ rendezi a sikertelen értékelés-összetevő javítását.

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 és a 14. pontban meghatározott félévközi feladatok legalább elégséges teljesítése.

15.2. Az értékelés:

A gyakorlati jegy a félévközi feleltválasztós teszt értékeléséből és a vizsgafeladatra adott érdemjegyekből adódik. Az elérendő teljesítmény százaléka mind a félévközi feleltválasztós teszt és a vizsgafeladat esetében: 60 %-tól elégséges, 70 %-tól közepes, 80-tól % jó, 90 %-tól jeles.

15.3. A kreditek megszerzésének feltételei:

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

16. Irodalomjegyzék:

16.1. Kötelező irodalom:

- Kovács László: A Kibertér Védelme. Nordex Kft., Budapest, 2018. ISBN: 9786155889639;
- Kovács László: Hadviselés a 21. Században. Budapest: Ludovika Egyetemi Kiadó, Budapest, 2023. ISBN:9789635317653;
- Kovács László – Krasznay Csaba. Digitális Mohács 3.0. In: Hadtudomány: A Magyar Hadtudományi Társaság Folyóirata, 34. évf., 3. sz., 2024. ISSN: 1215-4121;

16.2. Ajánlott irodalom:

- Bazzell, Michael: Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information. CreateSpace Independent Publishing Platform. 2018. ISBN 978-1984201577;

Budapest, 2025. szeptember 16.

Dr. Magyar Sándor sk.
tanszékvezető, egyetemi docens, NKE HHK

7. TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** KVTIS1198
2. **A tantárgy megnevezése (magyarul):** Mesterséges intelligencia és kibervédelem
3. **A tantárgy megnevezése (angolul):** Artificial intelligence and cyber defence
4. **Kreditérték és képzési karakter:**
   4.1. 2 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. Bányász Péter, egyetemi docens, PhD.
7. **A tanórák száma és típusa:**
   7.1. össz óraszám/félév /: 10 óra
   7.2. levelező munkarend: 10 óra (0 EA/L + 0 SZ/S + 10 GY/P (vagy 10 óra online gyakorlat, amennyiben az évfolyam létszáma indokolja))
8. **A tantárgy szakmai tartalma (magyarul):**

A tantárgy célja, hogy a hallgatók átfogó elméleti és gyakorlati ismereteket szerezzenek a mesterséges intelligencia technológiáinak alkalmazásáról a kibervédelem területén, különös tekintettel a generatív mesterséges intelligencia által jelentett új kockázatokra és lehetőségekre. A kurzus bemutatja a gépi tanulás és a generatív MI szerepét mind a kibertámadásokban, mind a védekezés fejlesztésében, beleértve az automatizált fenyegetettség-elemzést, a sérülékenység-tesztelést és az anomáliák felismerését. A tantárgy kitér a promptolás alapjaira és legjobb gyakorlataira, valamint az etikai és jogi aspektusokra is. A kurzus során a hallgatók képesek lesznek az MI-alapú eszközök gyakorlati alkalmazásának kritikus értékelésére, a fenyegetések felismerésére és a biztonsági stratégiák fejlesztésére.

A tantárgy szakmai tartalma (angolul):

The aim of the course is to provide students with comprehensive theoretical and practical knowledge of the application of artificial intelligence technologies in the field of cyber defense, with a particular focus on the new risks and opportunities presented by generative artificial intelligence. The course introduces the role of machine learning and generative AI in both cyberattacks and defense development, including automated threat analysis, vulnerability testing, and anomaly detection. The course also covers the basics and best practices of prompting, as well as ethical and legal aspects. Upon completion of the course, students will be able to critically evaluate the practical application of AI-based tools, recognize threats, and develop security strategies.

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

Tudása

- Átlátja, hogy milyen védelmi megoldások vannak a kibertámadás ellen.
- Ismeri a kibertámadás esetén alkalmazandó eljárásokat.

Képességei

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

Attitűdje

- 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.

Autonómiája és felelőssége

- Önállóan dolgozza fel az új és összetett információkat, problémákat, illetve jelenségeket, rendszerszerű és kritikus módon.
- Vállalja a szakterület, a szakmai praxis módszertanának fejlesztéséhez szükséges elméleti, tudományos kutatási és gyakorlati információk beszerzésének, értékelésének és hasznosításának végrehajtását.
- Gyakorlatába beépíti és alkalmazza az e szakterületen folyó kutatások eredményeit.

Elérendő kompetenciák (angolul) (Competences – English):

- He/She is familiar with defence solutions against cyberattacks.
- He/She is familiar with procedures applicable in case of a cyberattack.

Knowledge:

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

Capabilities:

- He/She is capable of understanding the current threats of cyberspace.
- 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 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.
- 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 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 put the results of scientific research in the field into his/her practice.

10. Előtanulmányi követelmények: -

11. A tantárgy tananyagának leírása, tematika(magyarul, angolul - English):

11.1. A generatív mesterséges intelligencia kiberbiztonsági kockázatai (Cybersecurity risk of generative artificial intelligence);

11.2. A promptolás alapjai (Basics of prompting);

11.3. Jó gyakorlatok a promptolásban (Best practices for prompting);

11.4. Bevezetés az MI és a kibervédelem kapcsolatába (An Introduction to the relationship between AI and cyber defense);

11.5. Gépi tanulással támogatott kibervédelmi eszközök (Machine learning-assisted cyber defense tools);

11.6. Mesterséges intelligencia előfordulása kibertámadásokban (The use of artificial intelligence in cyber attacks);

11.7. Etikai és jogi kérdések (Ethical and legal considerations);

11.8. MI támogatott eszközök gyakorlati alkalmazhatósága (The practical applicability of AI-supported tools);

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:

