NEMZETI KÖZSZOLGÁLATI EGYETEM
ÁLLAMTUDOMÁNYI ÉS NEMZETKÖZI TANULMÁNYOK KAR

Nyilvántartási szám: …
… számú példány

A KIBERBIZTONSÁGI MESTERKÉPZÉSI SZAK AJÁNLOTT TANTERVE

Alkalmazandó:
a 2024/2025 **tanévtől felmenő rendszerben**

Szenátusi döntés	**Fenntartói döntés**
Elfogadta a Szenátus számú határozatával.	Jóváhagyta a Fenntartó számú határozatával.

Budapest, 2024.

A szakfelelős: Dr. Krasznay Csaba, PhD, egyetemi docens

A szakirányok/specializációk felelősei

Az ajánlott tanterv jogi hátterét az alábbi főbb jogszabályok és egyetemi szabályzatok képezik:

1. A nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény;
2. A Nemzeti Közszolgálati Egyetemről, valamint a közigazgatási, rendészeti és katonai felsőoktatásról szóló 2011. évi CXXXII törvény;
3. A nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény egyes rendelkezéseinek végrehajtásáról szóló 87/2015. (IV. 9.) Korm. rendelet;
4. A Nemzeti Közszolgálati Egyetemről, valamint a közigazgatási, rendészeti és katonai felsőoktatásról szóló 2011. évi CXXXII. törvény egyes rendelkezéseinek végrehajtásáról szóló 363/2011. (XII.30.) Korm. rendelet;
5. A felsőoktatásban szerezhető képesítések jegyzékéről és az új képzések létesítéséről szóló 65/2021. (XII. 29.) ITM rendelet, valamint a felsőoktatási szakképzések, az alap- és mesterképzések képzési és kimeneti követelményeiről szóló vonatkozó miniszteri közlemény;*
6. Az államtudományi képzési terület képzéseiről szóló 534/2023. (XII. 5.) Korm. rendelet (államtudományi képzési területhez tartozó képzés esetén); **
7. A Nemzeti Közszolgálati Egyetem Tanulmányi és Vizsgaszabályzata;
8. A képzésekkel kapcsolatos eljárásrendről szóló rektori utasítás.

A képzés hitelesítő adatai

Kari Tanács határozatának száma:	61-2018. (V.4.) sz. határozat
Szenátusi határozat száma:	
Fenntartói határozat száma:	
MAB kód:	Ms1839
MAB határozat száma:	MAB 2019/5/VI/7.
OH nyilvántartásba vételi szám:	FNYF/329-10/2019.
A képzés FIR kódja:	MSZKKIZ
A meghirdetés első tanéve:	2024/2025

*nem államtudományi képzési területhez tartozó képzés esetén
**államtudományi képzési területhez tartozó képzés esetén

Tartalomjegyzék

1. **A szak megnevezése:**
   kiberbiztonsági mesterképzési szak
2. **Képzési terület, az NKE tv. 3. §-ában meghatározott felsőoktatási terület**
   államtudományi képzési terület, államtudományi és közigazgatási felsőoktatás
3. **A szak szakirányai/specializációi:**
   -
4. **Végzettségi szint:**
   mesterfokozat (magister, master of arts, rövidítve: MA)
5. **A szakon szerezhető szakképzettség oklevélben szereplő megnevezése:**
   okleveles kiberbiztonsági szakértő
6. **A képzés célja és az elsajátítandó szakmai kompetenciák:**

A képzés célja olyan felsőfokú végzettséggel rendelkező szakemberek felkészítése, akik a

közigazgatás, a védelmi igazgatás, a külügyi igazgatás területeihez tartozó szervezeteknél vezetői és szakértői munkakörökben képesek a kiberbiztonsági feladatok tervezését, szervezését és irányítását eredményesen végrehajtani. A mesterképzés azokra a kiberbiztonsági kérdésekre, aktuális és jövőbeli kihívásokra fókuszál, amelyekkel az állami és a magánszférának, illetve a társadalomnak egyaránt szembe kell néznie. A hallgatók széles körű ismereteket szereznek a kiberbiztonság elméleti és gyakorlati oldaláról, biztonsági, környezeti, társadalmi és gazdasági aspektusairól. A differenciált szakmai tananyag elsajátítása során (nemzetközi kapcsolatok a kiberbiztonságban, közszolgálati kiberbiztonság-menedzsment, létfontosságú elektronikus információs rendszerek védelme) alkalmassá válnak szakterületüknek megfelelően kutatási, fejlesztési és tervezési feladatok ellátására, védelmi problémakörök tudományos igényű elemzésére és következtetések kialakítására.Az államtudományi képzési terület közös szakmai kompetenciái mesterképzésben:Tudás:– Ismeri szakterülete átfogó tárgykörének általános és specifikus jellemzőit, legfontosabb irányait és pontosan kidolgozott határait, a terület legfontosabb összefüggéseit, elméleteit és az ezeket felépítő terminológiát, a szakterületnek a rokon szakterületekhez való kapcsolódását.– Ismeri szakterületének sajátos ismeretszerzési és probléma-megoldási módszereit, absztrakciós technikáit, az elvi kérdések gyakorlati vonatkozásainak kidolgozási módjait.– Szakterületéhez kapcsolódóan ismeri az alapvető környezeti erőforrások használata és a társadalmi-gazdasági folyamatok közötti összefüggéseket.– Ismeri a közszolgálatban a saját szakterületén rendszeresített digitális technológiákat és a velük történő kommunikáció módját, továbbá ismeri az adott környezethez megfelelő digitális kommunikációs eszközöket.– Rendelkezik a szakterületére jellemző szaknyelvi ismeretekkel legalább egy idegen nyelven.Képesség:– Képes arra, hogy a kellő szakmai elhivatottság birtokában és a közszolgálati életpályán elvárt szakmai és emberi standardok szerint szolgálja a közjót és a köz érdekét.– Átfogó megközelítéssel, komplex problémakezelési képességekkel rendelkezik, képes a nagyfokú információfeldolgozásra.– Képesség az újszerű problémamegoldásokat támogató rendszergondolkodásra, a változásra és annak tervezésére.– Megfelelően alkalmazza a közszolgálatban a saját szakterületén rendszeresített digitális technológiákat. Képes az IKT-rendszerek használata során a megfelelő biztonsági előírások és szabályok alkalmazására, betartására.– Legalább egy idegen nyelvet képes megfelelően alkalmazni szakterületén.Attitűd:– Elkötelezett a közszolgálat iránt, felismeri a közszolgálati hivatásrenddel járó felelősséget, és hitelesen képviseli annak szellemiségét.– Elkötelezett a demokratikus értékek és a jogállamiság, a fenntarthatóság, a társadalmi szolidaritás és az esélyegyenlőség mellett.– Fejlett szakmai identitással, hivatástudattal rendelkezik, amelyet a szakmai és szélesebb társadalmi közösség felé is vállal.– Szakmai álláspontjának képviseletével bátran és felelősségteljesen vesz részt munkaszervezetének működtetésében, a szakmai koncepciók kidolgozásában, megvitatásában és megvalósításában.– Felelősségteljesen építi fel szakmai karrierjét, és támogatja az általa irányított munkatársak szakmai életpályájának kibontakoztatását.– Szakmai érdeklődése elmélyül, megszilárdul, önképzése folyamatos, szemléletmódja révén nyitott az újdonságokra és azok elemző módon történő befogadására, valamint naprakészen követi és munkája során alkalmazza a jogszabályi változásokat. Elkötelezett a szakterület módszertanának fejlesztéséhez szükséges elméleti, tudományos kutatási és gyakorlati információk beszerzése, értékelése és hasznosítása iránt.– Munkavégzése során a szakmai normákban meghatározottak szerint jár el, továbbá elkötelezett a hatályos jogszabályok és erkölcsi normák teljeskörű figyelembevételével történő döntéshozatal iránt.– Rendelkezik azokkal a személyiségjegyekkel – önálló gondolkodás, problémafelismerés, felelősségtudat, mérlegelési és döntési képesség –, amelyek alkalmassá teszik a vezetői feladatok ellátására.– A munkakörével kapcsolatos problémák megoldása során törekszik a kezdeményezésre, személyes felelősségvállalásra és helyes döntés meghozatalára. Szakmai hivatástudatából adódóan elkötelezett a minőségi munkavégzés iránt.– Munkavégzése során önmagával szemben is kritikus és nyitott a megalapozott kritikai észrevételekre, amely szakmai értékrendjét tovább fejleszti.– A közös munkában eredményre és közösségi konszenzusra törekszik.Autonómia és felelősség:– Felelősséget vállal a munkájával és a magatartásával kapcsolatos szakmai, jogi és etikai normák és szabályok betartása terén.– Hatáskörén belül önállóan képes a beosztásából és munkaköréből fakadó javaslatok megtételére, a feladatok kijelölésére és végrehajtásuk előkészítésére és irányítására.–

Jelentős mértékű önállósággal rendelkezik átfogó és speciális szakmai kérdések kidolgozásában, szakmai nézetek képviseletében, indoklásában.– Önálló kezdeményező döntéshozatali képességgel, illetve személyes felelősségvállalással rendelkezik a döntések környezeti és társadalmi hatásaiért a szakmai feladatok teljesítésének megtervezése és végrehajtása során.– Felelős a szervezetében a feladatok megosztásáért, a szervezeti működésért, eredményességért, a vezetői utasítások kiadásáért, az önálló vezető-irányító munka végzéséért és a hatékony munkavégzésért egyéni és szervezeti szinten.– Felelősséget vállal a szakterületéhez tartozó szakmai együttműködés eredményességéért, elfogadja annak kereteit, valamint a rá háruló szerepeket, funkciókat és a kooperációból származó felelősséget.Az államtudományi és közigazgatási felsőoktatás közös szakmai kompetenciái mesterképzésben:Tudás:– Részleteiben ismeri a közigazgatás területén alkalmazott jogszabályok megalkotásával kapcsolatos eljárásokat, azok folyamatait, továbbá ismeri a szakterületén alkalmazott jogszabályok összefüggéseit.Képesség:– Változatos munkakörnyezetben képes önállóan vagy csapatban átfogó és komplex feladatokat elvégezni.– Képes kiemelkedő szervezői, koordinációs feladatok végrehajtására, konfliktuselemzésre és konfliktuskezelésre.– Információs rendszereket integrált és biztonságos módon alkalmaz.Attitűd:– Közigazgatási munkavégzés esetén elkötelezett az adott szervezet céljai és érdekei mellett.Autonómia és felelősség:– Közhatalmi tevékenysége során mások munkáját értékeli, javaslatokat tesz, és önellenőrzésre képes.A kiberbiztonsági mesterképzésen elsajátítandó szakmai kompetenciák:Tudás:– Ismeri azokat a fontosabb előírásokat a kiberbiztonsággal kapcsolatos hazai és nemzetközi szabályozásokból, amelyek a mindennapi munkáját befolyásolják.– Ismeri a nemzetközi jog alkalmazhatóságát a kibertérben.– 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 a nyomozóhatóság feladataival az egyes állami szervezetek, vállalatok és intézményeket érő támadások esetén.– Átlátja a kibertérrel kapcsolatos diplomáciai, illetve politikai információmegosztás folyamatát, valamint az esetleges válaszlépéseket.– Tisztában van az információmegosztás folyamatával bűncselekmény felmerülése esetén. Ismeri a fedett környezetből történő információgyűjtés eljárásait.– 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.Képesség:– Képes értelmezni a jogszabályokból eredő követelményeket.– Képes megszerezni a szervezet vezetőinek támogatását a jogszabályi megfelelőség kiépítéséhez.– Képes átlátni a kibertér speciális jogállását.– Képes a szükséges mértékben alkalmazni a kibertérre vonatkozó nemzetközi jogot kibertámadások esetén.– 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 együttműködni a nyomozóhatósággal a kiberbiztonsági eseményeket érintő nyomozások során.– Képes a szervezeténél keletkezett információkat oly módon megosztani külső szereplővel, hogy az ne sértse saját szervezetének érdekét, de hatékonyan tudja támogatni a külső felet.– Képes a keletkezett információk megosztásának szükségességével kapcsolatban komplex következtetések levonására.– Képes átlátni a kibertér aktuális fenyegetéseit.– Képes támogatni szervezetét a kibervédelmi képességek kialakításában.– Képes megfelelően támogatni szervezetét és a külső feleket egy kibertámadás kezelésében.Attitűd:– Megérti és elfogadja a nemzetközi kiberjog komplexitását, ennek köszönhetően a munkája során törekszik ennek a komplexitásnak a kezelésére.– 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.– Szükség esetén támogatja a külső feleket a szervezeténél keletkezett információk megosztásával.– Partner abban, hogy se a szervezete, se ő maga ne váljon kibertámadás áldozatává.Autonómia és

felelősség:– Tudatosan törekszik a kiberbiztonság sajátosságainak megfelelő, korszerű ismeretek hazai és nemzetközi szinten történő gyakorlati alkalmazására.– Kezdeményező módon lép fel az alternatív, eredeti megoldások kidolgozásában, bemutatásában és a bonyolult, nem tipikus helyzetekben történő adekvát döntések meghozatalában.– Vállalja a szakterület, a szakmai praxis módszertanának fejlesztéséhez szükséges elméleti, tudományos kutatási és gyakorlati információk beszerzésének, értékelésének és hasznosításának végrehajtását.– Felelősséget vállal a kiberbiztonság összefüggő ismeretének és a meghatározó jogi, szabályozási és gazdasági összefüggések ismeretének alapján a szakmai javaslatok kidolgozásában.– Értékkötelezett módon vesz részt a kibertér komplexitásának és kölcsönhatásainak ismerete által a különböző hivatásrendek feladatainak szervezésében.– Önállóan és pontosan vesz részt a kiberbiztonsági fenyegetések technológiai, politikai és adminisztratív megoldásában.– Vállalja a kiberbiztonsági fenyegetések kezelésének felelősségét.

7. A képzés időtényezői:

A képzési idő félévekben:
4 félév

A képzési idő részletezése:

A fokozat megszerzéséhez összegyűjtendő kreditek száma	120 kredit
Összes hallgatói tanulmányi munkaóra	3600
Hallgatói munkamennyiség kreditben egy tanulmányi félévben (átlagos kreditszám):	30 kredit
Egy tanulmányi félévben a tanórák száma nappali munkarendben	átlagosan 301 tanóra
A heti tanórák jellemző száma nappali munkarendben	átlagosan 21.5 tanóra, ebből a kredithez rendelt tanórák száma átlagosan: 21.5 tanóra
Egy tanulmányi félévben a tanórák száma levelező munkarendben (átlagos tanóraszám)	átlagosan 86 tanóra
Szakmai gyakorlat(ok) időtartama:	10 hét

8. A képzés felépítése

8.1. A szakdolgozat vagy diplomamunka elkészítéséhez rendelt kreditek száma:
20

8.2. Szakmai gyakorlati képzéshez rendelt kreditek száma:
0

8.3. A szakirány elvégzésével összegyűjtendő kreditek minimális száma:
-

9. A tanóra-, kredit- és vizsgaterv

A tanóra-, kredit- és vizsgaterv tartalmazza oktatási időszakonkénti bontásban az összes tantárgy (kritériumkövetelmény – a továbbiakban együtt: tantárgy) vonatkozásábana) a tantárgyak Neptun-kódját,b) a tantárgyak jellegét (kötelező, kötelezően választható, szabadon választható, kritériumkövetelmény),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 rövidítésekA tanóra-, kredit- és vizsgatervet az 1. számú melléklet tartalmazza.

10. Az előtanulmányi rend

A tanterv határozza meg, hogy az egyes tantárgyak felvételéhez milyen más tantárgyak előzetes vagy egyidejű teljesítése szükséges (előtanulmányi rend). Az előtanulmányi rendet a 2. számú melléklet tartalmazza.

11. 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.Kredittel nem rendelkező kritériumkövetelmény esetén annak teljesítésének feltétele önmagában az aláírás is lehet.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- projektfeladat: PF- alapvizsga: AV- szigorlat: SZG- komplex vizsga: KV- záróvizsga: ZVAz 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 12. pontjahatározzák meg.

12. A záróvizsga

12.1. A záróvizsgára bocsátás feltételei

A záróvizsgára bocsátás feltételei:- az abszolutórium (végbizonyítvány megszerzése): a tantervben előírt vizsgák eredményes letételét és – a szakdolgozat (diplomamunka) elkészítésének kivételével – más tanulmányi követelmények teljesítését, illetve a képzési és kimeneti követelményekben előírt kreditpontok megszerzését igazolja, amely minősítés és értékelés nélkül tanúsítja, hogy a hallgató a tantervben előírt tanulmányi és vizsgakövetelménynek mindenben eleget tett- a bírálaton részt vett szakdolgozat/diplomamunka

12.2. A záróvizsga részei

A záróvizsga a tantervben meghatározottak szerint több részből áll:- diplomamunka megvédése- szóbeli vizsga a Kockázatértékelés, kockázatmenedzsment (ÁKIBTM007) és a Számítógép hálózatok (HKHIRA83) tárgyak anyagából- gyakorlati vizsga egy kiberbiztonsági esemény komplex kezelésének a gyakorlatából

12.3. A záróvizsga eredménye

A záróvizsga érdemjegyét a kapott osztályzatok számtani átlaga adja. Bármelyik elem vizsgatételére kapott elégtelen osztályzat esetében a záróvizsga értékelése elégtelen. A több elemből álló záróvizsga esetén az egyes elemeket külön érdemjeggyel kell értékelni.A záróvizsga eredményét a részeredményeinek egyszerű átlaga képezi, az alábbiak szerint:ZvÖ = (SzD + Zv + Gy) / 3Azaz a záróvizsga összesített eredménye a szakdolgozatra adott egy osztályzat, a záróvizsga szóbeli részére (a több elemből álló záróvizsga esetén az elemek értékelésének egész számra kerekített átlaga) adott egy osztályzat és a gyakorlati feladat végrehajtására adott egy osztályzat összegének egyszerű átlaga.

13. A szakdolgozat/diplomamunka

A szakdolgozat/diplomamunka elkészítésének rendjét, tartalmi és formai követelményeit egyebekben a Tanulmányi és Vizsgaszabályzat határozza meg.

A szakdolgozat/diplomamunka tantárgya(i):
- ÁKIBERM001, Diplomamunka-tervezés 1., 10 kredit;
- ÁKIBERM002, Diplomamunka-tervezés 2., 10 kredit;

14. Az oklevél

14.1. Az oklevél kiadásának feltétele

Az oklevél kiadásának feltétele az eredményes záróvizsga.

14.2. Az oklevél minősítésének megállapítása

Az oklevél minősítését az alábbiak egyszerű átlaga adja meg:a) a diplomamunka védésére adott osztályzat;b) a záróvizsga szóbeli részére adott (több elemből álló vizsga esetén az elemekre adott osztályzatok átlaga egész számra kerekítve) egy osztályzat;c) a gyakorlati záróvizsgára adott osztályzat;d) a teljesített félévek (két tizedesig kifejezett) súlyozott tanulmányi átlagainak átlaga:(SZD + ZV + GY + (Á1+…+Án)/n) / 4Az oklevél minősítésének megállapítása az alábbi határértékek figyelembevételével történik, ha a fenti módszer alapján számított érték:a) kitűnő, ha az átlag 5,00b) jeles, ha az átlag 4,51-4,99c) jó, ha az átlag 3,51-4,50d) közepes, ha az átlag 2,51-3,50e) elégséges, ha az átlag legalább 2,00 – de legfeljebb 2,50.(5) 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.

15. A szakmai gyakorlat

A hallgatónak kötelező egy legalább 10 hetes időtartamú egybefüggő szakmai gyakorlatot teljesíteni. A szakmai gyakorlat a képzési és kimeneti követelmények, valamint az ajánlott tanterv rendelkezése szerint tantárgy vagy kritériumkövetelmény, teljesítése hiányában a hallgató abszolutóriumot nem kaphat.A szakmai gyakorlat egy olyan tanulási folyamat, amely egyszerre gyakorol hatást a hallgató tanulási és karriercéljaira. A szakmai gyakorlat során a hallgató megismeri a választott szervezet felépítését, működési mechanizmusát és beágyazottságát, illetve a mindennapi munkafolyamatokat. A szakmai gyakorlat célja, hogy a hallgató a képzés során megszerzett elméleti és gyakorlati ismereteket alkalmazza és munkatapasztalatok révén azokat elmélyítse. A hallgató a szakmai gyakorlat zárásaként rövid összefoglalót készít a szervezetnél szerzett tapasztalatokról, elvégzett feladatokról, amelyet csatol a szervezeti egység vezetője, vagy a szakmai gyakorlatot felügyelő személy által aláírt szakmai gyakorlati igazoláshoz.Szakmai gyakorlat végrehajtására az egyetemmel együttműködési megállapodást kötött szakmai gyakorlati helyen, kifejezetten kiberbiztonsággal foglalkozó szakmai környezetben van lehetőség. A szakmai gyakorlat végrehajtásáról a választott szervezet és a hallgató együttműködési megállapodást, szükség esetén hallgatói munkaszerződést köt. Amennyiben az egyetem a választott szakmai gyakorlati hellyel korábban együttműködési keretmegállapodást kötött, a hallgatónak elegendő a szakmai gyakorlati hely képviselője által aláírt befogadó nyilatkozatot leadnia a kar szakmai gyakorlati referensénél.A szakmai gyakorlat teljesítése a „szakmai gyakorlat” tárgy felvételével és a megfelelően kiállított teljesítési igazolással dokumentálandó. A szakmai gyakorlat teljesítéséről részletes értékeléssel ellátott igazolás készül, amelyet a hallgató a szakmai gyakorlat lejárta után az Oktatásszervezési Osztályon ad le. A szakmai gyakorlat folyamán a szakmai gyakorlati hely döntése alapján munkanapló vezethető.A szakmai gyakorlat tantárgya:ÁKIBERMSZGY001, Szakmai gyakorlat (10 hét), 0 kredit

16. A külföldi részképzés céljából nemzetközi hallgatói mobilitásra felhasználható időszak (mobilitási ablak)

Az Erasmus+ program lehetőséged ad a mesterképzésben résztvevő hallgatóknak, hogy tanulmányi mobilitási, illetve szakmai gyakorlati ösztöndíjban részesüljenek.A tanulmányi mobilitás lehetővé teszi, hogy a pályázatot elnyert hallgatók egy félévet az Egyetem valamely partnerintézményénél töltsenek, és az ott megszerzett krediteket beszámíttassák itthoni tanulmányaikba. Az ún. csereprogram révén a hallgatók tandíjmentesen tanulhatnak az adott intézményben.A pályázók az EU országaiba, illetve Izlandra, Lichtensteinbe, Norvégiába, illetve Törökországba, Szerbiába és Észak-Macedóniába utazhatnak, azokba az intézményekbe, amelyekkel az Egyetem intézményközi szerződést kötött. A választható Egyetemek listája az egyetem honlapján elérhető. A nemzetközi kreditmobilitás (Európán kívüli országok) keretein belül az Egyetem tanévenként és pályázati ciklusonként változó térségbeli partnerintézményekkel biztosít kapcsolatokat.A Kar által az egyes partnerintézményekkel kötött kétoldalú megállapodások száma folyamatosan növekszik. A képzés célkitűzéseiből adódóan a Kar ösztönzi a hallgatókat a nemzetközi mobilitásban történő részvételre. A külföldi tanulmányokat folytató hallgatók részére kedvezményes tanulmányi rendet biztosít, valamint a Kari Kreditátviteli és Validációs Bizottság széles körben fogadja be a külföldön teljesített tárgyakat a kötelező, vagy a szabadon választható tárgyak körébe.A képzés felépítéséből eredően a 3. szemeszter lehet alkalmas külföldi tanulmányok folytatására.

17. További szakspecifikus követelmények

17.1. Szakirányválasztás feltételei

-

17.2. Szigorlat/alapvizsga/komplex vizsga

-

17.3. Kritériumkövetelmények

Ludovika Fesztivál Szabadegyetem

17.4. A mesterképzésbe történő felvételkor hiányzó kreditek megszerzésének feltételei

17.4.1. A mesterképzésbe történő belépésnél előzményként elfogadott szakok- Teljes kreditérték beszámításával vehető figyelembe: -- A 17.4.2. pontban meghatározott kreditek teljesítésével elsősorban számításba vehető: az államtudományi osztatlan mesterképzési szak, a bűnügyi igazgatási, a gazdaságinformatikus, a had- és biztonságtechnikai mérnöki, a katasztrófavédelem, a katonai gazdálkodási, a katonai logisztika, a katonai üzemeltetés, a katonai vezetői, a közigazgatás-szervező, a mérnök informatikus, a nemzetbiztonsági, a nemzetközi biztonság- és védelempolitikai, a biztonság- és védelempolitikai, a nemzetközi igazgatási, a polgári nemzetbiztonsági, a programtervező informatikus és a rendészeti igazgatási alapképzési szak.- A 17.4.2. pontban meghatározott kreditek teljesítésével vehetők figyelembe továbbá azok az alapképzési és mesterképzési szakok, illetve a felsőoktatásról szóló 1993. évi LXXX. törvény szerinti szakok, amelyeket a kredit megállapításának alapjául szolgáló ismeretek összevetése alapján a felsőoktatási intézmény kreditátviteli bizottsága elfogad.17.4.2. A 17.4.1. pontban megadott oklevéllel rendelkezők

esetén a mesterképzési képzési ciklusba való belépés minimális feltételei:A mesterképzésbe való belépéshez a korábbi tanulmányokból szükséges minimális kreditek száma 60 kredit az alábbi területekről:- informatikai ismeretek (30 kredit): a szoftvertechnológia, a rendszertechnika és az adatbázisok és információs rendszerek ismeretkörei, kriptográfia alkalmazása, számítógépek architektúrája és számítógépes hálózatok témakörei;- államtudományi és társadalomtudományi ismeretek (30 kredit): közigazgatási jog, alkotmányjog, büntetőjog, közigazgatási büntetőjog, közigazgatási rendtartás, alkotmány- és jogtörténet, európai közjog, nemzetközi jog, államtan, közgazdaságtan, szociológia, politológia, pszichológia, vezetés- és szervezéselmélet.A mesterképzésbe való felvétel feltétele, hogy a felsorolt ismeretkörökben legalább 30 kredittel rendelkezzen a jelentkező.17.4.3. A hiányzó krediteket az első négy aktív tanulmányi félév alatt kell teljesíteni. Az NKE TVSz 10. § (6) bekezdés alapján amennyiben a hallgató a mesterképzésbe való felvétel feltételeként előírt tantárgyak kreditjeit az első aktív tanulmányi félév alatt nem szerezte meg, intézkedni kell hallgatói jogviszonyának tanulmányi elégtelenség miatti megszüntetéséről.A hiányzó krediteket a Kari Kreditátviteli és Validációs Bizottság által az előzetes kreditelismerési eljárás során hozott határozatban megjelölt tantárgyak teljesítésével szerezheti meg a hallgató. A Kari Kreditátviteli és Validációs Bizottság – a hallgató előzetes tanulmányait és az előzetes kreditelismerési eljárásban bemutatott teljesített tantárgyait figyelembe véve az alábbi tárgyak közül írhat elő előtanulmányi kötelezettséget:

17.5. A képzésben alkalmazott sajátos oktatási-tanulási, tanulás-támogatási eszköztár, módszertan, eljárások

Információ biztonsági laboratórium. Online és távoktatási tanulás-támogatási eszközök és módszerek használata (pl. Moodle e-learning keretrendszer, Neptun Tanulmányi rendszer, E-közszolgálati Tudásportál, Webináriumok készítése (EDUHOME) és publikálása (pl. Ludovika távoktatási portál).Az abszolutórium megszerzésének feltétele, hogy a hallgató a tantervben meghatározott kötelezően választható szaknyelvi csomagból egy tantárgyat teljesítsen, vagy az alábbiakban meghatározott kiváltási feltételeknek megfeleljen.Kötelezően választható szaknyelvek:-Szaknyelvi ismeretek I.- Hatékony előadás és tárgyalás technika,- Szaknyelvi ismeretek II.- Európai uniós szakpolitikák,- Szaknyelvi ismeretek III. - Gazdasági szaknyelv,- Szaknyelvi ismeretek IV. - Jogi szaknyelv,- Szaknyelvi ismeretek V. - Nemzetközi kapcsolatokA szaknyelvi kurzusok kiváltásának lehetőségei:-a tantervben meghatározott, tudományterülethez kapcsolódó, valamely kötelező szakmai tárgy idegen nyelven történő teljesítése;-idegen nyelvű OTDK dolgozat

írása;-Diplomáciai, közigazgatási, jogi, nemzetközi kapcsolatok, gazdasági, gazdaság és menedzsment, közgazdasági, katonai tudományterülethez kapcsolódó szaknyelvi vizsga megszerzése (legalább középfokú (B2) komplex szinten) az Európai Unió valamely hivatalos nyelvéből.-Diplomáciai, közigazgatási, jogi, nemzetközi kapcsolatok, gazdasági, gazdaság és menedzsment, közgazdasági tudományterülethez kapcsolódó idegennyelvű alap-, vagy mesterképzési szakon szerzett szakképzettség.-nemzetközi mobilitási programon történő részvétel:a) A hallgató a teljesítendő szaknyelvi tárgy témakörébe (Kormányzati rendszerek vagy Nemzetközi kapcsolatok) tartozó tantárgyat teljesített egyéni mobilitása alatt.A tanórákon való részvétel követelményei, az elfogadható hiányzások mértéke, a távolmaradás pótlásának lehetősége:Amennyiben a tantárgyi program nem rendelkezik másképp, akkor a hallgató köteles foglalkozások 75%-án részt venni. A 75%-ot meghaladó mértékű hiányzás az aláírás megtagadását vonhatja maga után. A 75%-ot meghaladó hiányzás indokolt esetben igazolható (pl.: orvosi kezelésben részesült, szolgálati jogviszonyban áll). Az igazolást a következő tanórán kell a kurzust oktató és a tárgyfelelős részére leadni, illetve elektronikus úton eljuttatni. Az így elmulasztott órák tananyaga önálló felkészüléssel pótolhatók.Tantárgyak kedvezményes tanulmányi rend mellett történő teljesítésre vonatkozó szabályok:Az NKE Tanulmányi és Vizsgaszabályzat 20. §-ban rögzített a HTVSZÜB által engedélyezett kedvezményes tanulmányi rendben tanulmányokat folytató hallgatók esetén, amennyiben a tantárgyi program másként nem határoz, a tanórákon való részvétel követelményei, az elfogadható hiányzások mértéke, a távolmaradás pótlásának lehetősége vonatkozásában a hallgatónak a kurzus oktatójával egyeztetett formában otthoni munkával elkészítendő feladatot szükséges teljesítenie a szorgalmi időszak végét megelőző utolsó munkanapig. A hallgatónak a kedvezményes tanulmányi rendet engedélyező határozat kézhezvételétől számított 10 munkanapon belül szükséges felvennie a kapcsolatot a kurzus oktatójával az otthoni munkával elkészítendő feladat teljesítési feltételeinek egyeztetése érdekében.

Budapest, 2024

A szakfelelős: Dr. Krasznay Csaba, PhD,
egyetemi docens

A tantárgyi programok listája

I. Törzsanyag

- A kiberbiztonság humán tényezői;- A kiberbiztonság jogi és szervezeti alapjai Magyarországon;- Adatvédelem;- Bevezetés a kiberbiztonság szakterületi ismereteibe;- Biztonsági tesztelés;- Felhőalapú rendszerek biztonsága;- Hálózati biztonsági technológiák alkalmazása;- Hírszerzés a kibertérben;- Incidensmenedzsment;- Kiberbiztonsági stratégia és vezetés;- Kiberbűnözés és kibernyomozás;- Kockázatértékelés és kockázatmenedzsment;- Közszolgálati információs rendszerek védelme;- Kritikus információs infrastruktúra védelem;- Nemzetállamok a kibertérben;- Operációs rendszerek;- Számítógép hálózatok;- Végponti biztonsági technológiák alkalmazása;

II. Szakdolgozat/Diplomamunka

III. Szakmai gyakorlat

IV. Szabadon választható tantárgyak

V. Kritériumkövetelmények

- Ludovika Fesztivál Szabadegyetem;- Szaknyelvi ismeretek I. - Hatékony előadás és tárgyalás technika;- Szaknyelvi ismeretek II. - Európai Uniós szakpolitikák;- Szaknyelvi ismeretek III. - Gazdasági szaknyelv;- Szaknyelvi ismeretek IV. - Jogi szaknyelv;- Szaknyelvi ismeretek V. - Nemzetközi kapcsolatok;

VI. Kötelezően választható tantárgyak

A kiberbiztonsági mesterképzési szak ajánlott tanterve

TANTÁRGYI PROGRAMOK

NEMZETI KÖZSZOLGÁLATI EGYETEM
Államtudományi és Nemzetközi Tanulmányok
Kar

TANTÁRGYI PROGRAM

NPNBM51 A kiberbiztonság humán tényezői

1. A tantárgy kódja: NPNBM51

2. A tantárgy megnevezése (magyarul): A kiberbiztonság humán tényezői

3. A tantárgy megnevezése (angolul): Human factors of cybersecurity

4. Kreditérték és képzési karakter:

4.1. 4 kredit

4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 50 % gyakorlat, 50 % elmélet

4.3. Az értékelés: kollokvium

5. A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):

5.1. kiberbiztonsági mesterképzési szak;

6. Az oktatásért felelős oktatási szervezeti egység megnevezése:

Nemzetbiztonsági Intézet, Polgári Nemzetbiztonsági Tanszék

7. A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:

Dr. Dobák Imre, PhD, intézetvezető

8. A tanórák száma és típusa

8.1.össz óraszám/félév:

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

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

8.2.heti óraszám - nappali munkarend: 2

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

9. A tantárgy szakmai tartalma (magyarul):

A tárgy az emberi tényező oldaláról vizsgálja a kiberbiztonság jelentőségét, és ismerteti meg a hallgatókat a „humán alapú” sebezhetőség témakörével. A „social engineering”, az emberi tényező kihasználására épülő támadási formák témakörében vizsgálja a humán kockázatok jelentőségét, a támadások humán alapú módszereit, technikáit, céljait, a védekezés lehetőségeit. Az információbiztoság emberi tényezői témakörében esettanulmányokkal, példákkal mélyíti a biztonságtudatos szakmai gondolkodás fejlődését. A tárgy emellett a kiberbiztonság pszichológiai kérdésköréhez kapcsolódóan tárgyalja a kibertérben zajló megtévesztés és befolyásolás széles kérdéskörét. Társadalomtudományi megközelítéssel ismerteti az állami és nem állami szereplők kapcsán megfigyelhető folyamatokat, a lélektani műveletek, a megtévesztés, a befolyásolás, az információgyűjtés, és információterjesztés, álhírek sajátosságait, azok jelenlétét, lehetséges céljait, hatásait. Példákon, esettanulmányokon keresztül hívja fel a figyelmet a jelenségre, különös tekintettel a közösségi média szerepére.

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

The course examines the importance of cybersecurity from a human factor perspective and introduces students to the issue of "human-based" vulnerability. It examines the importance of human risks, human-based methods, techniques, objectives and defences of attacks in the context of social engineering, the exploitation of the human factor. In the

area of human factors in information security, case studies and examples will deepen the development of security-aware professional thinking. The course will also address the broad issue of deception and influence in cyberspace in relation to the psychological issues of cyber security. It will take a social science approach to the processes of state and non-state actors, the psychological operations, deception, influence, information gathering and dissemination, fake news, their presence, possible purposes and effects. It draws attention to the phenomenon through examples and case studies, with particular reference to the role of social media.

10. Elérendő kompetenciák (magyarul):

Tudása
Tisztában van az emberi tényező szerepével a kibertámadások kivitelezése során. Ismeri a fedett környezetből történő információgyűjtés eljárásait.
-
Képességei
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.
-
Attitűdje
Hatékony lépéseket tesz a kibertámadások megelőzése érdekében, így csökkentve a szervezete kitettségét. A maga komplexitásában tervezi meg az információbiztonsági irányítási rendszert.
-
Autonómiája és felelőssége
Vállalja a kiberbiztonsági fenyegetések kezelésének felelősségét. Gyakorlatába beépíti és alkalmazza a kiberbiztonsági szakterületen folyó kutatások eredményeit.
-

Elérendő kompetenciák (angolul) (Competences – English):
Knowledge:
The role of human factors in the execution of cyber attacks. The procedures of covert information gathering.
-
Capabilities:
He/she is capable of taking defensive measures that ensure the reduction of risk resulting from threat against humans. He/she is capable of assessing cybersecurity risks posed by internal employees. He/she is capable of creating regulations to handle threats posed by internal employees.
-
Attitude:
An effort to take effective measures in order to prevent cyber attacks, by this means reducing the exposure of his/her organisation. An ability to treat internal employees as high risk and plans information security processes accordingly.
-
Autonomy and responsibility:
To handle cyber security threats. To incorporate and apply the results of ongoing research in the field of cybersecurity.
-

11. Előtanulmányi követelmények:

nincs

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

12.1. A kiberbiztonság humán oldala, az emberi tényező szerepe (The human side of cybersecurity, the role of human factor);12.2. A kibertér szereplői és támadói (Players and attackers in the cyberspace);12.3. Az emberi tényező kihasználására épülő támadási technikák és formák (Attacking techniques and forms based on human factors);12.4. A kiberpszichológia szerepe a kiberbiztonságban (The role of cyber psychology in cyber security);12.5. A közösségi oldalak, online tér, platformok - a személyiség befolyásolásának lehetőségei (Social networking sites, online space, platforms - possibilities of influencing personality);12.6. Internet-, közösségi média-, telefon-, játékfüggőség (Internet, social media, phone, game addiction);12.7. A közösségi média és egyéb platformok szerepe (The Role of Social Media);12.8. Közösségi kommunikáció, közösségi média és kríziskezelés (Social communications, social media and crisis management);12.9. Pszichológiai „műveletek" értelmezése és jelentősége a kibertérben (Understanding and Significance of Psychological Operations in Cyberspace);12.10. A pszichológiai műveletek céljai, szereplői (nemzet)biztonsági szemmel. Információgyűjtés a kibertérben (Objectives and actors of psychological operations with a view to (national) security. Information gathering in cyberspace);12.11. A befolyásolás jelensége, lehetséges céljai, sajátosságai, példái (Phenomenon of influence, its possible aims and peculiarities);12.12. A megtévesztés lehetőségei, technikái, nemzetközi példái, az álhírek sajátosságai, céljai, hatásai szereplői (nemzet)biztonsági szemmel. Az álhírek elleni küzdelem. (Possibilities, techniques, international examples of deception, characteristics, goals, and effects of fake news with a view to (national) security. Fight against fake news);12.13. A biztonságtudatosítás jelentősége, az oktatás szerepe (Importance of awareness, role of education);12.14. Biztonságtudatosítási program - csoportos gyakorlati projektfeladat végrehajtása (Security awareness program - implementation of a group practical project task);

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

3. félév/ősz;

14. 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.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje

A félév során a hallgatók két zárthelyi dolgozatot írnak. Az első zárthelyi a 13.1-13.7., a második a 13.8-13.13 témákat ellenőrzi. A zárthelyi dolgozat értékelése ötfokozatú skálán történik az alábbiak szerint: 51 %-tól elégséges, 63 %-tól közepes, 75 %-tól jó, 87 %-tól jeles. Sikertelen zárthelyi dolgozatot a félév utolsó tanulmányi hetében lehet pótolni.

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

16.1. Az aláírás megszerzésének feltételei:
Az aláírás megszerzésének feltétele a tanórákon való 70 %-os részvétel és a zárthelyi dolgozatok mindegyikének legalább elégséges osztályzata.

16.2. Az értékelés:

Az írásbeli kollokvium követelménye a tanórákon átadott ismeretekre és a kötelező irodalomra épül. Az írásbeli kollokvium esetében az értékelés a hallgató által 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)

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

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. Bányász Péter: A közösségi média szerepe a lélektani műveletekben az elmúlt időszak válságainak tükrében, Szakmai Szemle, Budapest 2016.2. Dobák Imre: A dezinformáció – napjaink kiemelt kihívása, Katonai Jogi és Hadijogi Szemle, Budapest 2022/1.3. Dobák Imre – Tóth Tamás: Régi módszerek a kibertérben? (CYBER-HUMINT, OSINT, SOCMINT, Social Engineering), Belügyi Szemle, Budapest 2021. ISBN: 2062-9494;4. Haig Zsolt: Információs műveletek a kibertérben, Dialóg Campus Kiadó, Budapest 2018. ISBN: 978-615-5945-05-2;5. Rashid A., Chivers H., Danezis G., Lupu E., Martin A.: The Cyber Security Body of Knowledge (CyBOK Version 1.0), The National Cyber Security Centre , 2019.

17.2. Ajánlott irodalom:

1. Christopher Hadnagy: Social Engineering: The Science of Human Hacking, Wiley, 2018. ISBN: 978-1-119-43373-6 (ebk);2. Cialdini, Robert B.: Hatás - A befolyásolás pszichológiája, HVG Könyvek, Budapest 2009. ISBN: 9789639686779;3. Dobák Imre - Babos Sándor: A biztonságtudatosítás lehetőségei a 21. századi platformok fényében, Nemzetbiztonsági Szemle, Budapest 2021.4. Rantos, K., Fysarakis, K., and Manifavas, C.: How effective is your security awareness program? An evaluation methodology, Information Security Journal 21(6), 2012. ISBN: https://doi.org/10.1080/19393555.2012.747234;5. Young, Heather & Vliet, Tony & Ven, Josine & Jol, Steven & Broekman, Carlijn: Understanding Human Factors in Cyber Security as a Dynamic System, 2018. ISBN: DOI 10.1007/978-3-319-60585-2_23;

Budapest, 2024

Dr. Dobák Imre, PhD, intézetvezető

Nemzeti Közszolgálati Egyetem
Államtudományi és Nemzetközi Tanulmányok
Kar

TANTÁRGYI PROGRAM

ÁKIBTM001 A kiberbiztonság jogi és szervezeti alapjai Magyarországon

1. A tantárgy kódja: ÁKIBTM001

2. A tantárgy megnevezése (magyarul): A kiberbiztonság jogi és szervezeti alapjai Magyarországon

3. A tantárgy megnevezése (angolul): Legal and organisational foundations of cybersecurity in Hungary

4. Kreditérték és képzési karakter:

4.1. 6 kredit

4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 0 % gyakorlat, 100 % elmélet

4.3. Az értékelés: kollokvium

5. A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):

5.1. kiberbiztonsági mesterképzési szak;

6. Az oktatásért felelős oktatási szervezeti egység megnevezése:

Kiberbiztonsági Tanszék

7. A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:

Dr. Szádeczky Tamás, PhD, egyetemi docens, tanszékvezető

8. A tanórák száma és típusa

8.1.össz óraszám/félév:

8.1.1.nappali munkarend: 56 (56 EA + 0 SZ + 0 GY)

8.1.2.levelező munkarend: 16 (16 EA + 0 SZ + 0 GY)

8.2.heti óraszám - nappali munkarend: 4

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

9. A tantárgy szakmai tartalma (magyarul):

A tantárgy célja a kiberbiztonsággal kapcsolatos hazai és európai jogszabályok, szabályozások és intézményrendszer bemutatása. Ezen belül a hallgató megismeri a magyar és Európai Uniós közigazgatás, mint szervezetrendszer felépítését, az alapvető szervezési elveket, a kiberbiztonságra fókuszálva. A hallgató továbbá megismeri a kiberbiztonsági joggal és a jogrendszerrel, a jogállamisággal kapcsolatos fogalmakat, összefüggéseket Magyarországon és az Európai Unióban, amelyek megalapozzák a közigazgatás elhelyezését az állami szervek rendszerében, és mint jogalkotót a jogforrási hierarchiában. A tantárgy kitér a kiberbiztonságra vonatkozó nemzeti és nemzetközi szabályozókra is, melyek érdemben határozzák meg a kiberbiztonsági szakemberek munkáját.

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

The aim of the course is to provide an introduction to the national and European legislation, regulations and institutional framework related to cybersecurity. In this context, the student will learn about the structure of the Hungarian and European Union public administration as an organisational system, , with a focus on cybersecurity. The student

will also learn about the concepts and contexts related to cybersecurity law and the legal system, the rule of law in Hungary and the European Union, which underpin the placement of public administration in the system of state bodies and as a legislator in the hierarchy of legal sources. The course will also cover national and international regulators on cybersecurity, which have a substantive impact on the work of cybersecurity practitioners.

10. Elérendő kompetenciák (magyarul):

Tudása

Ismeri azokat a fontosabb előírásokat a kiberbiztonsággal kapcsolatos hazai és nemzetközi szabályozásokból, amelyek a mindennapi munkáját befolyásolják.Ismeri a nemzetközi jog alkalmazhatóságát a kibertérben.Tisztában van az állami kibervédelmi rendszerrel.
Ismeri azokat a kulcsfontosságú előírásokat és szabályozásokat, amelyek a kiberbiztonság területén hazai és nemzetközi szinten irányadóak, és amelyek nap mint nap hatással vannak a munkavégzésére. Tisztában van a különböző nemzetközi normákkal és szabályokkal, amelyek a kibertérre vonatkoznak, és tudja, hogyan kell ezeket gyakorlatban alkalmazni. Ismeri a nemzetközi jog alkalmazhatóságát a kibertérben, beleértve azokat a specifikus rendelkezéseket, amelyek a kiberbűnözés elleni küzdelemre, valamint az adatvédelemre és az információbiztonságra vonatkoznak. Tisztában van az állami kibervédelmi rendszerrel, ismeri annak felépítését, a kibervédelemmel foglalkozó szervezeteket és hatóságokat, valamint azok feladat- és hatáskörét. Érti, hogyan működik együtt a hazai és nemzetközi szintű kibervédelem, és képes felismerni azokat a kihívásokat és lehetőségeket, amelyek ezen a területen felmerülnek.
Képességei

Képes értelmezni a jogszabályokból eredő követelményeket. Képes átlátni a kibertér speciális jogállását.
Képes értelmezni és megérteni a jogszabályokból eredő követelményeket, ami magában foglalja azok pontos elemzését és azoknak a mindennapi munkájába való integrálását. Képes felismerni és alkalmazni a releváns törvényi előírásokat, valamint képes azokat összevetni a gyakorlati tevékenységekkel, ezzel biztosítva a jogszabályi megfelelőséget. Továbbá, képes átlátni a kibertér speciális jogállását, beleértve azokat a különleges elveket és normákat, amelyek csak a digitális térben érvényesülnek.
Attitűdje

Megérti és elfogadja a nemzetközi kiberjog komplexitását, ennek köszönhetően a munkája során törekszik ennek a komplexitásnak a kezelésére. A maga komplexitásában tervezi meg az információbiztonsági irányítási rendszert.
Megérti és elfogadja a nemzetközi kiberjog komplexitását, beleértve azokat a különböző jogi rendszereket, szabályozásokat és normákat, amelyek a globális kibertérben irányadóak. Ennek köszönhetően a munkája során kiemelt figyelmet fordít ennek a komplexitásnak a kezelésére, ami magában foglalja a nemzetközi szabályozások nyomon követését, azok alkalmazását a gyakorlatban, valamint az ezzel kapcsolatos kihívások proaktív kezelését. Ezen ismeretek birtokában a maga komplexitásában tervezi meg az információbiztonsági irányítási rendszert, figyelembe véve a nemzetközi kiberjogi környezet változásait és azok hatását az információbiztonságra. Emellett, a tervezés során alkalmazza azokat a legjobb gyakorlatokat és standardokat, amelyek elősegítik egy olyan rendszer kialakítását, ami képes alkalmazkodni a kiberbiztonsági fenyegetések dinamikus természetéhez, valamint biztosítja az információk integritását, rendelkezésre állását és titkosságát.
Autonómiája és felelőssége

Tudatosan törekszik a kiberbiztonság sajátosságainak megfelelő, korszerű ismeretek hazai és nemzetközi szinten történő gyakorlati alkalmazására. Értékkötelezett módon vesz részt a kibertér komplexitásának és kölcsönhatásainak ismerete által a különböző hivatásrendek feladatainak szervezésében. Felelősséget vállal a kiberbiztonság összefüggő ismeretének és

a meghatározó jogi, szabályozási és gazdasági összefüggések ismeretének alapján a szakmai javaslatok kidolgozásában.
Tudatosan és proaktívan törekszik arra, hogy a kiberbiztonság területén szerzett korszerű ismereteit, melyek hazai és nemzetközi szinten egyaránt relevánsak, a gyakorlatban hatékonyan alkalmazza. Ez magában foglalja a legfrissebb technológiai fejlesztésekre, fenyegetési modellekre és védelmi stratégiákra való odafigyelést, annak érdekében, hogy az információvédelmi intézkedések mindig naprakészek és hatékonyak legyenek.
Értékkötelezett módon vesz részt a kibertér komplexitásának és kölcsönhatásainak mélyreható ismerete által támogatva a különböző hivatásrendek feladatainak szervezésében és koordinálásában, elősegítve ezzel a kiberbiztonsági kultúra erősítését és a szektorok közötti együttműködést. Felelősséget vállal a kiberbiztonság összefüggő ismeretének és a meghatározó jogi, szabályozási, technológiai és gazdasági összefüggések ismeretének alapján a szakmai javaslatok kidolgozásában, ezáltal hozzájárulva a szervezetek és intézmények kiberbiztonsági kihívásokkal szembeni ellenálló képességének növeléséhez. Aktívan részt vesz a kiberbiztonsági tudatosság növelésében, valamint az új szabályozási környezetek adaptációjában és az ezekből eredő gyakorlati megközelítések fejlesztésében, biztosítva a folyamatos fejlődést és az alkalmazkodó képességet a gyorsan változó digitális világban.