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

14. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A hallgató értékelése a szorgalmi időszakban egy gyakorlati feladat 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: gyakorlati projektfeladat megoldása, amelynek során egy elképzelt kiberbiztonsági incidens különböző szempontú megoldására kell javaslatot tennie a vizsgázónak, felhasználva a 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:

- Bagó Péter: Kiberbiztonság és a mesterséges intelligencia kapcsolata. In: Gazdaság és Pénzügy, 10 évf. 2. sz. 2023. ISSN: 2677-1314;
- Az EURÓPAI PARLAMENT ÉS A TANÁCS 2024. június 13-i (EU) 2024/1689 RENDELETE a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a 300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/1139 és az (EU) 2019/2144 rendelet, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelv módosításáról (a mesterséges intelligenciáról szóló rendelet);

- Robertson, Jeandri – Ferreira, Caitlin –Botha, Elsamari – Oosthuizen, Kim: Game changers: A generative AI prompt protocol to enhance human-AI knowledge co-construction. In: Business Horizons, 67. évf. 5. sz., Elsevier Ltd, 2024. ISSN: 00076813;

16.2. Ajánlott irodalom:

- NIST: AI Risk Management Framework. URL: https://www.nist.gov/itl/ai-risk-management-framework (Online tananyag);
- Europol: AI and policing- The benefits and challenges of artificial intelligence for law enforcement. Publications Office of the European Union, Luxembourg, ISBN: 978-92-95236-35-6, URL: https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing;
- Bansal, Prashant: Prompt Engineering Importance and Applicability with Generative AI. In: Journal of Computer and Communications, 12. évf. 10. sz., 2024. ISSN: 2327-5219;

Budapest, 2025. szeptember 16.

Dr. Bányász Péter sk.
egyetemi docens, NKE ÁNTK

8. TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** KVTIS1199
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: 40% gyakorlat, 60% elmélet
5. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** NKE KTI
6. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Krasznay Csaba, habilitált egyetemi docens, PhD
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 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 (Theory of incident management);
11.2. Az incidenskezelés jogi háttere (Legal background of incident management);
11.3. Az incidenskezelés szervezeti háttere Magyarországon és a nemzetközi térben, CERT/CSIRT szervezetek (Organizational background of incident management in Hungary and internationally, CERT/CSIRT);
11.4. A Biztonsági Műveleti Központok (Security Operation Centers);
11.5. Az incidenskezelés műszaki eszköztára, logforrások (Technical tools of incident management, log sources);
11.6. Naplóelemzés, SIEM rendszerek (Log analysis, SIEM systems);
11.7. EDR, XDR, MDR (EDR, XDR, MDR);
11.8. Incidenssel kapcsolatos információk megosztása, CTI (Incident information sharing, CTI);
11.9. Mesterséges intelligencia az incidensmenedzsmentben (Artificial Intelligence in incident management);
11.10. Üzletmenet-folytonosság tervezése (Business continuity planning);
11.11. Esemény, probléma, incidens fogalmának meghatározása, gyakorlati példák bemutatása (Definition of security event, problem and incident, practical examples);
11.12. Incidens esettanulmányok (Incident related case studies);

11.13. Incidenskezelő csapat létrehozása (Setup of an incident management team);
11.14. Az incidenskezelés folyamata a gyakorlatban, TTX (Incident management in practice, TTX);

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:

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

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 (2022): Incidensmenedzsment - Éves továbbképzés az elektronikus információs rendszerek védelméért felelős vezető számára;

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, 2025. szeptember 16.

Dr. Krasznay Csaba sk.
habilitált egyetemi docens, NKE ÁNTK

9. TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** KVTIS1200
2. **A tantárgy megnevezése (magyarul):** Biztonsági tesztelés
3. **A tantárgy megnevezése (angolul):** Security Testing
4. **Kreditérték és képzési karakter:**
   - 4.1. 3 kredit
   - 4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 100% gyakorlat, 0% elmélet
5. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** NKE KTI
6. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Tóth András, tanszékvezető, habilitált egyetemi docens, PhD.
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 (Steps to design and build a security test laboratory);

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

11.3. Biztonságtesztelő módszerek fő típusai (Main types of security testing methods);

11.4. Biztonsági eszközök vizsgálatának lehetőségei (Possibilities for testing security devices);

11.5. Biztonsági funkcionális tesztelés (Security functional testing);

11.6. Sérülékenység-vizsgálat (Vulnerability assessment);

11.7. Behatolás tesztelés (Penetration testing);

11.8. Helyi és távoli sérülékenység keresés és kihasználás (Local and remote vulnerability scanning and exploitation);

11.9. Alkalmazások és szolgáltatások tesztelésének lehetőségei (Possibilities for testing applications and services);

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

11.11. Felhasználói biztonságtudatossági vizsgálatok (Social engineering tests);

11.12. Vezeték nélküli rendszerek tesztelésének módszertana (Methodology of wireless testing);

11.13. Mobil eszközök (okos eszközök) tesztelésének lehetőségei (Mobile (smart) device testing);

11.14. Beágyazott rendszerek vizsgálatának lehetőségei (Possibilities of embedded systems' security testing);

11.15. Továbbképzés és önképzés egyéni és csoportos lehetőségei (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 gyakorlati 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, 2025. szeptember 16.