Elérendő kompetenciák (angolul) (Competences – English):
Knowledge:
know specifications of national and international cybersecurity regulations
Specifications of national and international cybersecurity regulations that have an immediate impact on his/her daily work. The applicability of international law in cyberspace. The cybersecurity system of the state.
Capabilities:
interpret legal requirements

He/she is capable of interpreting legal requirements. He/she is capable of having an overview of the special legal status of cyberspace.
Attitude:
understand and accept of the complexity of international cyber law
An understanding and acceptance of the complexity of international cyber law and thus strives to handle this complexity in his/her work. An effort to design the cyber security management system in its own complexity.
Autonomy and responsibility:

implement advanced knowledge characterising cybersecurity

To implement advanced knowledge characterising cybersecurity on a national and international level. To take part in organising tasks of the various professions by having an overview of the complexity and interactions of cyberspace. Moreover to take responsibility for making professional proposals based on comprehensive knowledge of cyber security and dominant legal, regulatory and economical processes.

11. Előtanulmányi követelmények:

nincs

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

12.1. Az információ- és kibervédelem szabályozásának fejlődése a kezdetektől napjainkig (Evolution of information security and cybersecurity regulation from the beginning to the present day);12.2. Az állam és a szervezet szerepe az információ- és kibervédelemben (The role of the state and the organisation in information and cyber security);12.3. Az állam, az állam szervezete (The state, the organization of the state);12.4. A közigazgatás fogalma és kialakulása (Concept and evolution of public administration);12.5. A közigazgatás feladatai, funkciói és tevékenységfajtái (Functions, functions and activities of public administration);12.6. A jog fogalma. A jogrendszer és tagozódása. A jogágak viszonya egymáshoz (Concept of law. The legal system and its division. The relationship between the branches of law);12.7. A közigazgatási jog fogalma, kialakulása, jellemzői (Concept, formation and characteristics of administrative law);12.8. A közigazgatási szervezetrendszer szervezési elvei és felépítése Magyarországon és az Európai Unióban. Szervezetelméleti ismeretek (The general principles and structure of the public administration as an organization system in Hungary and the European Union. Introduction to the Organizational Theories);12.9. A kiberbiztonság stratégiai szintű szabályozása Magyarországon (Cybersecurity regulation at strategic level in Hungary);12.10. A kiberbiztonsági törvényi szintű szabályozása Magyarországon (Regulation of cybersecurity at the legislative level in Hungary);12.11. A kiberbiztonsággal kapcsolatos végrehajtási rendeletek Magyarországon (Implementing regulations related to cybersecurity in Hungary);12.12. A kiberbiztonság stratégiai szabályozása Európában (Strategic cybersecurity regulation in Europe);12.13. A kiberbiztonsággal kapcsolatos rendeletek és irányelvek az Európai Unióban (Cybersecurity regulations and directives in the European Union);12.14. A kiberbiztonságért felelős magyar és európai közigazgatási szervek típusai és hatáskörei. Az egyes kiberbiztonságért felelős közigazgatási szervek és funkciójuk áttekintése (Overview on the different types of public organization in Hungary and the European Union and their functions which are responsible for cybersecurity);

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

1. félév/ősz;

14. 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.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje

A félév során a hallgatók két zárthelyi dolgozatot írnak. Az első zárthelyi a 13.1-13.8., a második a 13.9-13.14 témákat ellenőrzi. A zárthelyi dolgozat értékelése ötfokozatú skálán történik az alábbiak szerint: 51 %-tól elégséges, 63 %-tól közepes, 75 %-tól jó, 87 %-tól jeles. Sikertelen zárthelyi dolgozatot a félév utolsó tanulmányi hetében lehet pótolni.

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

16.1. Az aláírás megszerzésének feltételei:
Az aláírás megszerzésének feltétele a tanórákon való 70 %-os részvétel és a zárthelyi dolgozatok mindegyikének legalább elégséges osztályzata.

16.2. Az értékelés:

Az írásbeli kollokvium követelménye a tanórákon átadott ismeretekre és a kötelező irodalomra épül. Az írásbeli kollokvium esetében az értékelés a hallgató által 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)

16.3. A kreditek megszerzésének feltételei:

A kreditek megszerzésének feltétele az aláírás megszerzése és legalább elégséges kollokvium (K).Egyéni tanulmányi rend esetén: órai jelenlét nem szükséges, de a félévközi követelmények és a kollokvium változatlanul teljesítendőek.

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. A 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról,.2. Kovács László: A kibertér védelme, Dialog Campus, Budapest 2019. ISBN: 9786155889639;3. Muha Lajos – Krasznay Csaba: Az elektronikus információs rendszerek biztonságának menedzselése, Nemzeti Közszolgálati Egyetem, Budapest 2018. ISBN: 978- 615-5870-27-9;

17.2. Ajánlott irodalom:

1. Hegyesi Zoltán-Iván Dániel-Linder Viktória-Pollák Kitti-Szalai András-Temesi István-Vértesy László (Szalai András szerk.): A közigazgatás tudománya és gyakorlata, HVGOrac, Budapest 2020. ISBN: 978 963 258 495 9;2. Lapsánszky András (szerk.): Közigazgatási jog – Szakigazgatásaink elmélete és működése, CompLex Wolters Kluwer, Budapest 2020. ISBN: 978-963-295-919-1;3. Linder Viktória-Temesi István-Vértesy László (Temesi István szerk.): Közigazgatási jog, Dialóg Campus, Budapest 2018. ISBN: 978 615 5845 24 6;

Budapest, 2024

Dr. Szádeczky Tamás, PhD, egyetemi docens, tanszékvezető

Nemzeti Közszolgálati Egyetem
Államtudományi és Nemzetközi Tanulmányok
Kar

TANTÁRGYI PROGRAM

ÁAÖKTM07 Adatvédelem

1. A tantárgy kódja: ÁAÖKTM07

2. A tantárgy megnevezése (magyarul): Adatvédelem

3. A tantárgy megnevezése (angolul): Data Protection

4. Kreditérték és képzési karakter:

4.1. 4 kredit

4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 0 % gyakorlat, 100 % elmélet

4.3. Az értékelés: kollokvium

5. A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):

5.1. kiberbiztonsági mesterképzési szak;

6. Az oktatásért felelős oktatási szervezeti egység megnevezése:

Alkotmányjogi és Összehasonlító Közjogi Tanszék

7. A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:

Dr. Téglásiné dr. Kovács Júlia, PhD, adjunktus

8. A tanórák száma és típusa

8.1.össz óraszám/félév:

8.1.1.nappali munkarend: 56 (56 EA + 0 SZ + 0 GY)

8.1.2.levelező munkarend: 16 (16 EA + 0 SZ + 0 GY)

8.2.heti óraszám - nappali munkarend: 4

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

9. A tantárgy szakmai tartalma (magyarul):

A hallgatók az alapképzésben szerzett ismeretekre alapozva átfogó és elmélyült ismereteket szereznek az adatvédelem, köz és magánszféra adatkezelése területén, megismerkednek a hazai és nemzetközi joggyakorlattal. A tantárgyhoz kapcsolódó jogesetek feldolgozása. Ismereteket szereznek a közérdekből nyilvános személyes adat kezeléséről.

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

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

10. Elérendő kompetenciák (magyarul):

Tudása
Ismeri az adatvédelem körében alkalmazandó hazai és uniós szabályokat. Ismeri az adatvédelem alapfogalmait és alapintézményeit. Ismeri az adatvédelem alapelveit. Ismeri az adatvédelem területén az érintett jogokat. Ismeri az adatkezelői kötelezettségeket.

Ismeri az adatbiztonsági eljárásokat. Ismeri a Nemzeti Adatvédelmi és Információszabadság Hatóság eljárásait, feladatkörét, joghatóságát, hatáskörét, illetékességét. Ismeri az adatvédelem körében a tanúsítás és az akkreditáció szabályait.
-
Képességei
Képes azonosítani, ha egy tevékenység adatkezelésnek minősül, illetve képes megállapítani az egyes adatkezelési műveletek, valamint a kezelt személyes adatok körét. Képes szakmailag megfelelő módon meghatározni az adatkezelés jogalapját, az adatkezelési célokat. Képes szakmailag megfelelő módon elhatárolni egymástól az adatkezelőt és az adatfeldolgozót. Képes a Nemzeti Adatvédelmi és Információszabadság Hatóság eljárásait a gyakorlatban értelmezni. Képes az adatvédelmi incidensek azonosítására, kezelésére és bejelentésére.
-
Attitűdje
Fontosnak tartja az adatvédelem jogi, szervezeti, igazgatási, gyakorlati vetületeivel kapcsolatos kérdések magabiztos ismeretét. Törekszik az adatvédelmi kockázatok azonosítására, elemzésére és kezelésére. Törekszik az adatvédelmi tudatosítás minél szélesebb körű megvalósítására. Fontosnak tartja az adatbiztonság minél hatékonyabb megvalósulását. Nyitott az adatkezelői kötelezettségek megismerése és gyakorlati támogatása iránt.
-
Autonómiája és felelőssége
Felelősen viszonyul az új uniós adatvédelmi rezsim megismeréséhez és megértéséhez. Megfelelő ismeretekkel rendelkezik az adatbiztonság érvényre juttatásához. Önállóan képes egy adatkezelés során a kockázatok kiszűrésére, a körülmények reális értékelésére és a felmerülő problémák kezelésére.
-

Elérendő kompetenciák (angolul) (Competences – English):
Knowledge:
Knowledge of applicable national and EU rules in the field of data protection. Knowing the basic concepts and institutions of data protection. Knowing the basic principles of data protection. Thorough knowledge of the rights of the data subject. Thorough knowledge of the data controller’s responsibilities. Knowledge of data security procedures. Being familiar with the status, responsibility, jurisdiction, powers, and competence of the Hungarian National Authority for Data Protection and Freedom of Information (NAIH). Knows the practicies of certification and accreditation in the field of data protection.
-
Capabilities:
Ability to idenfity if an activity qualifies as data processing and to specify the relevant processing operations and the personal data being processed. Ability to identify, in a professional manner, the legal basis and the purposes of the data processing. Ability to distinguish, in a professional manner, between the data controller and the processor. Being able to apply the procedural rules before the Hungarian National Authority for Data Protection and Freedom of Information in practice. Ability to identify, handle and notify personal data breaches.
-
Attitude:
Finding important to have a strong knowledge of the legal, organizational, administrative and practical aspects of data protection. Seeks to identify, analyze and manage data protection risks. Strive to achieve a high level of privacy awareness. Finds it important to achieve the appropriate level of data security as effectively as possible. The student is open to study good practices that facilitate the implementation of the data controller's obligations.
-

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

11. Előtanulmányi követelmények:

nincs

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

12.1. Az adatvédelmi jog kialakulása és helye a jogrendszerben (The formation and place of data protection law in the Hungarian legal regime);12.2. A hazai adatvédelmi szabályozás általános bemutatása, különös tekintettel az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényre [a továbbiakban: Infotv.] (General overview of Hungarian data protection regulation, particularly Act CXII of 2011 on the right to informational self-determination and freedom of information [the Privacy Act]);12.3. Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adat (General overview of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive);12.4. A GDPR és az Infotv. személyi, tárgyi és területi hatálya (The personal, material and territorial scope of the GDPR and the Privacy Act);12.5. Alapfogalmak, alapelvek (Definitions, principles);12.6. Az adatkezelési jogalapok rendszerének bemutatása (Introduction to the system of legal bases for data processing);12.7. Az érintetti jogok általános bemutatása (Introduction to the rights of data subjects);12.8. Az elszámoltathatóság alapelvének részletes bemutatása (A detailed introduction to the principle of accountability);12.9. Az elszámoltathatóság alapelvének való megfelelést segítő, GDPR-ban nevesített és GDPR-on kívüli eszközei (The means of compliance with the principle of accountability under and outside the GDPR);12.10. Az adatkezelő feladatai (The duties of the data controller);12.11. A beépített és alapértelmezett adatvédelem (Data protection by design and default);12.12. Az adatkezelési tevékenységek nyilvántartása (Recording data processing activities);12.13. Az adatvédelmi tisztviselő (The Data Protection Officer);12.14. Az adatbiztonság (Data security);12.15. Egyéb adatkezelői kötelezettségek általános ismertetése (adatvédelmi incidens bejelentése, adatvédelmi hatásvizsgálat) (General introduction to other data controller obligations (reporting a privacy breaches, data protection impact assessment);12.16. A Nemzeti Adatvédelmi és Információszabadság Hatóság eljárásai (The proceedures of the Hungarian National Authority for Data Protection and Freedom of Information);12.17. Akkreditáció és

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

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

1. félév/ősz;

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

Követelmény a tanórákon történő részvétel. Az elfogadható hiányzások mértéke 25%, az e feletti távolmaradás esetén a tantárgy oktatója által meghatározott feladatot szükséges teljesíteni (házidolgozat, kiselőadás). Kedvezményes tanulmányi rendben tanuló hallgatók esetében az óralátogatás nem kötelező, egyénileg készülnek fel a féléves tananyagból. A kreditek teljesítéséhez azonban nekik is meg kell írniuk a zárthelyi dolgozatot.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje

Legalább egy zárthelyi dolgozat sikeres megírása.

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

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

16.2. Az értékelés:
A szorgalmi időszakban a zárthelyi dolgozat alapján. A vizsgaidőszakban kollokvium alapján.

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

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. Balogh Gyöngyi et.al.: Az adatvédelmi jog alapelvei, fogalmai, szereplői, profilalkotás, a személyes adatok különleges kategóriái, bűnügyi személyes adatok, NKE, Budapest 2019.2. Sziklay Júlia – Bendik Tamás: Az adatvédelem hazai és európai uniós szabályozása és alapintézményei, NKE, Budapest 2018.

17.2. Ajánlott irodalom:

1. Árvay Viktor György et.al.: Az elszámoltathatóság alapelve és az adatkezelői kötelezettségek, NKE, Budapest 2018.2. Balogh Gyöngyi et.al.: Az adatvédelmi jog alapelvei, fogalmai, szereplői, profilalkotás, a személyes adatok különleges kategóriái, bűnügyi személyes adatok, NKE, Budapest 2019.3. Bíró János et.al.: Jogalapok, érintetti jogok, NKE, Budapest 2018. ISBN: 978 963 295 761 6;4. Sziklay Júlia – Bendik Tamás: Az adatvédelem hazai és európai uniós szabályozása és alapintézményei, NKE, Budapest 2018.

Budapest, 2024

Dr. Téglásiné dr. Kovács Júlia, PhD, adjunktus

Nemzeti Közszolgálati Egyetem
Államtudományi és Nemzetközi Tanulmányok
Kar

TANTÁRGYI PROGRAM

ÁKIBTM002 Bevezetés a kiberbiztonság szakterületi ismereteibe

1. A tantárgy kódja: ÁKIBTM002

2. A tantárgy megnevezése (magyarul): Bevezetés a kiberbiztonság szakterületi ismereteibe

3. A tantárgy megnevezése (angolul): Introduction to cybersecurity

4. Kreditérték és képzési karakter:

4.1. 6 kredit

4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 50 % gyakorlat, 50 % elmélet

4.3. Az értékelés: gyakorlati jegy

5. A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):

5.1. kiberbiztonsági mesterképzési szak;

6. Az oktatásért felelős oktatási szervezeti egység megnevezése:

Kiberbiztonsági Tanszék

7. A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:

Dr. Krasznay Csaba, PhD, egyetemi docens

8. A tanórák száma és típusa

8.1.össz óraszám/félév:

8.1.1.nappali munkarend: 84 (0 EA + 0 SZ + 84 GY)

8.1.2.levelező munkarend: 24 (0 EA + 0 SZ + 24 GY)

8.2.heti óraszám - nappali munkarend: 6

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

9. A tantárgy szakmai tartalma (magyarul):

A tantárgy célja a kiberbiztonsággal kapcsolatos alapfogalmak bemutatása, a fontosabb fenyegetések ismertetése, a védelmi technológiák evolúciójának körbejárása. A hallgató megismeri a kibertér fogalmát, a kibertér kiterjedését, eszközeit és rendszereit. Ismereteket szerez a védendő adatok és a kritikus infrastruktúrák, ezen belül a kritikus információs infrastruktúrák területéről. Betekintést nyer az információs fenyegetések és veszélyek körébe, valamint a védelem lehetőségeibe. Elsajátítja az információbiztonság (komplex) összetevőit. Részletesen megtanulja a kiberbiztonság területén meghatározó nemzetközi szabványokat és ajánlásokat.

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

The aim of the course is to introduce the basic concepts of cybersecurity, the main threats, and the evolution of defence technologies. The student will learn about the concept of cyberspace, the scope, tools and systems of cyberspace. The student will gain knowledge of data to be protected and critical infrastructures, including critical information infrastructures. He/She will gain insight into the range of information threats and vulnerabilites and the options for cyberdefence. Master the (complex) components of information security. He/She will learn in detail about the international standards and recommendations in the field of cyber security.

10. Elérendő kompetenciák (magyarul):

Tudása
Ismeri azokat a fontosabb előírásokat a kiberbiztonsággal kapcsolatos hazai és nemzetközi szabályozásokból, amelyek a mindennapi munkáját befolyásolják. Átlátja, hogy milyen védelmi megoldások vannak a kibertámadás ellen, melyhez kapcsolódóan ismeri a létfontosságú rendszerelemek fogalmát. Továbbá átlátja a munkáltatók által meghatározott belső szabályzatok megalkotásának szükségességét az információs rendszerekben tárolt adatok sértetlensége és a rendelkezésre állás tekintetében.
-
Képességei
Képes értelmezni a jogszabályokból eredő követelményeket, és képes olyan technológiai védelmi intézkedések meghozatalára, amelyek a cyber kill chain egyes elemeihez kapcsolódnak.
-
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
Tudatosan törekszik a kiberbiztonság sajátosságainak megfelelő, korszerű ismeretek hazai és nemzetközi szinten történő gyakorlati alkalmazására. 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.

Elérendő kompetenciák (angolul) (Competences – English):
Knowledge:
Specifications of national and international cybersecurity regulations that have an immediate impact on his/her daily work, including defence solutions against cyber attacks and the concept of critical infrastructures. Furthermore 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 interpreting legal requirements. He/she is capable of taking technological defensive measures related to elements of the cyber kill chain.
-
Attitude:
An effort to design the cyber security management system in its own complexity. An ability to cooperate in preventing his/her organisation and him/herself from becoming a victim of a cyber attack.
-
Autonomy and responsibility:
To implement advanced knowledge characterising cybersecurity on a national and international level. Furthermore to take responsibility for making professional proposals

based on comprehensive knowledge of cybersecurity and dominant legal, regulatory and economical processes. Also takes part in providing technological, political and administrative solutions to cyber threats.
-

11. Előtanulmányi követelmények:

nincs

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

12.1. Az információs társadalmak és biztonsági kihívásaik (Information societies and their security challenges);12.2. A kiberbiztonság története (History of the cybersecurity);12.3. A kibertér fogalmai (Terminology of cyberspace);12.4. A kibertér aktorai (Actors of cyberspace);12.5. Adatok és infrastruktúrák (Data and infrastructure);12.6. Kibertéri fenyegetések: kiberbűnözés, kiberhadviselés, kiberterrorizmus, kiberkémkedés, hacktivizmus (Cyberthreats: cybercrime, cyberwarfare, cyberterrorism, cyber espionage and hacktivitsm);12.7. A közeljövő fenyegetései (Threats of the near future);12.8. Információbiztonság a szervezeteknél (Information security at organizations);12.9. A szabványok fogalma, az információbiztonsági szabványok összefüggései és felhasználásai lehetőségeik (The concept of standards, the context of information security standards and their uses);12.10. Az ISO/IEC 27xxx szabvány sorozat (The ISO / IEC 27xxx standard series);12.11. Az ISO/IEC 27001:2022 és ISO/IEC 27002:2022 szabványok (The ISO/IEC 27001 and the ISO/IEC 27002 standards);12.12. Az ISO/IEC 15408:2022 szabványsorozat (The ISO/IEC 15408:2022 standard series);12.13. A COBIT, az ITIL és a NIST SP 800 sorozat és az SP 800-53 (COBIT, ITIL and NIST SP 800 series and SP 800-53);12.14. Információbiztonsági menedzsment alapvetései (Basics of Information Security Management);

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

1. félév/ősz;

14. 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.A kedvezményes tanulmányi rendben tanuló hallgatók esetében az óralátogatás nem kötelező, egyénileg készülnek fel a féléves anyagból. A kredit teljesítéséhez előre egyeztetett időpontban el kell végezniük az órai teszteket és videós formában el kell készíteniük a kiselőadást. Munkájuk értékelése a 16. pont szerint történik.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje

A hallgatók minden előadáshoz kapcsolódóan egyénileg feldolgozandó szakanyagot kapnak, melynek ellenőrzése a következő előadás elején történik, nappali tagozaton 5, levelező tagozaton 15 kérdéses teszt kitöltésével. A félév végén ezek a pontszámok összesítésre kerülnek. Emellett a hallgatók személyre szabott feladatot kapnak, melyet kiselőadás formájában ismertetnek, nappali tagozaton az előadáson, levelező tagozaton videó formátumban rögzített módon.

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

16.1. Az aláírás megszerzésének feltételei:
Az aláírás megszerzésének feltétele a tanórákon való 70 %-os részvétel, a tesztkérdésekből legalább 50% elérése és a kiselőadások elkészítése.

16.2. 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)

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

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. A 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról,.2. Muha Lajos, Krasznay Csaba: Az elektronikus információs rendszerek biztonságának menedzselése, Nemzeti Közszolgálati Egyetem, Budapest 2018. ISBN: 9786155870279;3. Szádeczky Tamás: Információbiztonsági szabványok, Nemzeti Közszolgálati Egyetem, Budapest 2014.

17.2. Ajánlott irodalom:

1. ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Introduction and general model,.2. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements,.3. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls,.4. William Stallings, Lawrie Brown: Computer Security: Principles and Practice, Pearson, 2017. ISBN: 978-0134794105;

Budapest, 2024

Dr. Krasznay Csaba, PhD, egyetemi docens

Nemzeti Közszolgálati Egyetem
Államtudományi és Nemzetközi Tanulmányok
Kar

TANTÁRGYI PROGRAM

HKHIRA84 Biztonsági tesztelés

1. A tantárgy kódja: HKHIRA84

2. A tantárgy megnevezése (magyarul): Biztonsági tesztelés

3. A tantárgy megnevezése (angolul): Security testing

4. Kreditérték és képzési karakter:

4.1. 6 kredit

4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 100 % gyakorlat, 0 % elmélet

4.3. Az értékelés: gyakorlati jegy

5. A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):

5.1. kiberbiztonsági mesterképzési szak;

6. Az oktatásért felelős oktatási szervezeti egység megnevezése:

Híradó Tanszék

7. A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:

Dr. Tóth András, PhD, egyetemi docens, tanszékvezető

8. A tanórák száma és típusa

8.1.össz óraszám/félév:

8.1.1.nappali munkarend: 56 (0 EA + 0 SZ + 56 GY)

8.1.2.levelező munkarend: 16 (0 EA + 0 SZ + 16 GY)

8.2.heti óraszám - nappali munkarend: 4

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

9. A tantárgy szakmai tartalma (magyarul):

A tantárgy célja, az informatikai rendszerek biztonsági tesztelése tervezésének, végrehajtásának és a vizsgálatok dokumentálásának ismertetése a hallgatókkal. Laborgyakorlatok során a hallgatók elsajátítják a biztonsági tesztlabor tervezésének és kialakításának lépéseit, az IT rendszerek biztonsági tesztelésének különböző módszertanait, a sérülékenység keresés típusait és a végrehajtásuk lépéseit. Megismerik az informatikai rendszerek fejlesztése, rendszerbe integrálása, üzemelésének ellenőrzése során alkalmazható biztonságtesztelő módszerek fő típusait. Gyakorlati ismereteket kapnak a biztonsági eszközök vizsgálatának lehetőségeiről, a hálózati támadások „klasszikus" életciklusáról, a 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, a vezetéknélküli rendszerek tesztelésének módszertanát, a beágyazott rendszerek vizsgálatának lehetőségeit, a mobil eszközök (okoseszközök) tesztelésének lehetőségeit, illetve a biztonsági tesztelő csapat kommunikációjának, és a vizsgálatok dokumentálásának lehetőségeit, valamint a továbbképzés és önképzés egyéni és csoportos lehetőségeit. A kurzus emellett kitér a biztonságot sértő bűncselekmények, incidensek felderítéséhez

nélkülözhetetlen bizonyító elektronikus adatok jogszerű, szakszerű rögzítésére, valamint ennek a kriminológiai és kriminalisztikai tudásanyagára is.