Dr. Tóth András sk.
tanszékvezető, habilitált egyetemi docens, NKE HHK

10. TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** KVTIS1201
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: 30% gyakorlat, 70% elmélet
5. **Az oktatásért felelős oktatási szervezeti egység megnevezése:** NKE KTI
6. **A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:** Dr. Kovács László, egyetemi tanár, DSc.
7. **A tanórák száma és típusa:**
   - 7.1. összes óraszám/félév: 30 óra
   - 7.2. levelező munkarend: 30 óra (10 EA (vagy 10 óra online előadás, amennyiben az évfolyam létszáma indokolja) + 0 SZ + 20 GY (vagy 20 óra online gyakorlat, amennyiben az évfolyam létszáma indokolja))
8. **A tantárgy szakmai tartalma (magyarul):**

A tantárgy célja, hogy átfogó és gyakorlatorientált ismereteket nyújtson az információbiztonsági stratégia kialakításáról, megvalósításáról és folyamatos fejlesztéséről. A hallgatók megismerik a kiberbiztonság aktuális kihívásait, a biztonságpolitikai megközelítések szerepét a stratégiaalkotásban, valamint az információbiztonsági irányítási rendszer (ISMS) alapvető elemeit. A kurzus külön hangsúlyt fektet a biztonságtudatossági programok szervezeti bevezetésére, értékelésére és fejlesztésére, konkrét példákon keresztül szemléltetve. A tantárgy emellett vezetéselméleti aspektusokat is integrál, így a hallgatók megismerkednek az elektronikus információbiztonsági vezető (EIV) stratégiai szerepével, szervezeti beágyazottságával, valamint a döntéshozatali folyamatokkal a bizonytalan és gyorsan változó környezetben (VUCA). A kurzus kitér az etikai dilemmákra, a vezetői felelősségvállalás kérdéseire, és fejleszti a hallgatók azon kompetenciáit, amelyek szükségesek a biztonság iránt elkötelezett, felelős vezetői szerepkör betöltéséhez. A tantárgy elvégzését követően a hallgatók képessé válnak átfogó információbiztonsági stratégia megalkotására, annak szervezeti integrációjára, hatékony kommunikációjára és értékelésére, valamint biztonságtudatossági kezdeményezések irányítására a vezetői szerepvállalás perspektívájából.

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

The course aims to provide comprehensive and practice-oriented knowledge on the development, implementation, and continuous improvement of an information security strategy. Students will explore current challenges in cybersecurity, the role of security policy in strategic planning, and the foundational components of an Information Security Management System (ISMS). Special emphasis is placed on designing, evaluating, and enhancing organizational security awareness programs, supported by real-world examples. The course also integrates leadership theory, introducing students to the strategic role of the Electronic Information Security Manager (EISM), their organizational responsibilities, and the dynamics of decision-making in volatile, uncertain, complex, and ambiguous (VUCA) environments. Ethical dilemmas and leadership accountability are addressed, fostering a responsible and integrity-driven leadership mindset.

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. Biztonság és biztonságpolitika a kibertérben (Security and security policy in cyberspace);
11.2. Információbiztonsági irányítási rendszer alapjai (Foundations of the Information Security Management System);
11.3. Információbiztonsági stratégia készítése – biztonságtudatossági példával szemléltetve (Creating an Information Security Strategy - Illustrated by an example of security awareness);
11.4. Az információbiztonsági stratégia megvalósítása, módosítása (Implementation and

modification of the information security strategy);

11.5. Visszamérés – biztonságtudatossági példával szemléltetve (Feedback - illustrated with an example of security awareness);

11.6. Biztonságtudatossági alapok (Security Awareness Basics);

11.7. A biztonságtudatosság fejlesztésének lehetőségei (Opportunities for developing security awareness);

11.8. Az elektronikus információbiztonsági vezető: szerepek, felelősségi körök és szervezeti beágyazottság (Electronic Information Security Manager: Roles, Responsibilities, and Organizational Integration);

11.9. Döntéshozatal bizonytalan és gyorsan változó környezetben (VUCA-környezet) (Decision-making in Uncertain and Rapidly Changing Environments – The VUCA Model);

11.10. Etikai dilemmák és felelősségvállalás a vezetői gyakorlatban (Ethical Dilemmas and Accountability in Leadership 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 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 gyakorlati jegy.

16. Irodalomjegyzék:

16.1. Kötelező irodalom:

- Kovács László: Kiberbiztonság és -stratégia. Dialóg Campus Kiadó, Budapest 2018., ISBN: 9786155920936;
- Bonnyai Tünde – Kiss Adrienn – Tóth András (szerk.): Nagyvállalati biztonságtudatosság és nyílt forrású információszerzés: Kiber- és információbiztonsági tanulmányok. Ludovika Egyetemi Kiadó, Budapest 2023., ISBN: 9786156598691;
- Magyar Sándor – Bányász Péter – Bányász-Váczi Kincső Boróka – Pál Anita: Magyarország kibervédelmi stratégiáinak összehasonlítása és fejlődési íve 2013 és 2025 között. In: Szakmai Szemle, 23. évf., 1. sz., 2025. ISSN: 1785-1181;

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

16.2. Ajánlott irodalom:

- Bihari László – Magyar Sándor: Mennyország helyett a pokolba, avagy az informatikai támogatás kihívásai. In: Szakmai Szemle, 18. évf. 4. sz., 2020., ISSN: 1785-1181;
- Czuprák Ottó – Kovács Gábor: A szervezetvezetés elmélete. Dialóg Campus Kiadó, Budapest 2017. ISBN 978 615 576 442 4;
- Belényesi Emese – Koronváry Péter – Szabó Szilvia: Közszolgálati szervezés- és vezetéselmélet. Ludovika Egyetemi Kiadó, Budapest 2019., 9786156020277
- CIO Council: Chief InformaϴOn Security Officer Handbook. URL: https://www.cio.gov/assets/resources/CISO_Handbook.pdf;
- ISACA: CISM Review Manual, 16th Edition, ISBN-13: 978-1604209013, ISBN-10: 1604209011;

Budapest, 2025. szeptember 16.

Dr. Kovács László sk.
egyetemi tanár, NKE HHK

11. TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** KVTIS1202
2. **A tantárgy megnevezése (magyarul):** Biztonsági műveleti központok kialakítása
3. **A tantárgy megnevezése (angolul):** Designing Security Operation Centres
4. **Kreditérték és képzési karakter:**
   - 4.1. 3 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. Magyar Sándor, tanszékvezető egyetemi docens, PhD.
7. **A tanórák száma és típusa:**
   - 7.1. össz 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, hogy a hallgatók átfogó képet kapjanak a biztonsági műveleti központok (SOC) szerepéről az információbiztonságban. Megismerjék a SOC működésének alapelveit, felépítését, a működést meghatározó emberi, technológiai és szervezeti tényezőket. Képessé váljanak különböző kialakítási modellek (belső, külső, hibrid) értékelésére, valamint a szervezeti érettséghez illeszkedő megoldás kiválasztására. A tantárgy célja továbbá, hogy a hallgatók megértsék a SOC-ok közötti együttműködés jelentőségét és formáit a kibervédelem hatékonyságának növelésében.

   A tantárgy szakmai tartalma (angolul):

   The aim of this course is to provide students with a comprehensive understanding of the role of Security Operations Centres (SOCs) in information security. They will learn about the principles and structure of SOC operations, the human, technological and organisational factors that determine their operation. They will be able to evaluate different design models (internal, external, hybrid) and select the solution that best fits the organisational maturity. The course also aims to provide students with an understanding of the importance and forms of cooperation between SOCs in increasing the effectiveness of cyber defence.

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 kártékony kódok fogalmát és hatásmechanizmusát.
   - Megérti a szervezeti feladatokat a kibervédelemben.

   Képességei

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

Attitűdje

- Hatékony lépéseket tesz a kibertámadások megelőzése érdekében, így csökkentve a szervezete kitettségét.
- Partner abban, hogy se a szervezete, se ő maga ne váljon kibertámadás áldozatává.

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.
- 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.

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 the concept and mode of action of malware codes.
- He/She is familiar with organisational tasks in cybersecurity.

Capabilities:

- He/He/She is capable of taking defensive measures that ensure the reduction of risk resulting from threat against humans.
- He/She is capable of taking technological defensive measures related to elements of the cyber kill chain.
- He/She is capable of understanding the current threats of cyberspace.
- 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 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 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 implement advanced knowledge characterising cyber security on a national and international level.
- His/Her autonomy and responsibility are to process new and complex information, problems and phenomena in a systematic and critical way.
- His/Her personal attitude is characterized by an effort to design the cyber security management system in its own complexity.
- 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.
- 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 (magyarul, angolul - English):

11.1. A biztonsági műveleti központok alapjai. Fogalom, célja, feladatai, működési modelljei, elhelyezkedése a szervezetben. (Fundamentals of security operations centres. Concept, purpose, tasks, operational models, location in the organisation);

11.2. Az emberek, a folyamatok és a technológia hármasa a SOC szempontjából (The triad of people, processes and technology in the SOC perspective);

11.3. Szervezetek érettségi szintje**.** Érettségi modellek, szintek jellemzői, érettség mérése, fejlesztési lehetőségek (Maturity level of organisations. Maturity models, characteristics of levels, measurement of maturity, opportunities for improvement);

11.4. A biztonsági műveleti központok kialakítása. SOC igénybevétele szolgáltatásként; kialakítás a szervezeten belül, hibrid megoldás. Előnyök és hátrányok, kiválasztási szempontok, költség- és erőforrásigény (Design of security operations centres. Use of SOC as a service; design within the organisation, hybrid solution. Advantages and disadvantages, selection criteria, cost and resource requirements);

11.5. A biztonsági műveleti központok együttműködése. Információmegosztás, közös incidenskezelés, szervezeti és nemzetközi együttműködési formák (Cooperation between SOCs. Information sharing, joint incident management, organisational and international forms of cooperation);

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:

A hallgató köteles a foglalkozások legalább 70 %-án részt venni. A távollétet a hiányzást követő első foglalkozáson kell igazolnia. Hiányzás esetén a hallgató köteles a foglalkozások anyagát beszerezni, abból önállóan felkészülni.

14. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A tanulmányi munka alapja a gyakorlatok látogatása, az előírt olvasmányok ismerete. A hallgató a félév során egy feleletválasztós tesztet ír. A szorgalmi időszak végén egy vizsgafeladat gyakorlati megvalósítása. A félévközi feladatok összesítéséből áll a gyakorlati jegy. A TVSZ rendezi a sikertelen értékelés-összetevő javítását.

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 és a 14. pontban meghatározott félévközi feladatok legalább elégséges teljesítése.

15.2. Az értékelés:

A gyakorlati jegy a félévközi feleltválasztós teszt értékeléséből és a vizsgafeladatra adott érdemjegyekből adódik. Az elérendő teljesítmény százaléka mind a félévközi feleltválasztós teszt és a vizsgafeladat esetében: 60 %-tól elégséges, 70 %-tól közepes, 80-tól % jó, 90 %-tól jeles.