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

The objective of the course is to introduce students to the planning, execution and documentation of security testing of information systems. During laboratory exercises, students will learn the steps of designing and setting up a security test lab, different methodologies for security testing of IT systems, types of vulnerability scans and the steps of their implementation. They will learn about the main types of security testing methodologies that can be used in the development, integration and operational verification of IT systems. They will gain practical knowledge of the possibilities of security device testing, the "classic" life cycle of network attacks, local and remote vulnerability scanning and exploitation methods. They will learn about the role, advantages and disadvantages of automated vulnerability scanning, steps to interpret and validate results, options for testing applications and services on Windows and Linux operating systems, security testing of web services and databases, user security awareness testing, wireless systems testing methodology, embedded systems testing options, mobile devices (smart devices) testing options, and security testing team communication and test documentation options, as well as individual and group training and self-training options. The course will also cover the legal and professional recording of electronic evidence, which is essential for the detection of security-related crimes and incidents, and the criminological and forensic knowledge of this.

10. Elérendő kompetenciák (magyarul):

Tudása
Átlátja, hogy milyen védelmi megoldások vannak a kibertámadás ellen. Ismeri a kártékony kódok fogalmát és hatásmechanizmusát.
A tantárgy elvégzése után a hallgató átfogó áttekintést kap a kibertámadások elleni védelmi megoldásokról, és megtanulja az egyes támadásfajták megelőzésére szolgáló biztonsági tesztelési módszereket. A tantárgy kitér a rosszindulatú kódokra és azok hatásmechanizmusára, valamint a kiberbiztonsági ellenőrzésekre a hatások minimalizálása érdekében. A hallgató elsajátítja a szervezeteket fenyegető kiberbiztonsági kockázatok azonosításához, elemzéséhez és mérsékléséhez szükséges készségeket. A tantárgy elvégzése után a hallgató rendelkezik majd azzal a tudással, hogy ismereteit valós helyzetekben alkalmazza, és hozzájáruljon a kiberbiztonsági stratégiák kidolgozásához.
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.
A tantárgy célja, hogy a hallgatók elsajátítsák a szükséges készségeket és ismereteket a cyber kill chain különböző szakaszainak technológiai védelmi intézkedéseinek végrehajtásához. Emellett a tantárgy kiterjed az aktuális kiberfenyegetések azonosítására és a potenciális kockázatok mérséklését célzó biztonsági tesztek elvégzésére. A hallgatók azt is megtanulják, hogyan támogathatják a szervezeteket kibervédelmi képességeik fokozásában. A tantárgy elvégzése után a hallgatók képesek lesznek hatékonyan elvégezni a hálózati és szoftverbiztonsági teszteket, valamint átfogó ismereteket szereznek a kibertámadások legújabb trendjeiről.
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.
A tantárgy elvégzése után a hallgató rendelkezik a szükséges gondolkodásmóddal, készségekkel és ismeretekkel ahhoz, hogy megelőzze a kibertámadásokat, és útmutatást nyújtson kollégáinak. Képes lesz azonosítani a potenciális sebezhetőségeket, és megfelelő intézkedéseket foganatosítani a kiberfenyegetettség minimalizálása érdekében. A hallgató emellett pozitív hozzáállásával támogatni fogja szervezetét a biztonságtudatosság kultúrájának előmozdításában.

Autonómiája és felelőssége
Vállalja a szakterület, a szakmai praxis módszertanának fejlesztéséhez szükséges elméleti, tudományos kutatási és gyakorlati információk beszerzésének, értékelésének és hasznosításának végrehajtását. Kezdeményezőként dolgozik a technikai és operatív teendők stratégiai célokká való konvertálásában.
A képzés elvégzése után a hallgatók képesek lesznek önállóan megoldani összetett problémákat, megalapozott döntéseket hozni és alkalmazkodni az új technológiákhoz, hogy versenyképesek és naprakészek maradjanak. A biztonsági tesztelés módszertanának és gyakorlatának megismerése lehetővé teszi a hallgatók számára, hogy azonosítsák egy rendszer sebezhetőségeit, és felelős lépéseket tegyenek azok kijavítására.

Elérendő kompetenciák (angolul) (Competences – English):
Knowledge:
Defence solutions against cyber attacks, and the concept and mode of action of malware codes.
After completing the course, the student will get a comprehensive overview of the solutions to protect against cyber attacks and learn security testing methods to prevent each type of attack. The course will cover malicious code, its mechanism of action, and cybersecurity controls to minimise the impact. Students will acquire the skills necessary to identify, analyse and mitigate cyber security risks to organisations. Upon completing the course, students will know how to apply their knowledge in real-life situations and contribute to developing cybersecurity strategies.
Capabilities:
He/she is capable of taking technological defensive measures related to elements of the cyber kill chain. Moreover he/she is capable of understanding the current threats of cyberspace. Therefore he/she is capable of supporting his/her organisation in developing cyber security skills.
The course aims to equip students with the skills and knowledge necessary to implement technological protection measures at different stages of the cyber kill chain. It also covers the identification of current cyber threats and the execution of security tests to mitigate potential risks. Students will also learn how to support organisations in enhancing their cyber defence capabilities. Upon completing the course, students will be able to effectively conduct network and software security tests and gain a comprehensive understanding of the latest cyber-attack trends.
Attitude:
An effort to take effective measures in order to prevent cyber attacks, by this means reducing the exposure of his/her organisation. An ability to cooperate in preventing his/her organisation and him/herself from becoming a victim of a cyber attack.
Upon completion of the course, the student will have the necessary mindset, skills and knowledge to prevent cyber-attacks and provide guidance to colleagues. They will be able to identify potential vulnerabilities and take appropriate measures to minimise the cyber threat. The student will also support their organisation in promoting a culture of security awareness through a positive attitude.
Autonomy and responsibility:
To obtain, evaluate and utilize theoretical, scientific and practical information necessary for the improvement of the field and the methodology of professional practice. Furthermore to take the initiative in converting technical and operational tasks into strategic objectives.
After completing the course, students can solve complex problems independently, make informed decisions and adapt to new technologies to stay competitive and up-to-date. Familiarity with security testing methodology and practices will enable students to identify vulnerabilities in a system and take responsible steps to fix them.

11. Előtanulmányi követelmények:

nincs

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

12.1. Biztonsági tesztlabor tervezésének és kialakításának lépései (Steps to design and build a security test lab);12.2. IT rendszerek biztonsági tesztelésének különböző módszertanai (Different methodologies for security testing of IT systems);12.3. Biztonsági funkcionális tesztelés, sérülékenység-vizsgálat, behatolás tesztelés (Functional safety testing, Vulnerability testing, Penetration testing);12.4. Helyi és távoli sérülékenység keresés és kihasználás (Local and remote vulnerability discovery and exploitation);12.5. Alkalmazások, szolgáltatások, webszolgáltatások és adatbázisok tesztelésének lehetőségei (Opportunities for testing applications, services, web services and databases);12.6. Felhasználói biztonságtudatossági vizsgálatok (User safety awareness tests);12.7. Vezetéknélküli rendszerek tesztelésének módszertana és mobil eszközök (okoseszközök) tesztelésének lehetőségei (Methodology for testing wireless systems, opportunities for testing mobile devices (smart devices));12.8. Beágyazott rendszerek vizsgálatának lehetőségei (Possibilities of testing embedded systems);12.9. Továbbképzés és önképzés egyéni és csoportos lehetőségei (Individual and group opportunities for further education and self-education);12.10. A bizonyíték és bizonyítási eszköz fogalma, az elektronikus adat - digitális adat fogalma jogban (The concept of evidence and means of proof, concept of electronic data and digital data in law);12.11. A bizonyítékok forrásai a kibertérben (Sources of evidence in cyberspace);12.12. Digitális eszközök ismerete (Knowledge of digital devices);12.13. A számítógépben, kibertérben kutatásra és a lefoglalásra vonatkozó jogi rendelkezések (Legal Provisions of research and seizure in computer and cyberspace);12.14. A digitális nyomrögzítés krimináltechnikai és kriminálmetodika kérdései (Issues of digital forensic and criminal methodology of digital tracking);

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

4. félév/tavasz;

14. 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.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje

A hallgatók a félév folyamán heti feladatokat kapnak, melyeket adott időkereten belül kell megoldani. Minden feladathoz öt időkeret van meghatározva, a hallgató attól függően kap pontot, hogy melyik időkeretben tölti fel a helyes választ. A leggyorsabb megfejtők extra pontokat kapnak, ezzel erősítve a feladatok kompetitív jellegét.

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

16.1. Az aláírás megszerzésének feltételei:
Az aláírás megszerzésének feltétele a tanórákon való 70 %-os részvétel és a feladatokra adható pontszámokból legalább 51% elérése.

16.2. 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)

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

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. ATT&CK Evaluations,.2. OWASP Web Security Testing Guide,.3. Goricsán Tamás: A kényszerintézkedések végrehajtásának sajátosságai a számítástechnikai eszközök felhasználásával megvalósított bűncselekmények nyomozása körében, Pécs 2006. ISBN: 9789636421151;4. Gus Khawaja : Kali Linux Penetration Testing, 2021. ISBN: 978-1119719083;5. Radhi Shatob: Penetration Testing: Step By Step Guide, 2020. ISBN: 978-1999541248;

17.2. Ajánlott irodalom:

1. Open Source Security Testing Methodology Manual – OSSTMM,.2. OWASP recommendations,.3. PCI Data Security Standard (PCI DSS) - Information Supplement: Penetration Testing Guidance,.4. RTFM - Red Team Field Manual,.5. Jason T. Luttgens, Matthew Pepe, Kevin Mandia: Incident Response & Computer Forensics, Third Edition, McGraw-Hill Education, 2014. ISBN: 978-0071798686;

Budapest, 2024

Dr. Tóth András, PhD, egyetemi docens, tanszékvezető

Nemzeti Közszolgálati Egyetem
Államtudományi és Nemzetközi Tanulmányok
Kar

TANTÁRGYI PROGRAM

ÁKIBTM003 Felhőalapú rendszerek biztonsága

1. A tantárgy kódja: ÁKIBTM003

2. A tantárgy megnevezése (magyarul): Felhőalapú rendszerek biztonsága

3. A tantárgy megnevezése (angolul): Security of cloud-based systems

4. Kreditérték és képzési karakter:

4.1. 4 kredit

4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 100 % gyakorlat, 0 % elmélet

4.3. Az értékelés: beszámoló

5. A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):

5.1. kiberbiztonsági mesterképzési szak;

6. Az oktatásért felelős oktatási szervezeti egység megnevezése:

Kiberbiztonsági Tanszék

7. A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:

Koczka Ferenc, phd, tanársegéd

8. A tanórák száma és típusa

8.1.össz óraszám/félév:

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

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

8.2.heti óraszám - nappali munkarend: 2

8.3.Az ismeret átadásában alkalmazandó további sajátos módok, jellemzők:
Egyéni felkészülés e-learning segítségével, online gyakorlat formájában.

9. A tantárgy szakmai tartalma (magyarul):

A tantárgy célja olyan gyakorlati ismeretek nyújtása a hallgatók számára, melynek segítségével képessé válnak egy alapfokú felhőrendszerek biztonságával kapcsolatos ismereteket nyújtó, angol nyelvű, nemzetközi, gyártói vagy gyártófüggetlen vizsga megszerzésére. A kurzus folyamán a hallgatók kiválasztják azt a vizsgát, melynek megszerzését célul tűzték ki, önálló felkészüléssel, a képző által nyújtott e-learning rendszerben elsajátítják az ismereteket, melyek elmélyítésére hetente konzultációs lehetőség áll rendelkezésükre.

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

The aim of the course is to provide students with the practical skills to enable them to pass an international, vendor or vendor-independent exam in English, providing a basic level of cloud system security knowledge. During the course, students will choose the exam they wish to take and will learn the skills through self-study and e-learning provided by the trainer, with weekly consultations to reinforce their knowledge.

10. 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 átlátni a kibertér aktuális fenyegetéseit.
-
Attitűdje
Partner abban, hogy se a szervezete, se ő maga ne váljon kibertámadás áldozatává.
-
Autonómiája és felelőssége
Vállalja a szakterület, a szakmai praxis módszertanának fejlesztéséhez szükséges elméleti, tudományos kutatási és gyakorlati információk beszerzésének, értékelésének és hasznosításának végrehajtását. Önállóan és pontosan vesz részt a kiberbiztonsági fenyegetések technológiai, politikai és adminisztratív megoldásában.
-

Elérendő kompetenciák (angolul) (Competences – English):
Knowledge:
Defence solutions against cyber attacks. 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 understanding the current threats of cyberspace.
-
Attitude:
An ability to cooperate in preventing his/her organisation and him/herself from becoming a victim of a cyber attack.
-
Autonomy and responsibility:
To obtain, evaluate and utilize theoretical, scientific and practical information necessary for the improvement of the field and the methodology of professional practice. To take part in providing technological, political and administrative solutions to cyber threats.
-

11. Előtanulmányi követelmények:

nincs

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

12.1. Bevezetés a felhőbiztonságba (Introduction to Cloud Security)12.2. Platform- és

infrastruktúra-biztonság a felhőben (Platform and Infrastructure Security in the Cloud)12.3. Alkalmazásbiztonság a felhőben (Application Security in the Cloud)12.4. Adatbiztonság a felhőben (Data Security in the Cloud)12.5. Üzemeltetési biztonság a felhőben (Operation Security in the Cloud)12.6. Behatolásvizsgálat a felhőben (Penetration Testing in the Cloud)12.7. Incidensek észlelése és kezelése a felhőben (Incident Detection and Response in the Cloud)12.8. Forenzikus vizsgálatok a felhőben (Forensics Investigation in the Cloud)12.9. Üzletmenet-folytonosság és katasztrófa-helyreállítás a felhőben (Business Continuity and Disaster Recovery in the Cloud)12.10. Irányítás, kockázatkezelés és megfelelés a felhőben (Governance, Risk Management, and Compliance in the Cloud)12.11. Szabványok, irányelvek és jogi kérdések a felhőben (Standards, Policies, and Legal Issues in the Cloud)12.12. A DevOps-kultúra megértése (Understanding DevOps Culture)12.13. Bevezetés a DevSecOps-ba (Introduction to DevSecOps)12.14. DevSecOps szakaszok (DevSecOps Stages)

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

3. félév/ősz;

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

A hallgató önálló felkészüléssel teljesíti a féléves követelményeket, így a tanórákon a részvétel nem kötelező. Az órarendben meghatározott időpontokon az előadó online gyakorlat formájában konzultációs lehetőséget biztosít.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje

A félév során a hallgatók egyénileg, angol nyelvű e-learning segítségével készülnek fel egy, az oktató által ajánlott listából választott, nemzetközileg elismert kiberbiztonsági vizsgára.

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

16.1. Az aláírás megszerzésének feltételei:
Az aláírás megszerzésének feltétele az oktató által kijelölt e-learning modulok sikeres teljesítése.

16.2. Az értékelés:

A tantárgy beszámolóval zárul és értékelése háromfokozatú jeggyel történik, melynek minősítései:- Kiválóan megfelelt (5), amennyiben a hallgató a megadott vizsgaidőpontban sikeresen megszerzi a nemzetközi kiberbiztonsági vizsgát.- Megfelelt (3), amennyiben a hallgató a megadott vizsgaidőpontban megkísérli megszerezni a nemzetközi kiberbiztonsági vizsgát, de nem jár sikerrel.- Nem felelt meg (1), amennyiben a hallgató megszerzi az aláírást, de a vizsgaidőszakban nem próbálkozik meg a nemzetközi kiberbiztonsági vizsga megszerzésével.

16.3. A kreditek megszerzésének feltételei:
A kreditek megszerzésének feltétele az aláírás megszerzése és legalább megfelelt beszámoló (B).

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. Microsoft MD-102 Explore endpoint management,.2. Abraham Silberschatz, Greg

Gagne, Peter B. Galvin: Operating System Concepts, 10th Edition, John Wiley & Sons, 2018. ISBN: 978-1119439257;3. Andrew S. Tanenbaum: Operációs rendszerek, Panem, Budapest 2007. ISBN: 9789635451761;4. Emmett Dulaney: Linux, Taramix, 2016. ISBN: 2399973567770;5. Koczka Ferenc: Operációs rendszerek online tananyag,.

17.2. Ajánlott irodalom:

1. Microsoft Azure Security Technologies, Microsoft Corporation,.2. Mike Chapple, David Seidl : (ISC)2 CCSP Certified Cloud Security Professional Official Study Guide, Sybex, 2022. ISBN: 978-1119909378;3. Oláh István, Magyar Sándor: Biztonsági kérdések egy publikus felhőben, Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar , Budapest 2023.

Budapest, 2024

Koczka Ferenc, phd, tanársegéd

Nemzeti Közszolgálati Egyetem
Államtudományi és Nemzetközi Tanulmányok
Kar

TANTÁRGYI PROGRAM

ÁKIBTM004 Hálózati biztonsági technológiák alkalmazása

1. A tantárgy kódja: ÁKIBTM004

2. A tantárgy megnevezése (magyarul): Hálózati biztonsági technológiák alkalmazása

3. A tantárgy megnevezése (angolul): Application of network security technologies

4. Kreditérték és képzési karakter:

4.1. 4 kredit

4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 100 % gyakorlat, 0 % elmélet

4.3. Az értékelés: beszámoló

5. A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):

5.1. kiberbiztonsági mesterképzési szak;

6. Az oktatásért felelős oktatási szervezeti egység megnevezése:

Kiberbiztonsági Tanszék

7. A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:

Orbók Ákos, tanársegéd

8. A tanórák száma és típusa

8.1.össz óraszám/félév:

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

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

8.2.heti óraszám - nappali munkarend: 2

8.3.Az ismeret átadásában alkalmazandó további sajátos módok, jellemzők:
Egyéni felkészülés e-learning segítségével, online gyakorlat formájában.

9. A tantárgy szakmai tartalma (magyarul):

A tantárgy célja olyan gyakorlati ismeretek nyújtása a hallgatók számára, melynek segítségével képessé válnak egy alapfokú hálózati és hálózatbiztonsági ismereteket nyújtó, angol nyelvű, nemzetközi, gyártói vagy gyártófüggetlen vizsga megszerzésére. A kurzus folyamán a hallgatók kiválasztják azt a vizsgát, melynek megszerzését célul tűzték ki, önálló felkészüléssel, a képző által nyújtott e-learning rendszerben elsajátítják az ismereteket, melyek elmélyítésére hetente konzultációs lehetőség áll rendelkezésükre.

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

The aim of the course is to provide students with the practical skills to enable them to pass an international, vendor or vendor-independent exam in English, providing a basic level of network and network security knowledge. During the course, students will choose the exam they wish to take and will learn the skills through self-study and e-learning provided by the trainer, with weekly consultations to reinforce their knowledge.

10. Elérendő kompetenciák (magyarul):

Tudása

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

- Átlátja, hogy milyen különböző védelmi megoldások érhetők el a kibertámadások ellen. Ezek magukban foglalhatják a korszerű titkosítási módszerek, a fizikai,- logikai,-és egyéb védelmet biztosító technológiai eszközök kombinációját, melyek együttesen képesek hatékonyan csökkenteni a kiberbiztonsági kockázatokat.- Rendelkezik a kibertámadások esetén alkalmazandó eljárások teljes körű ismeretével. Az ilyen eseményekre való gyors és hatékony reagálás érdekében pontosan tudja, melyek az eljárás lépései a támadás forrásának azonosításától kezdve a rendszer helyreállításáig. Az előrelátó tervezés és gyakorlati tapasztalatok révén képes optimális válaszokat nyújtani, ezáltal maximalizálva a rendszerbiztonságot.

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 és megfelelően támogatni szervezetét és a külső feleket egy kibertámadás kezelésében.

- Képes proaktívan védelmi intézkedéseket hozni, amelyek célja a humán fenyegetettségekből eredő kockázatok hatékony csökkentése. Ezen intézkedések a felhasználói képzéstől kezdve a biztonságos hozzáférési jogosultságok beállításáig terjednek, és segítenek megelőzni az emberi tényezőből adódó potenciális biztonsági réseket.- Rendelkezik azzal a képességgel, hogy olyan technológiai védelmi intézkedéseket hozzon, amelyek kapcsolódnak a kiberbűnözők által alkalmazott cyber kill chain egyes elemihez. Ez magában foglalja az események felismerését, a fenyegetések elemzését, és az azok elleni hatékony védekezést, miközben megakadályozza a támadók előrehaladását a támadási láncban.- Rendelkezik azzal a képességgel, hogy átlássa a kibertér aktuális fenyegetéseit, és megfelelő támogatást nyújtson szervezetének és külső feleknek egy kibertámadás kezelésében. A folyamatos felkészültséggel és a fenyegetések naprakész ismeretével biztosítja, hogy az intézkedések mindig az aktuális kockázatoknak megfeleljenek, és hatékonyan segítsenek a támadások elhárításában és 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.

- Hatékonyan lépéseket tesz annak érdekében, hogy megelőzze a kibertámadásokat, ezzel csökkentve a szervezete kitettségét az ilyen fenyegetésekre. Ehhez tartoznak a rendszeres biztonsági felmérések, a sebezhetőségek azonosítása és az azokra adott gyors válasz, valamint az állandó monitorozás és az esetleges kockázatok azonosítása.- Parner abban, hogy saját szervezetében, és magánéletében is kiemelt figyelmet szenteljen annak érdekében, hogy ne váljon kibertámadás áldozatává. Ennek érdekében együttműködik a biztonsági partnerekkel, és szorosan együttműködik az iparági legjobb gyakorlatokkal, hogy mind a szervezete, mind ő maga maximális védelmet élvezzen a kiberbiztonsági fenyegetésekkel szemben.

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.

- Tudatosan és elkötelezetten törekszik arra, hogy a kiberbiztonság sajátosságainak megfelelő, korszerű ismereteket alkalmazzon mind hazai, mind nemzetközi szinten. Ezen erőfeszítések révén biztosítja, hogy mindig naprakész legyen a legújabb kiberbiztonsági trendekkel, technológiákkal és módszerekkel kapcsolatban, és képes legyen ezeket hatékonyan alkalmazni a gyakorlatban.-Vállalja a szakterület, a szakmai praxis módszertanának fejlesztéséhez szükséges elméleti, tudományos kutatási és gyakorlati információk beszerzését, értékelését és hasznosítását. Ennek keretében folyamatosan követi az iparági fejleményeket, részt vesz konferenciákon és képzéseken, valamint hajlandó elkötelezetten részt venni a kutatásokban, hogy hozzájáruljon a kiberbiztonsági szakma fejlődéséhez és hatékonyabbá tegye a szakmai gyakorlatot.

Elérendő kompetenciák (angolul) (Competences – English):
Knowledge:
- Defence solutions against cyber attacks, and also familiar with the procedures applicable in case of a cyber attack.

- It gives you an overview of the different defensive solutions available against cyber-attacks. These can include a combination of advanced encryption methods, physical, logical and other protection technologies that together can effectively reduce cyber security risks.- They have a comprehensive knowledge of the procedures to be used in the event of a cyber-attack. To respond quickly and effectively to such incidents, you will know exactly what the procedural steps are, from identifying the source of the attack to restoring the system. It can provide an optimal response through forward planning and hands-on experience, thereby maximising system security.
Capabilities:

- He/she is capable of taking defensive measures that ensure the reduction of risk resulting from threat against humans.- He/she is capable of taking technological defensive measures related to elements of the cyber kill chain.- Therefore capable of understanding the current threats of cyberspace. Furthermore also capable of supporting his/her organisation and external parties in handling a cyber attack.

- The ability to proactively take security measures to effectively reduce risks from human threats. These measures range from user training to the setting of secure access rights and help prevent potential vulnerabilities due to human factors.- It has the capability to put in place technological protection measures that are linked to certain elements of the cyber kill chain used by cybercriminals. This includes event detection, threat analysis and effective defence against threats, while preventing attackers from advancing in the attack chain.- It has the ability to understand the current threats in cyberspace and provide appropriate support to your organisation and external parties in dealing with a cyber attack. Through continuous preparedness and up-to-date knowledge of threats, it ensures that measures are always in line with the current risks and effectively help to counter and manage attacks.
Attitude:

- An effort to take effective measures in order to prevent cyber attacks, by this means reducing the exposure of his/her organisation.- An ability to cooperate in preventing his/her organisation and him/herself from becoming a victim of a cyber attack.

- It takes effective steps to prevent cyber-attacks, thereby reducing your organisation's exposure to such threats. This includes regular security assessments, identifying and responding quickly to vulnerabilities, and constantly monitoring and identifying potential risks.- Parner is committed to making sure that your organisation, and your personal life, is a top priority to avoid becoming a victim of a cyber-attack. To do this, he works with security partners and closely with industry best practices to ensure that both he and his organisation are fully protected against cyber security threats.

Autonomy and responsibility:

- To implement advanced knowledge characterising cybersecurity on a national and international level.- To obtain, evaluate and utilize theoretical, scientific and practical information necessary for the improvement of the field and the methodology of professional practice.