15.3. A kreditek megszerzésének feltételei:

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

16. Irodalomjegyzék:

16.1. Kötelező irodalom:

- Hámornik Balázs Péter: A Security Operations Center (SOC): A kiberbiztonsági csapatmunka és kihívásai. In: Hadmérnök, 13 évf. 2. sz., 393-408., 2018. ISSN: 1788-1919;
- Schinagl, Stef – Schoon, Keith – Paans, Ronald: 2015, A Framework for designing a

Security Operations Centre (SOC). In: Secure Cyberspace in 21st Century. Proceedings of the Hawaii International Conference on System Sciences (HICSS). Institute of Electrical and Electronics Engineers (IEEE), Hawai, Hawaii International Conference on System Sciences (HICSS), 8/01/15., 2015. ISSN: 1530-1605;
- SANS 2024 SOC Survey: Facing Top Challenges in Security Operations; URL: https://www.sans.org/white-papers/sans-2024-soc-survey-facing-top-challenges-security-operations/ (Online tananyag);
- Gubics Frigyes: SOC kialakítása projektmenedzsment segítségével és az üzemeltetés alapjai. In: Hadmérnök, 19. évf., 2. sz., 5-15., 2024. ISSN: 1788-1919;

16.2. Ajánlott irodalom:

- Magyar Sándor: A stratégiai gondolkodás szerepe a kiberbiztonságban, In: Stratégiák, Stratégiai Gondolkodás, Nemzetbiztonság, Ludovika Egyetemi Kiadó, Budapest, 2023. ISBN: 978-963-531-851-3;
- Hámornik Balázs Péter – Krasznay Csaba: 2017. "Prerequisites of Virtual Teamwork in Security Operations Centers: Knowledge, Skills, Abilities and Other Characteristics." Academic And Applied Research In Military And Public Management Science 16. évf., 3. sz., ISSN: 2498-5392;

Budapest, 2025. szeptember 16.

Dr. Magyar Sándor sk.
tanszékvezető, egyetemi docens, NKE HHK

12. TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** KVTIS1203
2. **A tantárgy megnevezése (magyarul):** Kríziskommunikáció
3. **A tantárgy megnevezése (angolul):** Crisis communication
4. **Kreditérték és képzési karakter:**
   4.1. 3 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, egyetemi docens, PhD.
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 a 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 stratégiáknak a válságok megelőzésében betöltött szerepével, eszközeivel, az esetleges krízisre felkészítő, szakszerűen megtervezett kommunikáció forgatókönyvével, illetve a már kialakult válság kezelésére szolgáló, a pánikot megelőzni képes kommunikáció professzionális megtervezésének jelentőségével, eszköztárával, alapszabályaival és a válságmédia működésével.

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

   The course aims to prepare students to recognize and analyze crises of different levels, sizes, types, identify causes, assess consequences, and understand the operating mechanisms of crisis warning systems. During the course, students will be introduced into the role and tools of adequate communication strategies in crisis prevention, the importance of professionally designed communication scenarios in preparing for a possible crisis, the tools and basic rules of professional communication design to prevent panic in the event of an emerging crisis, and the functioning of crisis media.
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 (The competence of crisis communication, the theoretical background and principles);
11.2. A kiberincidensek, a közvélemény és a média (Cyber incidents, the public opinion and the media);
11.3. A preventív kommunikáció jelentősége és lehetőségei (The importance and possibilities of preventive communication (pre-crisis communication);
11.4. Kommunikáció a kiberválságok aktív szakaszában, retorikai és esemény-közzétételi stratégiák (Responding, rhetorical and incidents-disclosure strategies);
11.5. A helyreállítás folyamatainak és eredményeinek kommunikációja (Communication on processes and results of the recovery);
11.1. A kommunikáció tervezésének szempontjai speciális területeken (hibrid válságok, megaválságok) (Communication planning aspects in specific areas (hybrid crises, mega-crises);
11.6. AI-támogatott megoldások és szcenárió alapú tréningek (AI-enabled solutions and scenario-based training);
11.7. Kutatási eredmények és esettanulmányok (Research results and 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 (rövid írásbeli beszámoló a mulasztott témakörből) 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 gyakorlati 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:

- Kaschner, Holger: Cyber Crisis Management. The Practical Handbook on Crisis Management and Crisis Communication. Springer, Berlin, 2021. ISBN: 978-3-658-35488-6;
- Max Boholm: Twenty-five years of cyber threats in the news: a study of Swedish newspaper coverage (1995–2019), Journal of Cybersecurity, Volume 7, Issue 1, 2021, tyab016, https://doi.org/10.1093/cybsec/tyab016;
- Coleman, Amanda: Crisis Communication Strategies. How to prepare in advance, respond effectively and recovery in full. Kogan Page, London–New York. 2020. ISBN: 978-1-78966-290-0;

Budapest, 2025. szeptember 16.

Dr. Kriskó Edina sk.
egyetemi docens, NKE ÁNTK

13. TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** KVTIS1204
2. **A tantárgy megnevezése (magyarul):** Kiberbiztonsági gyakorlatok
3. **A tantárgy megnevezése (angolul):** Cyberdefence exercises
4. **Kreditérték és képzési karakter:**
   - 4.1. 2 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. Magyar Sándor, tanszékvezető, egyetemi docens, PhD.
7. **A tanórák száma és típusa**
   - 7.1. össz óraszám/félév: 10 óra
   - 7.2. levelező munkarend: 10 óra (0 EA + 0 SZ + 10 GY (vagy 10 óra online gyakorlat, amennyiben az évfolyam létszáma indokolja))
8. **A tantárgy szakmai tartalma (magyarul):**

A tantárgy célja, hogy a hallgatók átfogó képet kapjanak a kibervédelmi gyakorlatok jelentőségéről és alkalmazási lehetőségeiről a kiberbiztonság fejlesztésében. A kurzus során megismerik a különféle gyakorlatok típusait, felépítését, céljait, valamint az ezekben betölthető szerepköröket. A hallgatók betekintést nyernek a nemzetközi (pl. NATO, EU) és hazai szintű gyakorlatok működésébe, és képet kapnak arról, hogyan tervezhetnek és valósíthatnak meg saját gyakorlatokat szervezeti környezetben. A tantárgy célja továbbá, hogy fejlessze a stratégiai gondolkodást és a koordinációs képességeket, különös tekintettel a Table Top Exercise típusú döntéshozói szimulációkra és a komplex, forgatókönyv-alapú gyakorlatokra.