- It is conscious and committed to applying state-of-the-art knowledge appropriate to the specificities of cybersecurity, both at national and international level. These efforts ensure that it is always up-to-date with the latest cybersecurity trends, technologies and methods and is able to apply them effectively in practice.-Responsible for the acquisition, evaluation and use of theoretical, scientific research and practical information necessary for the development of the methodology of the field, professional practice. In this context, he/she will keep abreast of industry developments, participate in conferences and training courses, and be committed to research to contribute to the development of the cyber security profession and to improve the effectiveness of professional practice.

11. Előtanulmányi követelmények:

nincs

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

12.1. Hálózati támadások és védelmi stratégiák (Network Attacks and Defense Strategies)12.2. Adminisztratív hálózati biztonság (Administrative Network Security)12.3. Technikai hálózatbiztonság (Technical Network Security)12.4. A hálózat peremének biztonsága (Network Perimeter Security)12.5. Vállalati virtuális hálózat biztonsága (Enterprise Virtual Network Security)12.6. Vállalati felhőalapú hálózati biztonság (Enterprise Cloud Network Security)12.7. Vállalati vezeték nélküli hálózatok biztonsága (Enterprise Wireless Network Security)12.8. Hálózati forgalom figyelése és elemzése (Network Traffic Monitoring and Analysis)12.9. Hálózati naplók felügyelete és elemzése (Network Logs Monitoring and Analysis)12.10. Incidensek kezelése és törvényszéki vizsgálat (Incident Response and Forensic Investigation)12.11. Üzletmenet-folytonosság és katasztrófa-helyreállítás (Business Continuity and Disaster Recovery)12.12. Kockázat-előrejelzés kockázatkezeléssel (Risk Anticipation with Risk Management)12.13.

Fenyegetésértékelés támadási felületelemzéssel (Threat Assessment with Attack Surface Analysis)12.14. Fenyegetés-előrejelzés kiberfenyegetettségi intelligenciával (Threat Prediction with Cyber Threat Intelligence)

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

1. félév/ősz;

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

A hallgató önálló felkészüléssel teljesíti a féléves követelményeket, így a tanórákon a részvétel nem kötelező. Az órarendben meghatározott időpontokon az előadó online gyakorlat formájában konzultációs lehetőséget biztosít.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje

A félév során a hallgatók egyénileg, angol nyelvű e-learning segítségével készülnek fel egy, az oktató által ajánlott listából választott, nemzetközileg elismert kiberbiztonsági vizsgára.

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

16.1. Az aláírás megszerzésének feltételei:
Az aláírás megszerzésének feltétele az oktató által kijelölt e-learning modulok sikeres teljesítése.

16.2. Az értékelés:

A tantárgy beszámolóval zárul és értékelése háromfokozatú jeggyel történik, melynek minősítései:• kiválóan megfelelt (5), amennyiben a hallgató a megadott vizsgaidőpontban sikeresen megszerzi a nemzetközi kiberbiztonsági vizsgát.• megfelelt (3), amennyiben a hallgató a megadott vizsgaidőpontban megkísérli megszerezni a nemzetközi kiberbiztonsági vizsgát, de nem jár sikerrel.• nem felelt meg (1), amennyiben a hallgató megszerzi az aláírást, de a vizsgaidőszakban nem próbálkozik meg a nemzetközi kiberbiztonsági vizsga megszerzésével.

16.3. A kreditek megszerzésének feltételei:
A kreditek megszerzésének feltétele az aláírás megszerzése és legalább megfelelt beszámoló (B).

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. Andrew S. Tanenbaum: Számítógép hálózatok , Panem Kft., 2013. ISBN: 9789635455294;2. Frész Ferenc, Kálovics Tamás, Puha Gábor: Hálózatok Biztonsága , ÁROP –2.2.21 Tudásalapú közszolgálati előmenetel, Nemzeti Közszolgálati Egyetem 2014.3. James Kurose, Keith Ross : Computer Networking: A Top-Down Approach, A Top-Down Approach, 2016. ISBN: 9780133594140;

17.2. Ajánlott irodalom:

1. Ciprian Adrian Rusen: Számítógépes eszközök hálózatba kötése lépésről lépésre, Szak Kiadó, 2011. ISBN: 9789639863217;2. Dr. Kónya László: Számítógép-hálózatok,

LSI OMAK Alapítvány, 2002. ISBN: 96357722X;3. Jill West, Tamara Dean, Jean Andrews: Network+ Guide to Networks, 2018. ISBN: 9781337569330;

Budapest, 2024

Orbók Ákos, tanársegéd

Nemzeti Közszolgálati Egyetem
Államtudományi és Nemzetközi Tanulmányok
Kar

TANTÁRGYI PROGRAM

HKKNBM15 Hírszerzés a kibertérben

1. A tantárgy kódja: HKKNBM15

2. A tantárgy megnevezése (magyarul): Hírszerzés a kibertérben

3. A tantárgy megnevezése (angolul): Intelligence in cyberspace

4. Kreditérték és képzési karakter:

4.1. 4 kredit

4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 75 % gyakorlat, 25 % elmélet

4.3. Az értékelés: gyakorlati jegy

5. A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):

5.1. kiberbiztonsági mesterképzési szak;

6. Az oktatásért felelős oktatási szervezeti egység megnevezése:

Nemzetbiztonsági Intézet, Katonai Nemzetbiztonsági Tanszék

7. A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:

Dr. Magyar Sándor, PhD, egyetemi docens

8. A tanórák száma és típusa

8.1.össz óraszám/félév:

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

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

8.2.heti óraszám - nappali munkarend: 2

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

9. A tantárgy szakmai tartalma (magyarul):

Az előadás bemutatja a hírszerzés önálló ágait, a nyílt forrású adatszerzés helyét és szerepét. A hallgató megismeri a nyílt forrású adatszerzés alapfogalmait, a nyílt forrású adatszerzés forrásai, valamint a nyílt forrású adatszerzés módszereit (gyűjtés, keresés, analizálás). Bemutatásra kerül az OSINT technikai eszközrendszere, a keresőmotorok lehetőségei. A hallgató megismeri a közösségi média hírszerzésben betöltött szerepét, a digitális helymeghatározás lehetőségeit, a digitális információk metaadatainak tartalomelemzését. A gyakorlat során felhasználásra kerülnek a nyílt forrású adatszerzésben használható ingyenes szoftverek.

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

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

10. Elérendő kompetenciák (magyarul):

Tudása

Ismeri a fedett környezetből történő információgyűjtés eljárásait.Tisztában van az állami kibervédelmi rendszerrel.

-

Képességei

Képes átlátni a kibertér speciális jogállását.Képes olyan védelmi intézkedések meghozatalára, amelyek segítik a humán fenyegetettségből eredő kockázatok csökkentését.Képes felmérni a belső munkavállalók jelentette kiberbiztonsági kockázatokat.

-

Attitűdje

Megérti és elfogadja a nemzetközi kiberjog komplexitását, ennek köszönhetően a munkája során törekszik ennek a komplexitásnak a kezelésére.Hatékony lépéseket tesz a kibertámadások megelőzése érdekében, így csökkentve a szervezete kitettségét.

-

Autonómiája és felelőssége

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

-

Elérendő kompetenciák (angolul) (Competences – English):
Knowledge:

The procedures of covert information gathering, and the cyber security system of the state.

-

Capabilities:

He/she is capable of having an overview of the special legal status of cyberspace.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 risks posed by internal employees.

-

Attitude:

An understanding and acceptance of the complexity of international cyber law and thus strives to handle this complexity in his/her work.An effort to take effective measures in order to prevent cyber attacks, by this means reducing the exposure of his/her organisation.

-

Autonomy and responsibility:

To initiate and introduce alternative and original solutions and appropriate decision making in complex, atypical contexts.To obtain, evaluate and utilize theoretical, scientific and practical information necessary for the improvement of the field and the methodology of professional practice.To take part in organising tasks of the various professions by having an overview of the complexity and interactions of cyberspace.

-

11. Előtanulmányi követelmények:

nincs

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

12.1. Hírszerzés önálló ágai, a nyílt forrású adatszerzés helye szerepe (Intelligence independent branches, the role of Open Source Intelligence);12.2. Nyílt forrású adatszerzés alapfogalmai (Basic concepts of Open Source Intelligence);12.3. Nyílt forrású adatszerzés forrásai (Source of Open Source Intelligence);12.4. Nyílt forrású adatszerzés módszerei (gyűjtés, keresés, analizálás) (Open Source Intelligence methods (collecting, searching, analyzing));12.5. OSINT technikai eszközrendszere (OSINT technical toolset);12.6. Gyakorlat 1. (Practical course 1.);12.7. Keresőmotorok lehetőségei (Search engine possibilities);12.8. Gyakorlat 2. (Practical course 2.);12.9. Közösségi média, helymeghatározás, képek tartalma (Social media, positioning, image content);12.10. Gyakorlat 3. (Practical course 3.);12.11. Nyílt forrású adatszerzésben használható ingyenes szoftverek (Free software for Open Source Intelligence);12.12. Gyakorlat 4. (Practical course 4.);12.13. Gyakorlat 5. (Practical course 5.);12.14. Gyakorlat 6. (Practical course 6.);

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

4. félév/tavasz;

14. 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.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje

A hallgatók a félév folyamán heti feladatokat kapnak, melyeket adott időkereten belül kell megoldani. Minden feladathoz öt időkeret van meghatározva, a hallgató attól függően kap pontot, hogy melyik időkeretben tölti fel a helyes választ. A leggyorsabb megfejtők extra pontokat kapnak, ezzel erősítve a feladatok kompetitív jellegét.

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

16.1. Az aláírás megszerzésének feltételei:
Az aláírás megszerzésének feltétele a tanórákon való 70 %-os részvétel és a feladatokra adható pontszámokból legalább 50% elérése.

16.2. 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)

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

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. Resperger István (szerk.): A nemzetbiztonság elmélete a közszolgálatban., Dialóg Campus, Budapest 2018. ISBN: ISBN 978-615-5845-65-9 (nyomtatott), ISBN 978-615-5845-66-6 (elektronikus);2. Vadász Pál: Információkeresés a nyílt forrású hírszerzésben, FELDERÍTŐ SZEMLE XIV. évfolyam 1. szám , Budapest 2015. ISBN: HU ISSN 1588-242X;

17.2. Ajánlott irodalom:

1. Ferenczy Gábor Zoltán: Internet alapú nyílt információszerzés elvi rendszertechnikai megvalósítása, ZMNE, doktori (PhD) értekezés 2009.2. Michael Bazzell: OSINT Techniques: Resources for Uncovering Online Information, Independently published (January 1, 2023), 2023. ISBN: 979-8366259064;3. Szabadföldi István: A mesterséges intelligenciával támogatott nyílt információszerzés (OSINT), Ludovika, Nemzetbiztonsági Szemle 2022. ISBN: ISSN 2064-3756 (online);

Budapest, 2024

Dr. Magyar Sándor, PhD, egyetemi docens

Nemzeti Közszolgálati Egyetem
Államtudományi és Nemzetközi Tanulmányok
Kar

TANTÁRGYI PROGRAM

ÁKIBTM005 Incidensmenedzsment

1. A tantárgy kódja: ÁKIBTM005

2. A tantárgy megnevezése (magyarul): Incidensmenedzsment

3. A tantárgy megnevezése (angolul): Incident management

4. Kreditérték és képzési karakter:

4.1. 6 kredit

4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 50 % gyakorlat, 50 % elmélet

4.3. Az értékelés: kollokvium

5. A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):

5.1. kiberbiztonsági mesterképzési szak;

6. Az oktatásért felelős oktatási szervezeti egység megnevezése:

Kiberbiztonsági Tanszék

7. A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:

Dr. Krasznay Csaba, PhD, egyetemi docens

8. A tanórák száma és típusa

8.1.össz óraszám/félév:

8.1.1.nappali munkarend: 56 (0 EA + 0 SZ + 56 GY)

8.1.2.levelező munkarend: 16 (0 EA + 0 SZ + 16 GY)

8.2.heti óraszám - nappali munkarend: 4

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

9. A tantárgy szakmai tartalma (magyarul):

A tantárgy célja a hallgatók megismertetése az incidensmenedzsment alapjaival és eljárásrendjével. Ezen belül tárgyalásra kerül az incidensek osztályozási rendszere, az incidens válasz terv egyes komponensei, az incidensek kezeléséért felelős szervezet felépítése és feladatköre. Bemutatásra kerül a hazai és nemzetközi CERT/CSIRT hálózat. Kitér továbbá az üzletmenetfolytonosság tervezési kérdéseire is. Az előadás tárgyalja az incidensekkel kapcsolatos információk megosztásának módját hivatalos és iparági szereplőkkel. A gyakorlati foglalkozások során bemutatásra kerülnek az incidensmenedzsment folyamat technikai eszközei, melyeknek segítségével a hallgatók esettanulmányokat oldanak meg.

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

The goal of this course is to introduce the basics and procedures of incident management for the students. In details, it discusses the qualification of incidents, components of incident response, the setup and role of the organization responsible for incident management. It introduces the national and international CERT/CSIRT network. It also includes the design questions of business continuity. The lecture highlights incident information sharing with official and private actors. On the practice lessons, technical tools of incident management are presented, that are used by the students to solve case studies.

10. Elérendő kompetenciák (magyarul):

Tudása
Ismeri azokat a fontosabb előírásokat a kiberbiztonsággal kapcsolatos hazai és nemzetközi szabályozásokból, amelyek a mindennapi munkáját befolyásolják. Ismeri a kibertámadás esetén alkalmazandó eljárásokat, illetve tisztában van az állami kibervédelmi rendszerrel.
-
Képességei
Képes értelmezni a jogszabályokból eredő követelményeket, és a szervezeténél keletkezett információkat oly módon megosztani külső szereplővel, hogy az ne sértse saját szervezetének érdekét, de hatékonyan tudja támogatni a külső felet. Képes megfelelően támogatni szervezetét és a külső feleket egy kibertámadás kezelésében.
-
Attitűdje
Hatékony lépéseket tesz a kibertámadások megelőzése érdekében, így csökkentve a szervezete kitettségét. Szükség esetén támogatja a külső feleket a szervezeténél keletkezett információk megosztásával.
-
Autonómiája és felelőssége
Vállalja a kiberbiztonsági fenyegetések kezelésének felelősségét. Gyakorlatába beépíti és alkalmazza a kiberbiztonsági szakterületen folyó kutatások eredményeit.
-

Elérendő kompetenciák (angolul) (Competences – English):
Knowledge:
Specifications of national and international cybersecurity regulations that have an immediate impact on his/her daily work. Familiar with the procedures applicable in case of a cyber attack, therefore the cyber security system of the state.
-
Capabilities:
He/she is capable of interpreting legal requirements and capable of sharing information generated within its organisation with an external party in a way that does not harm the interests of its own organisation, but can effectively support the external party. He/she is capable of supporting his/her organisation and external parties in handling a cyber attack.
-
Attitude:
An effort to take effective measures in order to prevent cyber attacks, by this means reducing the exposure of his/her organisation. An ability to support external parties by sharing information generated within the organisation.
-
Autonomy and responsibility:
To handle cyber security threats, and to incorporate and apply the results of ongoing research in the field of cybersecurity.
-

11. Előtanulmányi követelmények:

nincs

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

12.1. Az incidenskezelés elmélete (Theory of incident management);12.2. Az incidenskezelés jogi háttere (Legal background of incident management);12.3. Az incidenskezelés szervezeti háttere Magyarországon és a nemzetközi térben, CERT/CSIRT szervezetek (Organizational background of incident management in Hungary and internationally, CERT/CSIRT);12.4. A Biztonsági Műveleti Központok (Security Operation Centers);12.5. Az incidenskezelés műszaki eszköztára, logforrások (Technical tools of incident management, log sources);12.6. Naplóelemzés, SIEM rendszerek (Log analysis, SIEM systems);12.7. EDR, XDR, MDR (EDR, XDR, MDR);12.8. Incidenssel kapcsolatos információk megosztása, CTI (Incident information sharing, CTI);12.9. Mesterséges intelligencia az incidensmenedzsmentben (Artificial Intelligence in incident management);12.10. Üzletmenet-folytonosság tervezése (Business continuity planning);12.11. Esemény, probléma, incidens fogalmának meghatározása, gyakorlati példák bemutatása (Definition of security event, problem and incident, practical examples);12.12. Incidens esettanulmányok (Incident related case studies);12.13. Incidenskezelő csapat létrehozása (Setup of an incident management team);12.14. Az incidenskezelés folyamata a gyakorlatban, TTX (Incident management in practice, TTX);

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

4. félév/tavasz;

14. 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.A kedvezményes tanulmányi rendben tanuló hallgatók esetében az óralátogatás nem kötelező, egyénileg készülnek fel a féléves anyagból. A kredit teljesítéséhez előre egyeztetett időpontban teljesíteniük kell a zárthelyi dolgozatokat (szükség szerint online formában) és el kell készíteniük a féléves feladatot. Munkájuk értékelése a 16. pont szerint történik.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje

A félév során a hallgatók két zárthelyi dolgozatot írnak. Az első zárthelyi a 13.1-13.7., a második a 13.8-13.14 témákat ellenőrzi. A zárthelyi dolgozat értékelése ötfokozatú skálán történik az alábbiak szerint: 51 %-tól elégséges, 63 %-tól közepes, 75 %-tól jó, 87 %-tól jeles. Sikertelen zárthelyi dolgozatot a félév utolsó tanulmányi hetében lehet pótolni. Emellett a hallgatók személyre szabott feladatot kapnak, melyet a félév végén kell beadniuk.

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

16.1. Az aláírás megszerzésének feltételei:
Az aláírás megszerzésének feltétele a tanórákon való 70 %-os részvétel, a zárthelyi dolgozatok mindegyikének legalább elégséges osztályzata és a féléves feladat elkészítése.

16.2. Az értékelés:

Az írásbeli kollokvium követelménye a tanórákon átadott ismeretekre és a kötelező irodalomra épül. Az írásbeli kollokvium esetében az értékelés a hallgató által 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)

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

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. Berzsenyi Dániel – Zámbó Nóra: Incidensmenedzsment - Éves továbbképzés az elektronikus információs rendszerek védelméért felelős vezető számára, Nemzeti Közszolgálati Egyetem, Budapest 2022.2. Berzsenyi et al.: Incidensmenedzsment - Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára, Nemzeti Közszolgálati Egyetem, Budapest 2022.3. Berzsenyi et al.: Incidensmenedzsment - Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára., Nemzeti Közszolgálati Egyetem, Budapest 2022.

17.2. Ajánlott irodalom:

1. Arun E. Thomas: Security Operations Center - SIEM Use Cases and Cyber Threat Intelligence, CreateSpace Independent Publishing Platform, 2018. ISBN: 978-1986862011;2. Jason T. Luttgens, Matthew Pepe, Kevin Mandia: Incident Response & Computer Forensics, Third Edition, McGraw-Hill Education, 2014. ISBN: 978-0071798686;3. Knapp Gábor: A minősített elektronikus adatkezelés feltételrendszerének vizsgálata az eseménykezelés során, 2021.

Budapest, 2024

Dr. Krasznay Csaba, PhD, egyetemi docens

Nemzeti Közszolgálati Egyetem
Államtudományi és Nemzetközi Tanulmányok
Kar

TANTÁRGYI PROGRAM

ÁKIBTM006 Kiberbiztonsági stratégia és vezetés

1. A tantárgy kódja: ÁKIBTM006

2. A tantárgy megnevezése (magyarul): Kiberbiztonsági stratégia és vezetés

3. A tantárgy megnevezése (angolul): Cybersecurity Strategy and Leadership

4. Kreditérték és képzési karakter:

4.1. 4 kredit

4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 75 % gyakorlat, 25 % elmélet

4.3. Az értékelés: gyakorlati jegy

5. A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):

5.1. kiberbiztonsági mesterképzési szak;

6. Az oktatásért felelős oktatási szervezeti egység megnevezése:

Kiberbiztonsági Tanszék

7. A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:

Dr. Krasznay Csaba, PhD, egyetemi docens

8. A tanórák száma és típusa

8.1.össz óraszám/félév:

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

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

8.2.heti óraszám - nappali munkarend: 2

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

9. A tantárgy szakmai tartalma (magyarul):

A tantárgy felkészít az információbiztonsági stratégia kifejlesztésére, a szervezeti célok, funkciók és az információbiztonság kapcsolatának megértésére. A hallgatók elsajátítják a stratégiai tervek készítéséhez szükséges eljárásokat. Az információbiztonsági vezetés tekintetében megismerik az információbiztonsági vezető stratégiai feladatköreit, a kritikus szervezeti és információbiztonsági folyamatokat, illetve gyakorlati példákon keresztül ezek végrehajtási módját.

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

The course prepares the students to develop an information security strategy and to understand the relationship between business objectives, functions and information security. Students will learn the procedures required to prepare strategic plans. In terms of information security management, they will learn the strategic responsibilities of the information security manager, the critical information security processes and how to implement them through practical examples.

10. Elérendő kompetenciák (magyarul):

Tudása
Átlátja, hogy milyen védelmi megoldások vannak a kibertámadás ellen. Megérti a szervezeti feladatokat a kibervédelemben és ismeri a kibertámadás esetén alkalmazandó eljárásokat.
-
Képességei
Képes megszerezni a szervezet vezetőinek támogatását a jogszabályi megfelelőség kiépítéséhez, illetve képes támogatni szervezetét a kibervédelmi képességek kialakításában.
-
Attitűdje
A maga komplexitásában tervezi meg az információbiztonsági irányítási rendszert. Hatékony lépéseket tesz a kibertámadások megelőzése érdekében, így csökkentve a szervezete kitettségét.
-
Autonómiája és felelőssége
Felelősséget vállal a kiberbiztonság összefüggő ismeretének és a meghatározó jogi, szabályozási és gazdasági összefüggések ismeretének alapján a szakmai javaslatok kidolgozásában. Kezdeményező módon lép fel az alternatív, eredeti megoldások kidolgozásában, bemutatásában és a bonyolult, nem tipikus helyzetekben történő adekvát döntések meghozatalában.
-

Elérendő kompetenciák (angolul) (Competences – English):
Knowledge:
Defence solutions against cyber attacks, therefore understands organizational responsibilities in cybersecurity. Familiar with the procedures applicable in case of a cyber attack.
-
Capabilities:
He/she is capable of gaining the support of the organisation's leaders to build regulatory compliance. Moreover he/she is capable of supporting his/her organisation in developing cyber security skills.
-
Attitude:
An effort to design the cyber security management system in its own complexity. An effort to take effective measures in order to prevent cyber attacks, by this means reducing the exposure of his/her organisation.
-
Autonomy and responsibility:
To take responsibility for making professional proposals based on comprehensive knowledge of cybersecurity and dominant legal, regulatory and economical processes. To initiate and introduce alternative and original solutions and appropriate decision making in complex, atypical contexts.
-

11. Előtanulmányi követelmények:

nincs

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

12.1. Alapfogalmak: szervezet, stratégia, menedzsment, vezetés … Az információbiztonság helye és szerepe a szervezetben. (Basic terms: organisation, strategy, management, leadership. The place of Information Security in the organisation.)12.2. Szervezettípusok és stratégiai folyamatok. A klasszikus stratégiai tervezés és a stratégiai gondolkodás Mintzberg előtt és után. A stratégiai folyamatok és a 21. századi szervezetek. (Types of organisations and strategic processes. Classical strategic planning and strategic thinking before and after Mintzberg. 21st century changes in organisational strategic behaviour.)12.3. Információbiztonsági szerepek és felelősségi körök. (Information Security Roles & Responsibilities)12.4. A szervezeti stratégia tervezésének folyamatai. Az információbiztonság helye a stratégiában. (Organisational strategic planning processes. The place of Information Security in the strategy.)12.5. Külső és belső környezeti tényezők hatása a stratégiára és a szervezetre. (Internal and external factors influencing strategies and organisations.)12.6. A stratégiai tervezés eszköztára és módszerei. (The strategic planning toolkit: methodologies, methods, models, tools.)12.7. Az információbiztonsági vezetési rendszerfolyamatok felépítése és működtetése. (Managing Information Security.)12.8. Kockázati tervezés és menedzsment. (Risk Planning and Management)12.9. Krízismenedzsment. A kritikus infrastruktúrák és tevékenységek működtetésének biztosítása. (Crisis management, critical infrastructures: managing business continuity.)12.10. Információbiztonsági irányelvek és eljárások (Information Security Policies & Procedures)12.11. Összefoglalás, rendszerezés. (Summary)

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

1. félév/ősz;

14. 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.A kedvezményes tanulmányi rendben tanuló hallgatók esetében az óralátogatás nem kötelező, egyénileg készülnek fel a féléves anyagból. A kredit teljesítéséhez el kell készíteniük a féléves feladatot. Munkájuk értékelése a 16. pont szerint történik.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje

A hallgatók a félév folyamán egy releváns információbiztonsági témából 15 oldalas (3000 leütés oldalanként, plusz illusztrációk) esettanulmányt készítenek.

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

16.1. Az aláírás megszerzésének feltételei:
Az aláírás megszerzésének feltétele a tanórákon való 70 %-os részvétel és a beadandó félévközi feladat sikeres teljesítése. Az óralátogatás alól való felmentést kapók, valamint a megengedettnél több órát mulasztók ezen felül a félév anyagából szóbeli vizsgát tesznek.

16.2. Az értékelés:
A tantárgy a beadott félévközi feladat értékelésével zárul és háromfokozatú gyakorlati jeggyel történik, melynek minősítései: kiválóan megfelelt (5), megfelelt (3), nem felelt meg (1).

16.3. A kreditek megszerzésének feltételei:
A kreditek megszerzésének feltétele az aláírás megszerzése és legalább megfelelt gyakorlati jegy (GYJ).

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. Egyéb, az ENISA oldalain található releváns irodalmak és anyagok.,.2. ENISA Information Security Management Course (online tananyag),.3. legalább egy stratégiával, stratégiai tervezéssel és vezetéssel foglalkozó tankönyv,.4. Jennifer L. Bayuk: Stepping Through Cybersecurity Risk Management; A Systems Thinking Approach, Wiley , 2024. ISBN: 9781394213955;5. Rick Howard: Cybersecurity First Principles; A Reboot of Strategy and Tactics, Wiley, 2023. ISBN: 978-1-394-1708-2;

17.2. Ajánlott irodalom:

1. Gregory Falco, Erich Rosenbach: Confronting Cyber Risk; An Embedded Endurance Strategy for Cybersecurity, OUP, 2022. ISBN: 9780197526576;2. ISACA: COBIT 2019, 2019.3. Muha Lajos, Krasznay Csaba: Az elektronikus információs rendszerek biztonságának menedzselése, Nemzeti Közszolgálati Egyetem, Budapest 2018. ISBN: 9786155870279;4. Oroszi Eszter Diána: Információbiztonsági stratégia és vezetés, Nemzeti Közszolgálati Egyetem, Budapest 2014.5. Scott Ellis: The CSO Guide: The Chief Information Security Officer (CISO) Handbook, Independently published, 2016. ISBN: 978-1519090348;6. Yigal Behar: Digital War: The One Cybersecurity Strategy You Need to Implement Now to Secure Your Business, CreateSpace Independent Publishing Platform, 2017. ISBN: 1548459712;

Budapest, 2024

Dr. Krasznay Csaba, PhD, egyetemi docens

Nemzeti Közszolgálati Egyetem
Államtudományi és Nemzetközi Tanulmányok
Kar

TANTÁRGYI PROGRAM

RBGVB183 Kiberbűnözés és kibernyomozás

1. A tantárgy kódja: RBGVB183

2. A tantárgy megnevezése (magyarul): Kiberbűnözés és kibernyomozás

3. A tantárgy megnevezése (angolul): Cybercrime and cyber investigation

4. Kreditérték és képzési karakter:

4.1. 6 kredit

4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 25 % gyakorlat, 75 % elmélet

4.3. Az értékelés: kollokvium

5. A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):

5.1. kiberbiztonsági mesterképzési szak;

6. Az oktatásért felelős oktatási szervezeti egység megnevezése:

Bűnügyi, Gazdaságvédelmi és Kiberbűnözés Elleni Tanszék

7. A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:

Dr. Gyaraki Réka Eszter r. őrnagy, PhD, adjunktus

8. A tanórák száma és típusa

8.1.össz óraszám/félév:

8.1.1.nappali munkarend: 56 (56 EA + 0 SZ + 0 GY)

8.1.2.levelező munkarend: 16 (16 EA + 0 SZ + 0 GY)

8.2.heti óraszám - nappali munkarend: 4

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

9. A tantárgy szakmai tartalma (magyarul):

A tárgy átfogó képet kíván nyújtani a kiberbűnözés jellemzőiről, típusairól, jövőben várható tendenciáiról, annak anyagi-, eljárás-, nemzetközi jogi ismérveiről. A hallgatók megismerhetik a kiberbűnözés kriminológiai aspektusait is. A képzésben résztvevő hallgatók átfogó módon ismerkedhetnek meg a kiberbűnözéssel és a kiberbiztonsággal folalkozó hazai és a nemzetközi szervezetekkel, valamint feladataikkal. Az elméleti ismeretek elsajátítása előadások keretében, ám interaktív jellegű foglalkozásokon keresztül valósul meg. Az előadások alkalmával megbeszélendő jogszabályok és szervezetek különösen az elmúlt időszak változásai, az egyetemes (európai) és magyar kiberbiztonsági és a kiberbűnözés elleni harc lehetséges kapcsolódási pontjaira is rámutatnak.

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

The course aims to provide a comprehensive overview of the characteristics, types and future trends of cybercrime, its material, procedural and international legal aspects. Students will also learn about the criminological aspects of cybercrime. The students will also gain a comprehensive understanding of national and international organisations involved in cybercrime and cybersecurity and their responsibilities. Theoretical knowledge will be acquired through lectures and interactive sessions. In particular, recent changes in legislation and organisations, as well as the possible links between universal (European)

and Hungarian cybersecurity and the fight against cybercrime will be discussed during the lectures.

10. Elérendő kompetenciák (magyarul):

Tudása

Ismeri azokat a fontosabb előírásokat a kiberbiztonsággal kapcsolatos hazai és nemzetközi szabályozásokból, amelyek a mindennapi munkáját befolyásolják.Ismeri a kibertámadás esetén alkalmazandó eljárásokat.Tisztában van a nyomozóhatóság feladataival az egyes állami szervezetek, vállalatok és intézményeket érő támadások esetén.Megérti a szervezeti feladatokat a kibervédelemben

A kiberbűncselekmények felderítéséhez, bizonyításához és minősítéséhez elengedhetetlenül szükséges informatikai ismeretekkel mélyreható tudással bír, többek között a speciális jogi, kriminalisztikai és bűnügyi szolgálati ismeretekből.Magasszintű ismeretekkel rendelkezik az információs rendszerek bűnüldözés szempontjából releváns szegmenseirőlTisztában van a nyomozóhatóság feladataival az egyes állami szervezetek, vállalatok és intézményeket érő támadások esetén. Tisztában van az információmegosztás folyamatával bűncselekmény felmerülése esetén. Ismeri a fedett környezetből történő információgyűjtés eljárásait.
Képességei

Képes együttműködni a nyomozóhatósággal a kiberbiztonsági eseményeket érintő nyomozások során.Képes a szervezeténél keletkezett információkat oly módon megosztani külső szereplővel, hogy az ne sértse saját szervezetének érdekét, de hatékonyan tudja támogatni a külső felet.Képes a keletkezett információk megosztásának szükségességével kapcsolatban komplex következtetések levonására.Képes átlátni a kibertér aktuális fenyegetéseit.Képes támogatni szervezetét a kibervédelmi képességek kialakításában.

A hallgató tisztában lesz a bűnüldözési tevékenységhez kapcsolódó átfogó fogalmakkal, összefüggésekkel, szabályokkal, folyamatokkal és eljárásokkal, amelyeket képes lesz az önálló döntéshozatalba beépíteni.Képes értelmezni a jogszabályokból eredő követelményeket, és képes együttműködni a nyomozóhatósággal a kiberbiztonsági eseményeket érintő nyomozások során. Alkalmas a keletkezett információk megosztásának szükségességével kapcsolatban komplex következtetések levonására.
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.Szükség esetén támogatja a külső feleket a szervezeténél keletkezett információk megosztásával.
Hatékony lépéseket tesz a kibertámadások megelőzése érdekében, így csökkentve a szervezete kitettségét. Szükség esetén támogatja a külső feleket a szervezeténél keletkezett információk megosztásával.
Autonómiája és felelőssége

Felelősséget vállal a kiberbiztonság összefüggő ismeretének és a meghatározó jogi, szabályozási és gazdasági összefüggések ismeretének alapján a szakmai javaslatok kidolgozásában.Értékkötelezett módon vesz részt a kibertér komplexitásának és kölcsönhatásainak ismerete által a különböző hivatásrendek feladatainak szervezésében.Önállóan és pontosan vesz részt a kiberbiztonsági fenyegetések technológiai, politikai és adminisztratív megoldásában
Felelősséget vállal a kiberbiztonság összefüggő ismeretének és a meghatározó jogi, szabályozási és gazdasági összefüggések ismeretének alapján a szakmai javaslatok kidolgozásában. Vállalja a kiberbiztonsági fenyegetések kezelésének felelősségét.

Elérendő kompetenciák (angolul) (Competences – English):
Knowledge:

The tasks of investigative authorities in case of attacks against state organs, enterprises and institutions. The procedure of information sharing in case of a crime, and the procedures of covert information gathering.

Capabilities:

He/she is capable of interpreting legal requirements.Furthermore he/she is capable of cooperating with investigative authorities in investigations of cyber security incidents.He/she is capable of drawing complex conclusions in terms of the necessity of sharing information.
He/she is capable of inte
Attitude:

He/she is capable of interpreting legal requirements.Furthermore he/she is capable of cooperating with investigative authorities in investigations of cyber security incidents.He/she is capable of drawing complex conclusions in terms of the necessity of sharing information.

Autonomy and responsibility:

An effort to take effective measures in order to prevent cyber attacks, by this means reducing the exposure of his/her organisation.An ability to support external parties by sharing information generated within the organisation.

11. Előtanulmányi követelmények:

nincs

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

12.1. 12.1. Kiberbűncselekmények és a kibertérhez nem kötött bűncselekmények általában (Cybercrime and non-cybercrime in virtual space – generally);12.2. Szellemi tulajdonjog megsértése (copyright law, 3D nyomtatás stb.).(Infringement of Intellectual Property Rights (Copyright Law, 3D printing etc);12.3. Online csalások, pénzmosás (Online fraud, money laundering);12.4. Adatlopás esetei. Hacking, wardriving, social engineering, phishing (Cases of data theft. Hacking, wardriving, social engineering, phishing);12.5. A tartalomközléssel megvalósuló bűncselekmények (Content-crime in cyberspace);12.6. Internetes zaklatás típusai, „bosszú-pornó" (Cyberbullying. Cyber mobbing. „Revenge porn");12.7. A kiberbűncselekményekkel és kibervédelemmel foglalkozó hazai szervezetek (Domestic organizations dealing with cybercrime and cyber defence);12.8. A kiberbűncselekményekkel és kibervédelemmel foglalkozó nemzetközi szervezetek és feladataik (International organizations dealing with cybercrime and cyber defense and their tasks);12.9. A bűnügyi jogsegélyre vonatkozó jogszabályo (Mutual Assistance);12.10. A kiberbűnözés kriminológiai háttere (The criminological background of cybercrime);12.11. Együttműködési kötelezettségek, adatkérésekkel kapcsolatos szabályozás (Obligations of cooperation, Regulation of data requests);12.12. Rendőrségi eljárások a kiberbűnözés felderítése során (Police procedures in the investigation of cybercrime);12.13. Kiberbűncselekmények a nem rendőrségi nyomozóhatóságok szemszögéből (Cybercrime from the perspective of non-police investigative authorities);12.14. DoS, DDoS támadások, zsarolóvírusok, malware-támadások, defacing (DoS, DDoS attack, ransomware malware attacks, defacing);

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

2. félév/tavasz;

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

A hallgató köteles az előadások legalább 70%-án részt venni. Rövid/tartós távolmaradás indokolt esetben (orvosi, szolgálati) pótolható, amely pótlás egyéni megbeszélés szerint történik.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje

-

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

16.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele a tanórákon való 70 %-os részvétel és a zárthelyi dolgozatok mindegyikének legalább elégséges osztályzata.A félév során a hallgatók két zárthelyi dolgozatot írnak. Az első zárthelyi a 13.1-13.7., a második a 13.8-13.14 témákat ellenőrzi. A zárthelyi dolgozat értékelése ötfokozatú skálán történik az alábbiak szerint: 51 %-tól elégséges, 63 %-tól közepes, 75 %-tól jó, 87 %-tól jeles. Sikertelen zárthelyi dolgozatot a félév utolsó tanulmányi hetében lehet pótolni.

16.2. Az értékelés:

Az írásbeli kollokvium követelménye a tanórákon átadott ismeretekre és a kötelező irodalomra épül. Az írásbeli kollokvium esetében az értékelés a hallgató által 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)

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

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

17.2. Ajánlott irodalom:

Budapest, 2024

Dr. Gyaraki Réka Eszter r. őrnagy, PhD, adjunktus

Nemzeti Közszolgálati Egyetem
Államtudományi és Nemzetközi Tanulmányok
Kar

TANTÁRGYI PROGRAM

ÁKIBTM007 Kockázatértékelés és kockázatmenedzsment

1. A tantárgy kódja: ÁKIBTM007

2. A tantárgy megnevezése (magyarul): Kockázatértékelés és kockázatmenedzsment

3. A tantárgy megnevezése (angolul): Risk assessment and risk management

4. Kreditérték és képzési karakter:

4.1. 4 kredit

4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 50 % gyakorlat, 50 % elmélet

4.3. Az értékelés: gyakorlati jegy

5. A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):

5.1. kiberbiztonsági mesterképzési szak;

6. Az oktatásért felelős oktatási szervezeti egység megnevezése:

Kiberbiztonsági Tanszék

7. A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:

Dr. Krasznay Csaba, PhD, egyetemi docens

8. A tanórák száma és típusa

8.1.össz óraszám/félév:

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

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

8.2.heti óraszám - nappali munkarend: 2

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

9. A tantárgy szakmai tartalma (magyarul):

A tantárgy célja az információbiztonsági kockázatelemzés és kockázatkezelés bemutatása. Ennek kapcsán a hallgató megismeri a szabványokban használatos fogalmi eszköztárat, részletesen az ISO 31000 és az ISO/IEC 27005 szabványt, azaz általános és információbiztonsági kockázatkezelési szabványokat. Elsajátítja a kockázatbecslés kvantitatív, kvalitatív és szemikvantitatív megoldásait. Áttekintésre kerülnek a kockázatértékelési opciók és algoritmusok. Az előadás bemutatja az olyan kockázatkezelési szabványokat és keretrendszereket, mint az ISO/IEC 27005, a COBIT2019 - RiskIT,az ITILv4, az Octave és a NIST 800-53, illetve részletesen elemzésre kerül a 2013. évi L. tv. és a CISM alapú kockázatmenedzsment is. A gyakorlat során kockázatértékelési esettanulmányok kerülnek kidolgozásra, kockázati forgatókönyveket állítanak össze a hallgatók, valamint kockázatkezelési terveket készítenek el, beleértve ebbe a vagyonleltárakat és a sebezhetőség vizsgálatokat is.

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

The goal of the course is to introduce information security risk analysis and risk management. In this context, the student will become familiar with the conceptual toolkit used in the standards, in particular ISO 31000 and ISO/IEC 27005, which are general and information security risk management standards. Students will acquire quantitative,

qualitative and semi-quantitative solutions to risk assessment. The risk assessment options and algorithms are reviewed. The lecture introduces risk management standards and frameworks such as ISO/IEC 27005, COBIT2019 - RiskIT, ITILv4, Octave, and NIST 800-53 and detailed analysis of the Act L of 2013 and CISM-based risk management. As practice, risk assessment case studies are developed, students prepare risk scenarios and prepare risk management plans, including asset inventories and vulnerability analysis.

10. Elérendő kompetenciák (magyarul):

Tudása
Ismeri azokat a fontosabb előírásokat a kiberbiztonsággal kapcsolatos hazai és nemzetközi szabályozásokból, amelyek a mindennapi munkáját befolyásolják. 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.
-
Attitűdje
Hatékony lépéseket tesz a kibertámadások megelőzése érdekében, így csökkentve a szervezete kitettségét.A maga komplexitásában tervezi meg az információbiztonsági irányítási rendszert.
-
Autonómiája és felelőssége
Kezdeményező módon lép fel az alternatív, eredeti megoldások kidolgozásában, bemutatásában és a bonyolult, nem tipikus helyzetekben történő adekvát döntések meghozatalában. 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. Kezdeményezőként dolgozik a technikai és operatív teendők stratégiai célokká való konvertálásában.
-

Elérendő kompetenciák (angolul) (Competences – English):
Knowledge:
Specifications of national and international cybersecurity regulations that have an immediate impact on his/her daily work. Understands organizational responsibilities in cybersecurity.
-
Capabilities:
He/she is capable of interpreting legal requirements. Furthermore he/she is capable of gaining the support of the organisation's leaders to build regulatory compliance. He/she is capable of supporting his/her organisation in developing cyber security skills.
-
Attitude:
An effort to take effective measures in order to prevent cyber attacks, by this means reducing the exposure of his/her organisation. An effort to design the cyber security management system in its own complexity.
-
Autonomy and responsibility:
To initiate and introduce alternative and original solutions and appropriate decision making in complex, atypical contexts. Furthermore to take responsibility for making professional proposals based on comprehensive knowledge of cybersecurity and dominant legal, regulatory and economical processes. Moreover to take part in providing technological, political and administrative solutions to cyber threats, and to take the initiative in converting technical and operational tasks into strategic objectives.
-

11. Előtanulmányi követelmények:

nincs

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

12.1. Bevezetés: a 2013. évi L. tv. és a CISM alapú kockázatkezelés (Introduction: risk assessment based on the Act L of 2103 and CISM);12.2. Kockázatmenedzsment a 2013. évi L. törvényben és a 41/2015 BM rendeletben (Risk assessment in the Act L of 2013 and Decree 41/2015);12.3. 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);12.4. Kockázatértékelés és az ISO/IEC 27001:2022 szabvány (Risk assessment and the ISO/IEC 27001:2022 standard);12.5. Kockázatkezelés az ISO/IEC 27005:2022 mentén (Risk management according to the ISO/IEC 27005:2022);12.6. Szabályozott kockázatkezelés (Áttekintés: COBIT2019 - RiskIT, ITILv4, Octave, NIST 800) (Regulated risk management (Review: COBIT2019 - RiskIT, ITILv4, Octave, NIST 800));12.7. Vagyonleltár és sebezhetőség vizsgálat (Asset and vulnerability assessment);12.8. Kockázati forgatókönyv (Risk scenario);12.9. A kockázatértékelési folyamat (azonosítás, elemzés, kiértékelés) (Risk assessment process (identification, analysis, evaluation));12.10. Kockázatbecslés (kvantitatív, kvalitatív, szemikvantitatív) (Risk estimation (quantitative, qualitative, semi-quantitative));12.11. Kockázatmenedzsment – kockázatkezelési terv (Risk management plan);12.12. Az információvédelmi intézkedések területei (Areas of countermeasures in information security);12.13. Lehetséges intézkedések meghatározása és értékelése (Identification and evaluation of potential countermeasures);12.14. A kockázatértékelés karbantartása (megismétlése) (Review (repeat) of risk assessment);

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

3. félév/ősz;

14. 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.A kedvezményes tanulmányi rendben tanuló hallgatók esetében az óralátogatás nem kötelező, egyénileg készülnek fel a féléves anyagból. A kredit teljesítéséhez részt kell venniük a csoportmunkában, szükség szerint online formában. Munkájuk értékelése a 16. pont szerint történik.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje

A hallgatók a félév folyamán kiscsoportos foglalkozás során egy fiktív kockázatelemzést készítenek el egy GRC szoftverben, a félév során megadott információkat követve.

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

16.1. Az aláírás megszerzésének feltételei:
Az aláírás megszerzésének feltétele a tanórákon való 70 %-os részvétel és a félévközi feladat sikeres teljesítése.

16.2. Az értékelés:
A tantárgy a beadott félévközi feladat értékelésével zárul és háromfokozatú gyakorlati jeggyel (GYJ) történik, melynek minősítései: kiválóan megfelelt (5), megfelelt (3), nem felelt meg (1).

16.3. A kreditek megszerzésének feltételei:
A kreditek megszerzésének feltétele az aláírás megszerzése és legalább megfelelt gyakorlati jegy.

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. László Gábor: Kockázatértékelés, kockázatmenedzsment, Nemzeti Közszolgálati Egyetem, Budapest 2014.2. Mark Talabis: Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis, Syngress, 2012. ISBN: 978-1597497350;3. Raymond Pompon: IT Security Risk Control Management: An Audit Preparation Plan, Apress, 2016. ISBN: 978-1484221396;4. Som Zoltán: Kockázatmenedzsment gyakorlat, Nemzeti Közszolgálati Egyetem, Budapest 2014.

17.2. Ajánlott irodalom:

1. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements,.2. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls,.3. MSZ ISO 31000:2018 Kockázatmenedzsment. Irányelvek,.4. Evan Wheeler: Security Risk Management: Building an Information Security Risk Management Program from the Ground Up, Syngress, 2011. ISBN: 978-1597496155;

Budapest, 2024

Dr. Krasznay Csaba, PhD, egyetemi docens

Nemzeti Közszolgálati Egyetem
Államtudományi és Nemzetközi Tanulmányok
Kar

TANTÁRGYI PROGRAM

ÁKIBTM008 Közszolgálati információs rendszerek védelme

1. A tantárgy kódja: ÁKIBTM008

2. A tantárgy megnevezése (magyarul): Közszolgálati információs rendszerek védelme

3. A tantárgy megnevezése (angolul): Defense of information systems for public services

4. Kreditérték és képzési karakter:

4.1. 6 kredit

4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 50 % gyakorlat, 50 % elmélet

4.3. Az értékelés: gyakorlati jegy

5. A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):

5.1. kiberbiztonsági mesterképzési szak;

6. Az oktatásért felelős oktatási szervezeti egység megnevezése:

Kiberbiztonsági Tanszék

7. A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:

Dr. Bányász Péter, PhD, egyetemi docens

8. A tanórák száma és típusa

8.1.össz óraszám/félév:

8.1.1.nappali munkarend: 56 (0 EA + 0 SZ + 56 GY)

8.1.2.levelező munkarend: 16 (0 EA + 0 SZ + 16 GY)

8.2.heti óraszám - nappali munkarend: 4

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

9. A tantárgy szakmai tartalma (magyarul):

A képzésben résztvevő hallgatók átfogó módon ismerkedhetnek meg a magyar közszolgálati információs rendszerek védelmét szabályozó jogszabályokkal, információbiztonsági felelősi gyakorlattal, valamint a védelem eszközeinek alapjaival. Az elméleti ismeretek elsajátítása interaktív szemináriumi foglalkozások keretében valósul meg. Az előadások rámutatnak az egyes védelmi elemek kapcsolódási pontjaira, egymáshoz való viszonyára is.

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

The students participating in the course will be comprehensively acquainted with the legislation regulating the defence of Hungarian public service information systems, information security practices and the basics of defence tools. The theoretical knowledge is acquired in interactive seminar sessions. The presentations will also highlight the interconnections and interrelationships between the different elements of defence.