A tantárgy szakmai tartalma (angolul):

The aim of the course is to provide students with a comprehensive overview of the importance and application possibilities of cyber defense exercises in the development of cyber security. During the course, students will learn about the different types of exercises, their structure, objectives, and the roles that can be played in them. Students will gain insight into the functioning of international (e.g., NATO, EU) and domestic exercises and learn how to plan and implement their own exercises in an organizational environment. The course also aims to develop strategic thinking and coordination skills, with a particular focus on Table Top Exercise-type decision-making simulations and complex, scenario-based exercises.

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 kártékony kódok fogalmát és hatásmechanizmusát.
- Tisztában van az állami kibervédelmi rendszerrel.
- Megérti a szervezeti feladatokat a kibervédelemben.

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 olyan technológiai védelmi intézkedések meghozatalára, amelyek a Cyber Kill Chain egyes elemeihez kapcsolódnak.
- 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.
- 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.

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.
- 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 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 the concept and mode of action of malware codes.
- 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 obtaining the support of leaders of the organisation in establishing regulatory compliance.
- He/He/She is capable of taking defensive measures that ensure the reduction of risk resulting from threat against humans.
- He/She is capable of taking technological defensive measures related to elements of the cyber kill chain.
- He/She is capable of understanding the current threats of cyberspace.
- 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 attention to and application of laws of cyber security in his/her work.
- His/Her personal attitude is characterized by an ability to treat internal employees as high risk and plans information security processes accordingly.
- 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 implement advanced knowledge

characterising cyber security on a national and international level.
- His/Her autonomy and responsibility are to process new and complex information, problems and phenomena in a systematic and critical way.
- His/Her personal attitude is characterized by an effort to design the cyber security management system in its own complexity.
- 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(magyarul, angolul - English):

11.1. A kibervédelmi gyakorlatok típusai, céljai, szerepkörei és alkalmazott környezetei (Types, objectives, roles, and environments of cyber defense exercises);

11.2. Nemzetközi szintű gyakorlatok a NATO, az EU és más szervezetek keretein belül (International exercises within the framework of NATO, the EU, and other organizations);

11.3. Szervezetek által önállóan megvalósítható gyakorlatok tervezése és lebonyolítása (Planning and conducting exercises that can be implemented independently by organizations);

11.4. Komplex szimulációk és forgatókönyvek szerepe a védekezési képességek fejlesztésében (The role of complex simulations and scenarios in developing defense capabilities);

11.5. Table Top Exercise gyakorlattípus végrehajtása (Implementation of Table Top Exercise);

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:

A hallgató köteles a foglalkozások legalább 70 %-án részt venni. A távollétet a hiányzást követő első foglalkozáson kell igazolnia. Hiányzás esetén a hallgató köteles a foglalkozások anyagát beszerezni, abból önállóan felkészülni.

14. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A tanulmányi munka alapja a gyakorlatok látogatása, az előírt olvasmányok ismerete. A hallgató a félév során egy feleletválasztós tesztet ír. A szorgalmi időszak végén egy vizsgafeladat gyakorlati megvalósítása. A félévközi feladatok összesítéséből áll a gyakorlati jegy. A TVSZ rendezi a sikertelen értékelés-összetevő javítását.

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 és a 14. pontban meghatározott félévközi feladatok legalább elégséges teljesítése.

15.2. Az értékelés:

A gyakorlati jegy a félévközi feleltválasztós teszt értékeléséből és a vizsgafeladatra adott érdemjegyekből adódik. Az elérendő teljesítmény százaléka mind a félévközi feleltválasztós teszt és a vizsgafeladat esetében: 60 %-tól elégséges, 70 %-tól közepes, 80-tól % jó, 90 %-tól jeles.

15.3. A kreditek megszerzésének feltételei:

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

16. Irodalomjegyzék:

16.1. Kötelező irodalom:

- Szabó András: Technikai kiberbiztonsági gyakorlatok–Nemzetközi kitekintés. In: Hadmérnök, 13.,1 sz., 2018. ISSN: 1788-1919;
- Debrecenine Deák Veronika. Prototípus-implementáció kibervédelmi technikák gyakorlati oktatására. In: Hadmérnök, 18. évf. 3. sz., 2023. ISSN: 1788-1919;

16.2. Ajánlott irodalom:

- Magyar Sándor – Szulcsányi, Viktor: The importance of cyber defense exercises to increase resilience, In: 1. Bilsel International Efes Scientific Researches And Innovation Congress, Bilgesina, 2023. pp. 607-615;

Budapest, 2025. szeptember 16.

Dr. Magyar Sándor sk.
tanszékvezető, egyetemi docens, NKE HHK

14. TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** KVTIS1205
2. **A tantárgy megnevezése (magyarul):** Információbiztonsági rendszerek auditja
3. **A tantárgy megnevezése (angolul):** Audit of information security systems
4. **Kreditérték és képzési karakter:**
   4.1. 5 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, habilitált egyetemi docens, PhD.
7. **A tanórák száma és típusa:**
   7.1. össz óraszám/félév: 20 óra
   7.2. levelező munkarend: 20 óra (10 EA (vagy 10 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):**

   A kurzus célja az információbiztonsági rendszerek auditálásának elméleti és gyakorlati alapjainak bemutatása, különös tekintettel a szabványos megfelelőség-ellenőrzési keretrendszerekre (pl. ISO/IEC 27001), a vonatkozó hazai és nemzetközi jogszabályi környezetre, valamint az auditálás folyamatának lépéseire. A hallgatók megismerik az információbiztonsági auditok típusait, a kockázatértékelés szerepét az auditfolyamatban, valamint az audit során alkalmazott módszertanokat, eszközöket és értékelési technikákat. A kurzus külön hangsúlyt fektet az információbiztonsági irányítási rendszerek (ISMS) vizsgálatára, a tanúsító auditok lefolytatására, a szabálytalanságok feltárására és a javító intézkedések meghatározására. Emellett részletesen foglalkozik a NIS2 irányelv és a 2024. évi LXIX. törvény szerinti auditkövetelményekkel. A hallgatók gyakorlati példákon keresztül sajátítják el az auditálás során alkalmazott dokumentációkészítési feladatokat, interjútechnikákat és a helyszíni ellenőrzés lépéseit.