10. Elérendő kompetenciák (magyarul):

Tudása

- Ismeri azokat a fontosabb előírásokat a kiberbiztonsággal kapcsolatos hazai és nemzetközi 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.
-

Attitűdje

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

Autonómiája és felelőssége

- 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.
-

Elérendő kompetenciák (angolul) (Competences – English):
Knowledge:

- Specifications of national and international cybersecurity regulations that have an immediate impact on his/her daily work.- The need for introducing internal regulations defined by employers in order to maintain integrity and availability of the data stored in information systems.- Understands organizational responsibilities in cybersecurity.
-

Capabilities:

- He/she is capable of interpreting legal requirements.- He/she is capable of gaining the support of the organisation's leaders to build regulatory compliance.- He/she is capable of supporting his/her organisation in developing cyber security skills.
-

Attitude:

- An effort to design the cyber security management system in its own complexity.- An effort to take effective measures in order to prevent cyber attacks, by this means reducing the exposure of his/her organisation.
-

Autonomy and responsibility:

- To take responsibility for making professional proposals based on comprehensive knowledge of cyber security and dominant legal, regulatory and economical processes.- To take part in providing technological, political and administrative solutions to cyber threats.- To handle cyber security threats.
-

11. Előtanulmányi követelmények:

nincs

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

12.1. Állami és önkormányzati rendszerek védelmének alapjai (2013. évi L. törvény., 41/2015. (VII. 15.) BM., 185/2015. (VII. 13.) Korm. rendelet, 186/2015. (VII. 13.) Korm. rendelet, 187/2015. (VII. 13.) Korm. rendelet) (Fundamentals of the Protection of State and Local Government Systems (Act L. of 2013, Government Decree 41/2015 (VII. 15.) BM., 185/2015 (VII. 13.) Government Decree 186/2015 (VII. 13) .) Government Decree 187/2015 (VII. 13.) Government Decree));12.2. Együttműködés a hazai kibervédelmi szervezetekkel (Cooperation with domestic cyber defence organizations);12.3. Kiberbiztonsági feladat és felelősségelhatárolás az állami és önkormányzati rendszereknél (Segregation of cybersecurity tasks and responsibilities in state and local government systems);12.4. A védelem eszközei: Információbiztonság alapok, megfontolások (The means and methods of defence: basics os information security, considerations);12.5. Biztonsági kizárások: incidensek megelőzése, kezelése: védelmi technológiák, folyamatok, proaktív – preventív – reaktív védelem, sérülékenység-menedzsment, sérülékenységvizsgálatok, vizibilitás biztosítása (Security exclusions: incident prevention and management: defense technologies, processes, proactive - preventive - reactive protection, vulnerability management, vulnerability testing, provision of visibility);12.6. Biztonságos beengedések: hitelesítés, engedélyezés, hozzáférés-kezelési technológiák, kiemelt jogosultsággal rendelkezők kezelése (Secure access: authentication, authorization, access management technologies, privileged management);12.7. Kockázatmenedzsment a gyakorlatban: kockázatkezelési alapelvek, GRC (Governance, risk management, and compliance) rendszere (Risk management in practice: principles of risk management, GRC (Governance, risk management, and compliance) system);12.8. A komplex vagyonvédelem fogalma, felépítése, összetevői, egymásra épülésük (Complex physical security: elements and their interconnection);12.9. Titkosítás alkalmazási területei (Applications of encryption);12.10. Szimmetrikus (titkos) kulcsú rendszerek (Symmetric key systems);12.11. Aszimmetrikus (nyilvános) kulcsú rendszerek (Asymmetric key systems);12.12. A vállalati kommunikáció fő területei (The main fields of organizational communication);12.13. Válságmenedzsment és válságkommunikáció (Crisis management

and crisis communication);12.14. Közösségi kommunikáció, közösségi média és kríziskezelés (Social communications, social media and crisis management);

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

3. félév/ősz;

14. 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.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje

A hallgatók minden előadáshoz kapcsolódóan egyénileg feldolgozandó szakanyagot kapnak, melynek ellenőrzése a következő előadás elején történik, nappali tagozaton 5, levelező tagozaton 15 kérdéses teszt kitöltésével. A félév végén ezek a pontszámok összesítésre kerülnek. Emellett a hallgatók személyre szabott feladatot kapnak, melyet a félév végén kell beadniuk.

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

16.1. Az aláírás megszerzésének feltételei:

Az aláírás megszerzésének feltétele a tanórákon való 70 %-os részvétel, a tesztkérdésekből legalább 50% elérése és a féléves feladat elkészítése. Amennyiben a hallgató átlépi a megengedett hiányzás mértékét, az aláírás megtagadható.A kedvezményes tanulmányi rendben tanuló hallgatók esetében az óralátogatás nem kötelező, egyénileg készülnek fel a féléves anyagból. Az aláírás megszerzéséhez az oktatóval előre egyeztetett feladatot kell abszolválniuk. A kedvezményes tanulmányi rend kapcsán meghatározott feladat csupán az óralátogatás alól ad felmentést, és az aláírás feltétele. A kredit megszerzése érdekében az e pontban meghatározott tesztkérdésekből legalább 50% elérése és a féléves feladat elkészítése ugyanúgy elvárás. Munkájuk értékelése a 16. pont szerint történik.

16.2. 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)

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

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. Anthonissen P. F. : Kríziskommunikáció. A válságkezelés és reputációmenedzsment pr-stratégiái, HVG, Budapest 2009.2. Berek Lajos: Biztonságtechnika, Nemzeti Közszolgálati Egyetem, Budapest 2014. ISBN: 9786155491511;3. Buttyán Levente, Vajda István : Kriptográfia és alkalmazásai, Typotex Kft, Budapest 2004. ISBN: 9789632796963;4. Muha Lajos, Krasznay Csaba: Az elektronikus információs rendszerek biztonságának menedzselése, Nemzeti Közszolgálati Egyetem, Budapest 2018. ISBN: 9786155870279;5. Virasztó Tamás : Titkosítás és adatrejtés - Biztonságos kommunikáció és algoritmus adatvédelem, Netacademica, Budapest 2004. ISBN: 9789632142531;

17.2. Ajánlott irodalom:

1. Anne Kohnke, Ken Sigler : Implementing Cybersecurity: A Guide to the National Institute of Standards and Technology Risk Management Framework, Auerbach Publications, 2017. ISBN: 9781498785143;2. Barlai Róbert – Kővágó György : Krízismenedzsment, Kríziskommunikáció, Századvég Kiadó, Budapest 2004.3. Knoke, Michael E., Peterson, Kevin E. (eds.): Physical Security Principles. ASIS International, ASIS International, 2015. ISBN: 9781934904619;4. Lukács Gy., Gábor L. (szerk.) et al: Új Vagyonvédelmi Nagykönyv, Cedit 2000 Kft, Budapest 2002. ISBN: 9638180390;5. Schneier, Bruce : Applied Cryptography: Protocols, Algorithms and Source Code in C, Wiley, 2015. ISBN: 9781119096726;

Budapest, 2024

Dr. Bányász Péter, PhD, egyetemi docens

Nemzeti Közszolgálati Egyetem
Államtudományi és Nemzetközi Tanulmányok
Kar

TANTÁRGYI PROGRAM

ÁKIBTM009 Kritikus információs infrastruktúra védelem

1. A tantárgy kódja: ÁKIBTM009

2. A tantárgy megnevezése (magyarul): Kritikus információs infrastruktúra védelem

3. A tantárgy megnevezése (angolul): Critical information infrastructure protection (CIIP)

4. Kreditérték és képzési karakter:

4.1. 4 kredit

4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 25 % gyakorlat, 75 % elmélet

4.3. Az értékelés: kollokvium

5. A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):

5.1. kiberbiztonsági mesterképzési szak;

6. Az oktatásért felelős oktatási szervezeti egység megnevezése:

Kiberbiztonsági Tanszék

7. A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:

Dr. Szádeczky Tamás, PhD, egyetemi docens, tanszékvezető

8. A tanórák száma és típusa

8.1.össz óraszám/félév:

8.1.1.nappali munkarend: 56 (56 EA + 0 SZ + 0 GY)

8.1.2.levelező munkarend: 16 (16 EA + 0 SZ + 0 GY)

8.2.heti óraszám - nappali munkarend: 4

8.3.Az ismeret átadásában alkalmazandó további sajátos módok, jellemzők:
Az előadásokra egyéni felkészülés szükséges, melynek ellenőrzése óra eleji felméréssel történik.

9. A tantárgy szakmai tartalma (magyarul):

A tárgy elsődleges célja az alapvető és létfontosságú szolgáltatásokat, illetve a kritikus rendszereket kiszolgáló elektronikus információs rendszerek védelmét biztosító EU-s szabályozási keretrendszer elsajátítása. A hallgatók megismerik a kritikus rendszerek védelmével kapcsolatos nemzetközi és hazai szabályozást, valamint az ágazati és hatósági feladatokat, hatásköröket, üzemeltetői követelményeket és azok végrehajtását a komplex biztonság szavatolása szempontjából. Betekintést nyernek emellett a 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, a kritikus infrastruktúrák és kritikus információs infrastruktúrák korábbi értelmezésével, a kritikus rendszerek és a kiberbiztonság kapcsolatával, az összefüggések magyarázatával. Bemutatja továbbá a kapcsolódó EU-s és magyar szabályozási környezetet, a hatósági és eseménykezelési tevékenységet Magyarországon, valamint az információbiztonsági követelményrendszert a kritikus rendszerek elektronikus információs rendszereire vonatkozóan.

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

The primary aim of the course is to learn the EU regulatory framework that ensures the protection of electronic information systems serving essential, or vital services and critical systems. Students learn about the international and domestic regulations related to the protection of critical systems, as well as the sectoral and authority type of tasks, purviews, operator requirements and their implementation from the point of view of guaranteeing complex security. In addition, students gain insight into the related planning, documentation, authority and control, and information security tasks. The subject deals with the evolution of the definitional environment from the 2000s to the present, in international and domestic contexts, the previous interpretation of critical infrastructures and critical information infrastructures, the relationship between critical entities and cyber security, and the explanation of the connections. It also presents the related EU and Hungarian regulatory environment, the authorities and incident management activities in Hungary, as well as the information security requirement system for the electronic information systems of critical entities.

10. Elérendő kompetenciák (magyarul):

Tudása

Ismeri a létfontosságú rendszerelemek fogalmát
Ismeri azokat a fontosabb előírásokat a kiberbiztonsággal kapcsolatos hazai és nemzetközi szabályozásokból, amelyek a mindennapi munkáját befolyásolják. Ismeri a létfontosságú rendszerelemek fogalmát és megérti a szervezeti feladatokat a kibervédelemben.

Képességei

Képes támogatni szervezetét a kibervédelmi képességek kialakításában
Képes értelmezni a jogszabályokból eredő követelményeket, továbbá képes megszerezni a szervezet vezetőinek támogatását a jogszabályi megfelelőség kiépítéséhez. Képes a szervezeténél keletkezett információkat oly módon megosztani külső szereplővel, hogy az ne sértse saját szervezetének érdekét, de hatékonyan tudja támogatni a külső felet.

Attitűdje

Hatékony lépéseket tesz a kibertámadások megelőzése érdekében, így csökkentve a szervezete kitettségét
Megérti és elfogadja a nemzetközi kiberjog komplexitását, ennek köszönhetően a munkája során törekszik ennek a komplexitásnak a kezelésére. Szükség esetén támogatja a külső feleket a szervezeténél keletkezett információk megosztásával.

Autonómiája és felelőssége

Tudatosan törekszik a kiberbiztonság sajátosságainak megfelelő, korszerű ismeretek hazai és nemzetközi szinten történő gyakorlati alkalmazására.
Tudatosan törekszik a kiberbiztonság sajátosságainak megfelelő, korszerű ismeretek hazai és nemzetközi szinten történő gyakorlati alkalmazására. Kezdeményezőként dolgozik a technikai és operatív teendők stratégiai célokká való konvertálásában.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge:

Knows specifications of national and international cybersecurity regulations
Specifications of national and international cybersecurity regulations that have an immediate impact on his/her daily work. The concept of critical infrastructures, and understands organizational responsibilities in cybersecurity

Capabilities:

Interpret legal requirements
He/she is capable of interpreting legal requirements furthermore he/she is capable of gaining the support of the organisation's leaders to build regulatory compliance. He/she is capable of sharing information generated within its organisation with an external party in a way that does not harm the interests of its own organisation, but can effectively support the external party

Attitude:
Understand and accept the complexity of international cyber law
An understanding and acceptance of the complexity of international cyber law and thus strives to handle this complexity in his/her work. An ability to support external parties by sharing information generated within the organisat
Autonomy and responsibility:
Implement advanced knowledge characterising cybersecurity on a national and international level
To implement advanced knowledge characterising cybersecurity on a national and international level. Moreover to take the initiative in converting technical and operational tasks into strategic objectives

11. Előtanulmányi követelmények:

nincs

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

12.1. Biztonságpolitikai alapismeretek, EU Biztonsági Stratégia, kapcsolódó nemzeti stratégiák, hazai megközelítések (Basic knowledge of security policy, EU Security Strategy, national strategies, national approaches);12.2. Az infrastruktúrákat és szolgáltatásokat veszélyeztető tényezők (Risks to infrastructures and services);12.3. Infrastruktúra, kritikus infrastruktúra, kritikus szervezet, alapvető szolgáltatás definíciós környezete. Az EU megközelítése és szabályozási mérföldkövei (Definition for infrastructure, critical infrastructure, critical entities, essential services. Protection and regulation of EU critical entities);12.4. A kritikus szervezetek védelmének szabályozása Magyarországon. Történeti előzmények, kiberbiztonsági kapcsolódások (Regulation for the protection of critical entities in Hungary. Historical summary, cyber security connections);12.5. Az üzemeltetői reziliencia terv készítésének célja és alapvető módszere, a biztonsági összekötő szerepe (The purpose and basic method of preparing the operator resilience plan, the role of the security liaison);12.6. Kritikus információs infrastruktúrák fogalomrendszerének és a kapcsolódó szakmai terminológiájának ismertetése. Definíciós környezet evolúciója a kétezres évektől napjainkig, nemzetközi és hazai viszonylatban (Definition of critical information infrastructures and related terminology. Evolution of the definitional environment from the 2000s to the present, internationally and domestically);12.7. Nemzetközi kitekintés a kiberbiztonság fejlődése vonatkozásában. A kritikus szervezetek és kritikus információs rendszerek értelmezésének, összefüggéseinek és eltéréseinek bemutatása (International outlook on the development of cybersecurity. Description of the interpretation, context and divergence of critical entities and critical information infrastructures);12.8. A hálózati és információs rendszerek biztonságával kapcsolatos Európai Uniós szabályozási környezet ismertetése (Description of the regulatory environment in the European Union for the security of network and information systems);12.9. A hatályos irányelvi és rendeleti kötelezettségek a tagállamokban (Details of the obligations of directives and regulations in the Member States);12.10. A hálózati és információs rendszerek biztonságával kapcsolatos magyarországi jogszabályi

követelmények ismertetése, beleértve a szervezeti rendszert, a felelősségi köröket és a kötelezettségeket (Description of the legal requirements in Hungary relating to the security of network and information systems, including the organisational system, responsibilities and obligati);12.11. A kibertámadások megelőzésére vonatkozó eszközök és módszerek bemutatása a hatósági feladatrendszerek keretében (Presentation of the tools and methods for preventing cyber-attacks in the framework of authority task systems);12.12. A kritikus szervezeteket érintő események kezelésének szabályai (The rules for managing events affecting critical information infrastructures);12.13. Információbiztonsági követelmények értelmezése és nevesítése a kritikus szervezetek védelme kapcsán (Interpretation and naming of information security requirements for the protection of critical entities);12.14. Kritikus szervezetek kiberbiztonsága a negyedik ipari forradalomban (Cybersecurity of critical entities in the fourth industrial revolution);

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

2. félév/tavasz;

14. 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.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje

A hallgatók minden előadáshoz kapcsolódóan egyénileg feldolgozandó szakanyagot kapnak, melynek ellenőrzése a következő előadás elején történik: nappali tagozaton alkalmanként 5 tesztkérdés, amelyek mindegyikét legalább 60%-os eredménnyel kell teljesíteni; levelező tagozaton 15 kérdéses teszt kitöltésével, amelyek mindegyikét legalább 50%-os eredménnyel kell teljesíteni. A szorgalmi időszak végén ezek a pontszámok az értékelés részét képezik, nappali tagozaton kiegészül a számonkérés kiegészül egy zárthelyi dolgozat legalább 60%-os teljesítésével.

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

16.1. Az aláírás megszerzésének feltételei:
Az aláírás megszerzésének feltétele a tanórákon való 70 %-os részvétel, és a 16. pont szerinti számonkérések esetében a tagozatonként meghatározott minimum eredmények elérése.

16.2. Az értékelés:

Az írásbeli kollokvium követelménye a tanórákon átadott ismeretekre és a kötelező irodalomra épül. Az írásbeli kollokvium esetében az értékelés a hallgató által 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)

16.3. A kreditek megszerzésének feltételei:

A kreditek megszerzésének feltétele az aláírás megszerzése és legalább elégséges kollokvium (K)Egyéni tanulmányi rend esetén: órai jelenlét nem szükséges, de a félévközi követelmények és a kollokvium változatlanul teljesítendőek.

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. Bonnyai Tünde; Danyek Miklós; Görgey Péter; Kriskó Edina; Molnár Anna; Tikos Anita: Kritikus információs infrastruktúrák védelme - Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára, NKE, Budapest 2022. ISBN: 978-963-498-486-3;2. Kovács László: A kibertér védelme, Dialog Campus, Budapest 2019. ISBN: 9786155889639;3. Kovács László: Kiberbiztonság és -stratégia, Dialog Campus, Budapest 2018. ISBN: 9786155920936;

17.2. Ajánlott irodalom:

1. Bihaly Barbara: A kibervédelem szerepe az Európai Unió közös biztonsági és védelmi politikájában, Hadtudományi Szemle, Budapest 2021.2. Puskás Béla: A kritikus információs infrastruktúrák biztonságos üzemeltetésének vizsgálata hálózatelméleti megközelítésből, az ember-technika-környezet relációjában, OE, Budapest 2017.3. Theron, Paula; Bologna, Sandroc: Critical information infrastructure protection and resilience in the ICT sector, IGI Global, USA 2013. ISBN: 978-146662964-6;

Budapest, 2024

Dr. Szádeczky Tamás, PhD, egyetemi docens, tanszékvezető

Nemzeti Közszolgálati Egyetem
Hadtudományi és Honvédtisztképző Kar

TANTÁRGYI PROGRAM

LFSZE01 Ludovika Fesztivál Szabadegyetem

1. A tantárgy kódja: LFSZE01

2. A tantárgy megnevezése (magyarul): Ludovika Fesztivál Szabadegyetem

3. A tantárgy megnevezése (angolul): Ludovika Festival Open University

4. Kreditérték és képzési karakter:

4.1. 0 kredit

4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 0 % gyakorlat, 100 % elmélet

4.3. Az értékelés: aláírás

5. A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):

5.1. bűnügyi igazgatási alapképzési szak / valamennyi szakirány;5.2. International Public Service Relations mesterképzési szak;5.3. katasztrófavédelem alapképzési szak / valamennyi szakirány;5.4. katonai infokommunikáció alapképzési szak / valamennyi szakirány;5.5. katonai logisztika alapképzési szak / valamennyi szakirány;5.6. katonai nemzetbiztonsági alapképzési szak;5.7. katonai vezetői alapképzési szak / valamennyi szakirány;5.8. kiberbiztonsági mesterképzési szak;5.9. kormányzás és vezetés mesterképzési szak;5.10. közigazgatási mesterképzési szak;5.11. magánbiztonsági alapképzési szak;5.12. nemzetközi biztonság- és védelempolitikai alapképzési szak;5.13. nemzetközi biztonság- és védelempolitikai mesterképzési szak;5.14. nemzetközi igazgatási alapképzési szak (angol nyelven);5.15. nemzetközi közszolgálati kapcsolatok mesterképzési szak / valamennyi szakirány;5.16. nemzetközi vízpolitika és vízdiplomácia mesterképzési szak;5.17. pénzügyi rendészeti alapképzési szak / valamennyi szakirány;5.18. polgári nemzetbiztonsági alapképzési szak / valamennyi szakirány;5.19. rendészeti alapképzési szak / valamennyi szakirány;5.20. rendészeti igazgatási alapképzési szak / valamennyi szakirány;5.21. valamennyi, az államtudományi képzési területhez tartozó alapképzési szak;5.22. valamennyi, az államtudományi képzési területhez tartozó mesterképzési szak;

6. Az oktatásért felelős oktatási szervezeti egység megnevezése:

Elektronikai Hadviselés Tanszék

7. A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:

Prof. Dr. Kovács László, DSc, egyetemi tanár

8. A tanórák száma és típusa

8.1.össz óraszám/félév:

8.1.1.nappali munkarend: 4 (4 EA + 0 SZ + 0 GY)

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

8.2.heti óraszám - nappali munkarend: 1

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

9. A tantárgy szakmai tartalma (magyarul):

Az Egyetem hagyományteremtő céllal indította útjára több mint 10 évvel ezelőtt a Ludovika Fesztivált, amelynek egyik hangsúlyos eleme az Egyetem oktatási, kutatási portfóliójához illeszkedő kétnapos előadássorozat, a Ludovika Fesztivál Szabadegyetem neves nemzetközi szakamberek és véleményformálók közreműködésével. Az érdeklődők (lakosság, egyetemi polgárok) számára nyitott esemény a hallgatók mellett a szélesebb közönségnek is áttekintést kíván adni az Egyetemen folyó és külsős szakmai kutatásokról, az Egyetem tudományos életéről, közérthető módon mutatva be az egyes karok és intézetek specifikus és interdiszciplináris szakterületeit, különös tekintettel a had- és rendészettudomány, a nemzetközi biztonság- és védelempolitika, nemzetközi igazgatás, állam és EU, továbbá a geopolitika és fenntartható fejlődés témakörökben.

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

The Ludovika University of Public Service launched the Ludovika Festival program more than 10 years ago. The main core of the event is the two-day-long Free University lecture series based on the research and training portfolio of University with internationally renowned experts and influencers. The aim of the program is to introduce a summary to the students and the public about the University's internal and external professional research, the scientific life of the University, the specific and interdisciplinary areas of the University's faculties and institutes such as the field of law enforcement, military science, international security and defence policy, international public relations, state, EU, geopolitics and sustainability.

10. Elérendő kompetenciák (magyarul):

Tudása

Ismeretekkel rendelkezik Magyarország történelmével, társadalmi, környezeti jellemzőivel, kulturális örökségével és geopolitikai helyzetével kapcsolatban, valamint a 21. századi világ stratégiai dimenzióiról, az aktuális globális és lokális problémákról és ezek összefüggéseirőlÖsszességében átfogó képpel rendelkezik a rendészettudományi, a hadtudományi, az állam- és jogtudományi területek alapvető tényeiről, irányairól és határairól hazai és nemzetközi vonulatban is.

A hallgató a tantárgy elvégzésével megfelelő ismeretekkel rendelkezik a hadtudományi, a rendészettudományi, a nemzetközi igazgatási, az állam- és társadalomelméleti-, államtudományi kutatásokról, a nemzetbiztonsági munka sajátosságairól.Átfogóan ismeri a közszolgálat – hivatásrendjétől eltérő – további területeinek alapvető tudásanyagát, általános műveltsége erőteljesen bővül, megérti a különböző hátterű jelenségek kapcsolatát, különös tekintettel a nemzetközi, geopolitikai összefüggésekre.

Képességei

Képes hatékonyan értelmezni és értékelni az Európára és Magyarországra ható globális eseményeket és világfolyamatokat, valamint hatékonyan feldolgozza a kapcsolódó információkat, adatokat.Képes rendszerben gondolkozni és felismerni az ökológiai rendszer alapvető szolgáltatásainak hasznosításából eredő kockázatokat és konfliktusokat, továbbá munkaköréhez és feladataihoz kapcsolódóan megoldásokat keresni azok megelőzésére, enyhítésére, megoldására.

Fejlődik a kritikai készsége, lojalitása és felelősségérzete a társadalom és a nemzet iránt. A nemzetközi előadóknak is köszönhetően új szemlélettel és megközelítésekkel találkozik.A megszerzett ismereteket alkalmazott tudásként kezeli. Képessé válik komplex problémák megértésére, geopolitikai összefüggések észrevételére, következtetések megfogalmazására, amelyet hivatásába beépíthet.

Attitűdje

Elkötelezett az ország jövője és sikerei iránt, nyitott az új ismeretekre és kihívásokra, amelyek Magyarország helyét és lehetőségeit érintik a 21. századbanNyitott szakterülete új eredményei, innovációi iránt, törekszik azok megismerésére, megértésére és alkalmazására. Elkötelezett saját szakmai fejlődése iránt. Nyitott arra, hogy a hivatásrendjétől eltérő további közszolgálati hivatásrendek tudásbázisának alapvető ismereteit is elsajátítsa.

A kurzus elvégzése után határozottabb és szélesebb látókörű világszemlélettel fog rendelkezni, közös közszolgálati érték- és fogalomkészlettel bír és nyitott a teljes hazai és nemzetközi közszolgálat egészére, közszolgálati gondolkozása, értékrendje erősödik.Közszolgálati elkötelezettség, ambíció és kíváncsiság jellemzi.Érdeklődése megnő a szakterületével kapcsolatos újító és megőrző feladatok ellátására, a szakmai kihívások komplex szemléletű kezelésére.

Autonómiája és felelőssége

Szabadon és felelős módon viszonyul az Európa és Magyarország jövőjével kapcsolatos kihívásokhoz, valamint az egyéni és közösségi felelősségvállalás lehetőségeihez.

Nagyra értékeli a hivatástudatot és felismeri az egyéni hozzájárulás jelentőségét a közösség, a társadalom és a nemzet életében.Munkáját folyamatos tanulásnak tekinti, saját hibáiból tanul, képes tanácsot kérni és másokat meghallgatni.Önállóan végzi a problémák végig gondolását és a rendelkezésre álló adatok objektív értékelését, elemzését.A szakterületéhez kapcsolódóan megfelelő áttekintő-, rendszerező-, valamint rendszerszemléletű képességgel rendelkezik.

Elérendő kompetenciák (angolul) (Competences – English):
Knowledge:
The student has some knowledge of Hungary’s history, social, environmental characteristics, cultural heritage and geopolitical situation as well as the strategic dimensions of the 21st century world, current global and local problems and their connections. - Overall, the student has a comprehensive overview of the basic facts, trends and boundaries of the fields of law enforcement, military science, state and legal studies at national and international level as well.