   A tantárgy szakmai tartalma (angolul):

   The aim of the course is to present the theoretical and practical foundations of auditing information security systems, with a particular focus on standardized compliance assessment frameworks (e.g., ISO/IEC 27001), the relevant national and international legal environment, and the steps involved in the auditing process. Students will become familiar with the different types of information security audits, the role of risk assessment in the audit process, as well as the methodologies, tools, and evaluation techniques applied during audits. The course places special emphasis on the examination of Information Security Management Systems (ISMS), the conduct of certification audits, the identification of non-conformities, and the definition of corrective actions. In addition, it addresses in detail the audit requirements under the NIS2 Directive and the Hungarian Act LXIX of 2024. Through practical examples, students will learn the key aspects of documentation, interview techniques, and on-site inspection methods used during auditing.

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.
- Megérti a szervezeti feladatokat a kibervédelemben.

Képességei
- Képes értelmezni a jogszabályokból eredő követelményeket.
- Képes megszerezni a szervezet vezetőinek támogatását a jogszabályi megfelelőség kiépítéséhez.
- 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.
- A maga komplexitásában tervezi meg az információbiztonsági irányítási rendszert.
- Hatékony lépéseket tesz a kibertámadások megelőzése érdekében, így csökkentve a szervezete kitettségét.

Autonómiája és felelőssége
- Tudatosan törekszik a kiberbiztonság sajátosságainak megfelelő, korszerű ismeretek hazai és nemzetközi szinten történő gyakorlati alkalmazására.
- Önállóan dolgozza fel az új és összetett információkat, problémákat, illetve jelenségeket, rendszerszerű és kritikus módon.
- Felelősséget vállal a kiberbiztonság összefüggő ismeretének és a meghatározó jogi, szabályozási és gazdasági összefüggések ismeretének alapján a szakmai javaslatok kidolgozásában.
- Gyakorlatába beépíti és alkalmazza az e szakterületen folyó kutatások eredményeit.

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.
- He/She is familiar with organisational tasks in cybersecurity.

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

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 process new and complex information, problems and phenomena in a systematic and critical way.
- He/She is responsible 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(magyarul, angolul - English):

11.1. Az információbiztonsági audit célja, szerepe és főbb típusai (Purpose, role and main types of information security audits);

11.2. Az auditok jogszabályi és szabványos környezete, különös tekintettel a 2024. évi LXIX. törvényre (Legal and standards environment of audits, with special emphasis on Act LXIX of 2024);

11.3. Az auditfolyamat lépései I.: tervezés, előkészítés, kockázatalapú megközelítés (Audit process steps I: planning, preparation, risk-based approach);

11.4. Az auditfolyamat lépései II.: végrehajtás, helyszíni vizsgálat, interjúk (Audit process steps II: execution, on-site examination, interviews);

11.5. Az auditfolyamat lépései III.: jelentéskészítés, nemmegfelelőségek kezelése (Audit process steps III: reporting, handling of non-conformities)

11.6. Javító és megelőző intézkedések meghatározása és nyomon követése (Definition and follow-up of corrective and preventive actions);

11.7. A belső auditok szerepe és lefolytatása a gyakorlatban (Role and execution of internal audits in practice);

11.8. Az ISO/IEC 27001 szabvány és más nemzetközi keretrendszerek áttekintése (Overview of ISO/IEC 27001 and other international frameworks);

11.9. A hatósági megfelelés értelmezése a 2024. évi LXIX. törvény szerint (Understanding regulatory compliance under Act LXIX of 2024);

11.10. Esettanulmány és szimuláció: auditálási gyakorlat csoportmunkában (Case study and simulation: audit practice in group work);

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:

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

14. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A hallgatók minden előadáshoz kapcsolódóan egyénileg feldolgozandó szakanyagot kapnak, melynek ellenőrzése a következő előadás elején történik, 10 kérdéses online teszt formájában (pl. Kahoot rendszerben). A félév végén ezek a pontszámok összesítésre kerülnek, és a féléves jegy részét képezik.

Emellett a hallgatók személyre szabott feladatot kapnak, amelynek keretében egy fiktív szervezet NIS2-irányelv szerinti információbiztonsági auditjára készítenek elő egy audit-tervet. A dokumentum benyújtható írásban vagy videó formátumban. Az írásos leadás esetén kötelező a kulcselemekhez saját reflexiókat (magyarázat, kritika, alternatíva) fűzni. A hallgatóknak szükséges jelezni, ha generatív mesterséges intelligenciát használtak a

szöveg előállításához, és az így készült részeket röviden kommentálniuk kell.

A félév során a hallgatók minden előadás elején 10 kérdéses online tesztet töltenek ki, amelyek eredményei összeadódnak és az érdemjegy 50%-át adják. A fennmaradó 50%-ot egy egyéni auditterv elkészítése adja, amely egy fiktív szervezet NIS2-megfelelőségét vizsgálja.

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:

Az értékelés a hallgató által a félév során elért pontok alapján a következő módon történik:

0-50% = elégtelen (1)

51%-62% = elégséges (2)

63%-74% = közepes (3)

75%- 86% = jó (4)

87%-100% = jeles (5)

15.3. A kreditek megszerzésének feltételei:

A kreditek megszerzésének feltétele az aláírás megszerzése és legalább elégséges gyakorlati jegy (GYJ).

16. Irodalomjegyzék:

16.1. Kötelező irodalom:

- Muha Lajos, Krasznay Csaba: Az elektronikus információs rendszerek biztonságának menedzselése, Budapest, 2018, Nemzeti Közszolgálati Egyetem, ISBN 978-615-5870-27-9;
- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról;

16.2. Ajánlott irodalom:

- Nemzeti Kibervédelmi Intézet – Kézikönyvek és audit segédanyagok;

Budapest, 2025. szeptember 16.

Dr. Krasznay Csaba sk.
habilitált egyetemi docens, NKE ÁNTK

15. TANTÁRGYI PROGRAM

1. **A tantárgy kódja:** KVTIS1206
2. **A tantárgy megnevezése (magyarul):** Hatósági megfelelés támogatása
3. **A tantárgy megnevezése (angolul):** Assistance for compliance with public authorities
4. **Kreditérték és képzési karakter:**
   - 4.1. 2 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. Bányász Péter, egyetemi docens, PhD.
7. **A tanórák száma és típusa:**
   - 7.1. össz óraszám/félév: 10 óra
   - 7.2. levelező munkarend: 10 óra (0 EA/L + 0 SZ/S + 10 GY/P (vagy 10 óra online gyakorlat, amennyiben az évfolyam létszáma indokolja))
8. **A tantárgy szakmai tartalma (magyarul):**

A tantárgy célja, hogy gyakorlati példákon keresztül mutassa be a kiberbiztonsági és adatvédelmi hatóságokkal való együttműködés legfontosabb aspektusait. A hallgatók megismerik a Nemzeti Kiberbiztonsági Hatóság, az adatvédelmi hatóság, valamint az incidenskezelésért felelős szervek elvárásait, az ügyfelek feladatait, a bejelentési kötelezettségeket és a leggyakoribb megfelelési hibákat. A kurzus gyakorlatorientált megközelítése segíti a hallgatókat a hatósági megfelelés és incidensbejelentés szabályainak elsajátításában, különböző szervezeti kontextusokban.

A tantárgy szakmai tartalma (angolul):…

The course aims to provide practical insights into cooperation with cybersecurity and data protection authorities. Students will learn about the responsibilities of clients interacting with the National Cybersecurity Authority, the Data Protection Authority, and the body responsible for incident reporting. The course covers key compliance obligations, common regulatory failures, and the procedures for reporting incidents. Through real-life examples and a practice-oriented approach, students will gain essential knowledge to support regulatory compliance and incident management across different organizational contexts.

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(magyarul, angolul - English):

11.1. Nemzeti Kiberbiztonsági Hatóság ügyfeleinek feladatai (Responsibilities of clients of the National Cybersecurity Authority);

11.2. Ügyfélkötelezettségek és tipikus megfelelési hibák a kiberbiztonsági hatósági gyakorlatban (Client obligations and common compliance failures in cybersecurity regulatory practice);

11.3. Az adatvédelmi incidens kockázati besorolása, kockázatcsökkentő intézkedések, gyakorlati példák és jogesetek (Risk classification of data protection incidents, risk mitigation measures, practical examples and legal cases);

11.4. Az adatvédelmi incidens bejelentése, a kapcsolódó hatósági eljárások (Reporting of data protection incidents, and related regulatory procedures);

11.5. Az adatvédelmi incidens nyilvántartása, az érintettek tájékoztatása, az incidenst követő lépések (Documentation of data protection incidents, informing data subjects, and follow-up actions);

11.6. Hatóság által elvárt kötelezettségek (Compliance obligations defined by the Authority);

11.7. Audit módszertan, felügyeleti díj (Methodology of regulatory audits and the supervisory fee);

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:

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

14. Félévközi feladatok, ismeretek ellenőrzésének rendje:

A hallgató értékelése a szorgalmi időszakban egy gyakorlati feladat 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: gyakorlati projektfeladat megoldása, amelynek során egy elképzelt kiberbiztonsági incidens különböző szempontú megoldására kell javaslatot tennie a vizsgázónak, felhasználva a gyakorlati foglalkozásokon elsajátított ismereteket.

15.3. A kreditek megszerzésének feltételei:

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

16. Irodalomjegyzék:

16.1. Kötelező irodalom:

- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról és kapcsolódó végrehajtási rendeletei;
- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről;

16.2. Ajánlott irodalom:

- Sziklay Júlia – Bendik Tamás: Az adatvédelem hazai és európai uniós szabályozása és alapintézményei. Negyedik, hatályosított kiadás, Nemzeti Közszolgálati Egyetem, Budapest, 2018. ISBN: 978-615-5870-98-9;
- Európai Adatvédelmi Hatóság: Iránymutatás az adatvédelmi incidensek GDPR-rendelet szerinti bejelentéséről – 2.0 verzió. URL: https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202209_personal_data_breach_notification_v2.0_hu.pdf (Online tananyag);
- Európai Adatvédelmi Testület 01/2021. számú iránymutatás az adatvédelmi incidensek bejelentésével kapcsolatos példákról – 2.0 verzió. URL: https://www.edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_hu.pdf (Online tananyag);

Budapest, 2025. szeptember 16.

Dr. Bányász Péter sk.
egyetemi docens, NKE ÁNTK