By completing the course, the students will have sufficient knowledge of military, law enforcement, public administration, national security work, social theory, and state science research.In general, they know the basic knowledge of the public service - in their own, and different professional rules too.His overall knowledge is expected to be broadened, so that he will be able to understand the complicated connections between different phenomena with particular regards to international and geopolitical contexts.
Capabilities:

The student is able to interpret and evaluate effectively the global events and world processes affecting Europe and Hungary, as well as efficiently process the related information and data.The student is able to think systematically and to identify risks and conflicts arising from the use of the basic services of the ecosystem as well as find solutions to prevent, mitigate and resolve them in relation to his/her work and tasks.

They will improve skills in critical thinking, loyalty, and sense of responsibility towards the society and the nation. Due to the wide range of international lecturers, they will obtain a system-wide perspective and holistic approach.They will be able to use the learned thoughts as part of their practical knowledge.They will be able to interpret complex issues, notice geopolitical correlations and draw conclusions.
Attitude:

The student is committed to public service, recognises the repsonsibility associated with the professions of public service and authentically represents its spirit.The student is open to new findings, innovations in his/her professional field, he/she strives to learn about them, understand them and apply them. He/he is committed to his/her own professional development. In addition to his/her own public service profession, he/she is open to acquire the basic knowledge of the knowledge-base of other public service professions.

After completing the course, students' world view becomes more well-defined.They will boast a set of values closely associated with national and international public service.They are characterized by critical thinking, public service commitment, ambition, and curiosity.Their interest in developing their own profession increases and they are willing to learn and acknowledge innovations in their fields.
Autonomy and responsibility:
The student takes a free and responsible approach to the challenges related to the future of Europe and Hungary, and to the possibilities of the individual and community responsibility.

They will be able to value professionalism and recognise the importance of individual contribution in the life of a community, society and the nation.Consider their own work a constant learning act, learns from their own mistakes, able to ask for advice and listens to others.They will be able to think about problems independently and they can study information in an objective way.They have a systematic and systemic overview ability in relation to their field.

11. Előtanulmányi követelmények:

nincs

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

12.1. A Ludovika Fesztivál Szabadegyetem előadásainak témái szerteágazóak, évről évre változóak, a témák jelentős mértékben reagálnak az aktuális hazai és nemzetközi társadalmi, gazdasági, külpolitikai eseményekre, geopolitikai trendekre az alábbi főbb témakörö (The lecture topics of the Ludovika Festival Open University are varied year by year. To update our students' knowledge in a most up to date fashion, the chosen topics largely react to current homeland and international issues regarding society, foreign po);12.2. Hazai és nemzetközi hadtudományi kutatások eredményeinek bemutatása, hivatásrendi ismeretek nyújtása (Presentation of the Hungarian and international military researches, expound professional rules for army officers);12.3. Hazai és nemzetközi rendészettudományi kutatások eredményeinek bemutatása, hivatásrendi ismeretek nyújtása (Presentation of the Hungarian and international results of law enforcement researches, expound professional rules for police officers);12.4. Közigazgatás-tudományi kutatások eredményeinek a bemutatása, különös tekintettel a nemzetközi igazgatásra, az állammal és az EU-val kapcsolatos ismeretekre. (Presentation of the results of public administration researches special regards to international public relations, state and EU);12.5. Nemzetbiztonsági munka sajátosságainak bemutatása. (Presentation of the specialities of national security work.);12.6. Állam- és társadalomelméleti-, államtudományi kutatások eredményeinek a bemutatása (Presentation of the results of state, social theory and political science research.);12.7. A fenntartható fejlődéssel, vízdiplomáciával és víztudománnyal kapcsolatos kutatások eredményeinek bemutatása. (Presentation of the results of sustainability, water diplomacy and water sciences research.);12.8. Nemzetközi biztonság- védelempolitikai ismeretek nyújtása, különös tekintettel a geopolitikaii összefüggésekre. (Presentation of the results of international security and defence policy with special regards to geopolitical contexts);12.9. A Ludovika Fesztivál Szabadegyetemen az intézmény hallgatói, oktatói, kutatói és külsős szakemberek személyesen is találkozhatnak és közvetlenül megoszthatják legújabb kutatási eredményeiket (With the help of „Ludovika Festival Open University" students, professors, researchers of the university and other experts can meet personally and share their latest research results directly);

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

2. félév/tavasz; 4. félév/tavasz; 6. félév/tavasz; 8. félév/tavasz; 10. félév/tavasz;

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

A részvétel kötelező, igazolt távollét esetén a tantárgy a következő tavaszi félévben pótolandó

15. Félévközi feladatok, ismeretek ellenőrzésének rendje

A Ludovika Fesztivál Szabadegyetem előadásain kötelező a részvétel, az előadásokra a LudEvent felületén kötelező a regisztráció.

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

16.1. Az aláírás megszerzésének feltételei:
Személyes részvétel legalább három előadáson a Ludovika Fesztivál Szabadegyetem keretében.

16.2. Az értékelés:
Aláírás

16.3. A kreditek megszerzésének feltételei:
Személyes részvétel legalább három előadáson a Ludovika Fesztivál Szabadegyetem keretében, melyet LudEventes regisztrációval kell igazolni.

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

17.2. Ajánlott irodalom:

Budapest, 2023

Prof. Dr. Kovács László, DSc, egyetemi tanár

Nemzeti Közszolgálati Egyetem
Államtudományi és Nemzetközi Tanulmányok
Kar

TANTÁRGYI PROGRAM

HKEHVM68 Nemzetállamok a kibertérben

1. A tantárgy kódja: HKEHVM68

2. A tantárgy megnevezése (magyarul): Nemzetállamok a kibertérben

3. A tantárgy megnevezése (angolul): Nation states in cyberspace

4. Kreditérték és képzési karakter:

4.1. 6 kredit

4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 75 % gyakorlat, 25 % elmélet

4.3. Az értékelés: gyakorlati jegy

5. A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):

5.1. kiberbiztonsági mesterképzési szak;

6. Az oktatásért felelős oktatási szervezeti egység megnevezése:

Elektronikai Hadviselés Tanszék

7. A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:

Prof. Dr. Kovács László, DSc, egyetemi tanár

8. A tanórák száma és típusa

8.1.össz óraszám/félév:

8.1.1.nappali munkarend: 84 (0 EA + 0 SZ + 84 GY)

8.1.2.levelező munkarend: 24 (0 EA + 0 SZ + 24 GY)

8.2.heti óraszám - nappali munkarend: 6

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

Kiselőadások készítése és csoportos megbeszélése.Külső, szakmai előadók meghívása és szakmai tevékenységük bemutatása.

9. A tantárgy szakmai tartalma (magyarul):

A tantárgy elsődleges célja, hogy a képzésében részt vevő hallgatók számára megfelelő elméleti alapismeretek elsajátítását biztosítsa a biztonságpolitika, kiberdiplomácia és a kiberhadviselés területén. A hallgatók ismereteket szereznek a biztonsági tanulmányok alapjairól, a nemzetközi kapcsolatokról és intézményrendszerről, továbbá megismerkednek a konfliktusok lokális, regionális és globális vonatkozásaival. Ezen túlmenően a kurzus során kiemelt figyelmet fordítunk a biztonság különböző szektorainak működésére, az új típusú biztonság kihívások megjelenésére és azok következményeire. A hallgatók ennek keretében betekintést kapnak a kiberbiztonság aktuális kérdéseibe, illetve a kibertérben fellépő veszélyek természetébe. A tantárgy emellett átfogó képet nyújt a nemzetközi kapcsolatok kiberteret érintő főbb kérdéseiről, betekintést adva az aktuális trendekről és kihívásokról. A hallgató megismeri azokat a kiberdiplomáciával és kiberhadviseléssel kapcsolatos alapvető fogalmakat, összefüggéseket, amelyek segítséget nyújtanak a komplex témakör megértésében és megalapozzák a jövőbeni szakmai fejlődést. Az általános trendek bemutatásán túl a kurzus alatt kiemelt figyelem irányul a témát érintő olyan meghatározó kérdésekre, mint a kiberteret érintő jogi szabályozás lehetőségei, a kiberhadviselés és a kiberkémkedés veszélyei, a kiberelrettentés, az internet kormányzás

nemzetközi aspektusai, vagy a különböző nemzetközi szervezetek tevékenységei. A képzésben résztvevő hallgatók továbbá megismerkednek a komplex információs támadások összetevőivel és hatásaival. Ezen belül ismertetésre kerülnek az információs infrastruktúrák és támadható pontjaik; a támadási módok; az offenzív kiberműveleti képességek és a kiberelrettentés összefüggései; illetve a kiberhadviselés és a nemzetközi jogi normák öszefüggései. A tárgy kitér a kiberhadviselés összetevőire, amelyben a felderítés és információszerzés; a kibertámadások módszertana; a kibervédelem és stratégia összefüggései kerülnek bemutatásra. A kiberhadviselés kapcsolatainak ismeretése során az információs műveletek, elektronikai hadviselés médiahadviselés és a befolyásolás, valamint a kiberterrorizmus kerül bemutatásra.

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

The primary objective of the course is to provide students with the theoretical background in the fields of security policy, cyber diplomacy and cyber warfare. Students will acquire knowledge of the basics of security studies, international relations and institutions, and will learn about the local, regional and global aspects of conflict. In addition, the course will pay particular attention to the functioning of different sectors of security, the emergence of new types of security challenges and their consequences. Students will gain insights into current issues in cybersecurity and the nature of threats in cyberspace. The course will also provide a comprehensive overview of the main issues in international relations that affect cyberspace, giving insights into current trends and challenges. Students will learn the basic concepts and contexts of cyber diplomacy and cyber warfare that will help them to understand this complex subject and lay the foundations for future professional development. In addition to general trends, the course will also focus on key issues such as the potential for legal regulation of cyberspace, the threats of cyber warfare and cyber espionage, cyber deterrence, international aspects of Internet governance, and the activities of various international organisations. Students will also learn about the components and effects of complex information attacks. In particular, they will learn about information infrastructures and their attack vectors; attack modes; the relationship between offensive cyber operations capabilities and cyber deterrence; and the interrelationship between cyber warfare and international legal norms. The course will cover the components of cyber warfare, in which detection and intelligence gathering; the methodology of cyber attacks; and the interrelationship between cyber defence and strategy will be discussed. Information operations, electronic warfare media warfare and influence, and cyberterrorism will be introduced in the context of cyber warfare.

10. Elérendő kompetenciák (magyarul):

Tudása

Ismeri azokat a fontosabb előírásokat a kiberbiztonsággal kapcsolatos hazai és nemzetközi szabályozásokból, amelyek a mindennapi munkáját befolyásolják.Ismeri a nemzetközi jog alkalmazhatóságát a kibertérben.Ismeri a létfontosságú rendszerelemek fogalmát.Átlátja a kibertérrel kapcsolatos diplomáciai, illetve politikai információmegosztás folyamatát, valamint az esetleges válaszlépéseket.

Ismeri azokat a fontosabb előírásokat a kiberbiztonsággal kapcsolatos hazai és nemzetközi szabályozásokból, amelyek a mindennapi munkáját befolyásolják:hazai és nemzetközi ajánlások részletes megismertetése: NIS, COBIT, ISO 27001.Ismeri a nemzetközi jog alkalmazhatóságát a kibertérben:Megismeri a Tallinn Manual felvetéseid és a nemzetközi jog jelenlegi helyzetét a kibertérre vetítve.

Képességei

Képes értelmezni a jogszabályokból eredő követelményeket.Képes átlátni a kibertér speciális jogállását.Képes a szükséges mértékben alkalmazni a kibertérre vonatkozó nemzetközi jogot kibertámadások esetén.Képes átlátni a kibertér aktuális fenyegetéseit.

Képes értelmezni a jogszabályokból eredő követelményeket:Ismeri a hazai jogszabályi hátteret az Ibtv-től a NIS 2.0-ig.Képes a szükséges mértékben alkalmazni a kibertérre vonatkozó nemzetközi jogot kibertámadások esetén:Képes alkalmazni a nemzetközi jogban rögzített meghatározásaokat egy esetleges hazai/nemeztközi kiberincidens során.
Attitűdje

Megérti és elfogadja a nemzetközi kiberjog komplexitását, ennek köszönhetően a munkája során törekszik ennek a komplexitásnak a kezelésére.A maga komplexitásában tervezi meg az információbiztonsági irányítási rendszert.

Megérti és elfogadja a nemzetközi kiberjog komplexitását, ennek köszönhetően a munkája során törekszik ennek a komplexitásnak a kezelésére:Összefüggéseiben látja a kibertér nemzetközi komplexitását.A maga komplexitásában tervezi meg az információbiztonsági irányítási rendszert:Képes IBIR (ISMS) rendszert tervezni egy szervezetnél.
Autonómiája és felelőssége

Felelősséget vállal a kiberbiztonság összefüggő ismeretének és a meghatározó jogi, szabályozási és gazdasági összefüggések ismeretének alapján a szakmai javaslatok kidolgozásában.Gyakorlatába beépíti és alkalmazza a kiberbiztonsági szakterületen folyó kutatások eredményeit.

Felelősséget vállal a kiberbiztonság összefüggő ismeretének és a meghatározó jogi, szabályozási és gazdasági összefüggések ismeretének alapján a szakmai javaslatok kidolgozásában.Gyakorlatába beépíti és alkalmazza a kiberbiztonsági szakterületen folyó kutatások eredményeit.

Elérendő kompetenciák (angolul) (Competences – English):
Knowledge:

Specifications of national and international cybersecurity regulations that have an immediate impact on his/her daily work.The applicability of international law in cyberspace.Tthe concept of critical infrastructures.The procedure of diplomatic and political information sharing related to cyberspace, as well as possible responses.

Know the main provisions of national and international cybersecurity regulations that affect his/her daily work:Detailed knowledge of national and international recommendations: NIS, COBIT, ISO 27001.Knowledge of the applicability of international law in

cyberspace:Understand the Tallinn Manual's assumptions and the current state of international law as applied to cyberspace.
Capabilities:

He/she is capable of interpreting legal requirements.He/she is capable of having an overview of the special legal status of cyberspace.He/she is capable of applying international law on cyberspace to the extent necessary in the event of cyber-attacks.He/she is capable of understanding the current threats of cyberspace.

Ability to interpret the requirements of the legislation:Knowledge of the national legislative background from national information security law to NIS 2.0.Ability to apply international cyberspace law to the extent necessary in case of cyber attacks:Ability to apply the definitions set out in international law in the event of a domestic/international cyber incident.
Attitude:

An understanding and acceptance of the complexity of international cyber law and thus strives to handle this complexity in his/her work.An effort to design the cyber security management system in its own complexity.

Understands and accepts the complexity of international cyber law, and as a result seeks to address this complexity in his or her work:Understands the international complexity of cyberspace in its context.It designs information security governance in its complexity:Ability to design an ISMS) ystem for an organization.
Autonomy and responsibility:

To take responsibility for making professional proposals based on comprehensive knowledge of cybersecurity and dominant legal, regulatory and economical processes.To incorporate and apply the results of ongoing research in the field of cybersecurity.

To take responsibility for making professional proposals based on comprehensive knowledge of cybersecurity and dominant legal, regulatory and economical processes.To incorporate and apply the results of ongoing research in the field of cybersecurity.

11. Előtanulmányi követelmények:

nincs

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

12.1. Biztonságpolitika (Security Policy);12.2. Fogalmi keretek (Conceptual framework);12.3. Főbb nemzetközi biztonsági szervezetek (Major international security organizations);12.4. Új típusú biztonság kihívások (New security challenges);12.5. Kiberdiplomácia (Cyber Diplomacy);12.6. A kiberteret érintő jogi szabályozás lehetőségei (Opportunities for legal regulation in cyberspace);12.7. Az Európai Unió és a NATO diplomáciai tevékenysége a kibertérben (The European Union and NATO diplomatic activity in cyberspace));12.8. A komplex információs támadások összetevői és hatásai (Complex information attacks and their components and effects);12.9. Az információs infrastruktúrák és támadható pontjaik (Information infrastructures and their vulnerabilities);12.10. Az offenzív kiberműveleti képességek és a kiberelrettentés összefüggései (Relationships between offensive cyber capabilities and cyber-deterrence);12.11. Kiberfelderítés és offenzív kiberműveletek a gyakorlatban (Cyber intelligence and offensive cyber operations in practice);12.12. A felderítés és információszerzés (Intelligence and information gathering);12.13. A kibertámadások módszertana (The methodology of cyberattacks);12.14. Az információs műveletek, elektronikai hadviselés médiahadviselés és a befolyásolás (Information operations, electronic warfare, media warfare and influence);12.15. A kiberterrorizmus (Cyber terrorism);

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

2. félév/tavasz;

14. 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.A kedvezményes tanulmányi rendben tanuló hallgatók esetében az óralátogatás nem kötelező, egyénileg készülnek fel a féléves anyagból. A kredit teljesítéséhez előre egyeztetett időpontban teljesíteniük kell a tesztet (szükség szerint online formában) és el kell készíteniük a féléves feladatot (kiselőadások készítése). Munkájuk értékelése a 16. pont szerint történik.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje

A hallgatók minden előadáshoz kapcsolódóan egyénileg feldolgozandó szakanyagot kapnak, melynek ellenőrzése a következő előadás elején történik, nappali tagozaton 5, levelező tagozaton 15 kérdéses teszt kitöltésével. A félév végén ezek a pontszámok összesítésre kerülnek. Emellett a hallgatók személyre szabott feladatot kapnak, melyet kiselőadás formájában ismertetnek, nappali tagozaton az előadáson, levelező tagozaton videó formátumban rögzített módon.

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

16.1. Az aláírás megszerzésének feltételei:
Az aláírás megszerzésének feltétele a tanórákon való 70 %-os részvétel, a tesztkérdésekből legalább 50% elérése és a kiselőadások (2 előadás) elkészítése.

16.2. Az értékelés:

Az értékelés a hallgató által a félév során megírt teszt és az elaődások 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)

16.3. A kreditek megszerzésének feltételei:

A tantárgyhoz rendelt kredit megszerzésének feltétele a leaglább elégséges értékelés (16.2 pont).

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. Gazdag Ferenc – Remek Éva: A biztonsági tanulmányok alapjai, Dialóg Campus Kiadó, Budapest 2018. ISBN: 978-615-5845-871;2. Kovács László: A kibertér védelme, Dialog Campus, Budapest 2019. ISBN: 9786155889639;3. Kovács László: Kiberbiztonság és -stratégia, Dialog Campus, Budapest 2018. ISBN: 9786155920936;4. Molnár Anna: Az Európai Unió külkapcsolati rendszere és eszközei: a külkapcsolatoktól a kül-, a biztonság- és védelempolitikáig, Dialóg Campus, Budapest 2018. ISBN: 9786155877070;5. Molnár Anna – Molnár Dóra (szerk.): Kiberdiplomácia, Ludovika Egyetemi Kiadó, Budapest 2022. ISBN: 9789635316496;

17.2. Ajánlott irodalom:

1. Egedy Gergely: Bevezetés a nemzetközi kapcsolatok elméletébe, HVG, Budapest 2017. ISBN: 978 963 258 348;2. Jason Andress, Steve Winterfeld : Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, Syngress, London 2013. ISBN: 9780124166721;3. N Schmitt, Michael (szerk.): Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, London 2017. ISBN: 9781316822524;

Budapest, 2024

Prof. Dr. Kovács László, DSc, egyetemi tanár

Nemzeti Közszolgálati Egyetem
Államtudományi és Nemzetközi Tanulmányok
Kar

TANTÁRGYI PROGRAM

ÁKIBTM010 Operációs rendszerek

1. A tantárgy kódja: ÁKIBTM010

2. A tantárgy megnevezése (magyarul): Operációs rendszerek

3. A tantárgy megnevezése (angolul): Operating systems

4. Kreditérték és képzési karakter:

4.1. 6 kredit

4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 25 % gyakorlat, 75 % elmélet

4.3. Az értékelés: kollokvium

5. A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):

5.1. kiberbiztonsági mesterképzési szak;

6. Az oktatásért felelős oktatási szervezeti egység megnevezése:

Kiberbiztonsági Tanszék

7. A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:

Dr. Krasznay Csaba, PhD, egyetemi docens

8. A tanórák száma és típusa

8.1.össz óraszám/félév:

8.1.1.nappali munkarend: 56 (56 EA + 0 SZ + 0 GY)

8.1.2.levelező munkarend: 16 (16 EA + 0 SZ + 0 GY)

8.2.heti óraszám - nappali munkarend: 4

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

9. A tantárgy szakmai tartalma (magyarul):

A tárgy célja a hallgatók megismertetése az operációs rendszerek által kínált szolgáltatásokkal és segédprogramokkal, valamint az általuk kínált erőforrások kezelésével. A tárgyban a következő területek kerülnek bemutatásra: az operációs rendszerek felépítése, a folyamatok kezelése és szinkronizálása, a memória- és háttértármenedzsment, a fájlrendszer, valamint az operációs rendszerek védelmi rendszere. A hallgatóknak emellett meg kell ismerkedniük a Linux és Windows implementációinak alapvető jellemzőivel is.

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

The aim of the course is to familiarise students with the services and utilities offered by operating systems and the management of the resources they provide. The following areas will be covered: operating system architecture, process management and synchronisation, memory and storage management, file systems, and operating system security. Students will also be introduced to the basics of Linux and Windows implementations.

10. 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 átlátni a kibertér aktuális fenyegetéseit.
-
Attitűdje
Partner abban, hogy se a szervezete, se ő maga ne váljon kibertámadás áldozatává.
-
Autonómiája és felelőssége
Vállalja a szakterület, a szakmai praxis módszertanának fejlesztéséhez szükséges elméleti, tudományos kutatási és gyakorlati információk beszerzésének, értékelésének és hasznosításának végrehajtását. Önállóan és pontosan vesz részt a kiberbiztonsági fenyegetések technológiai, politikai és adminisztratív megoldásában.
-

Elérendő kompetenciák (angolul) (Competences – English):
Knowledge:
Defence solutions against cyber attacks. 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 understanding the current threats of cyberspace.
-
Attitude:
An ability to cooperate in preventing his/her organisation and him/herself from becoming a victim of a cyber attack.
-
Autonomy and responsibility:
To obtain, evaluate and utilize theoretical, scientific and practical information necessary for the improvement of the field and the methodology of professional practice. To take part in providing technological, political and administrative solutions to cyber threats.
-

11. Előtanulmányi követelmények:

nincs

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

12.1. Bevezetés (Introduction);12.2. Az operációs rendszerek felépítése (Operating System

Structures);12.3. Folyamatok (Processes);12.4. Szálak és konkurencia (Threads and Concurrency);12.5. A CPU időzítése (CPU Scheduling);12.6. A szálak szinkronizálása (Process Synchronization);12.7. Memóriamenedzsment: a fő memória (Memory Management: the Main Memory);12.8. Memóriamenedzsment: a virtuális memória (Memory Management: Virtual Memory);12.9. Háttértárak felépítése (Mass Storage Structure);12.10. I/O rendszerek (I/O Systems);12.11. Fájlrendszerek (File Systems);12.12. Az operációs rendszerek biztonsága és védelme (Security);12.13. A Linux operációs rendszer (Linux Operating System);12.14. A Windows operációs rendszer (Windows Operating System);

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

2. félév/tavasz;

14. 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.A kedvezményes tanulmányi rendben tanuló hallgatók esetében az óralátogatás nem kötelező, egyénileg készülnek fel a féléves anyagból. A kredit teljesítéséhez előre egyeztetett időpontban teljesíteniük kell a zárthelyi dolgozatokat, szükség szerint online formában. Munkájuk értékelése a 16. pont szerint történik.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje

A félév során a hallgatók két zárthelyi dolgozatot írnak. Az első zárthelyi a 13.1-13.8., a második a 13.9-13.14 témákat ellenőrzi. A zárthelyi dolgozat értékelése ötfokozatú skálán történik az alábbiak szerint: 51 %-tól elégséges, 63 %-tól közepes, 75 %-tól jó, 87 %-tól jeles. Sikertelen zárthelyi dolgozatot a félév utolsó tanulmányi hetében lehet pótolni.

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

16.1. Az aláírás megszerzésének feltételei:
Az aláírás megszerzésének feltétele a tanórákon való 70 %-os részvétel és a zárthelyi dolgozatok mindegyikének legalább elégséges osztályzata.

16.2. Az értékelés:

Az írásbeli kollokvium követelménye a tanórákon átadott ismeretekre és a kötelező irodalomra épül. Az írásbeli kollokvium esetében az értékelés a hallgató által 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)

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

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. Moodle-re feltett segédanyagok (tankönyvi fejezetek, feladatok, ppt-k),.2. Abraham Silberschatz, Greg Gagne, Peter B. Galvin: Operating System Concepts, 10th Edition, John Wiley & Sons, 2018. ISBN: 978-1119439257;3. Koczka Ferenc: Operációs rendszerek online tananyag,.

17.2. Ajánlott irodalom:

1. Microsoft MD-102 Explore endpoint management,.2. Andrew S. Tanenbaum: Operációs rendszerek, Panem, Budapest 2007. ISBN: 9789635451761;3. Emmett Dulaney: Linux, Taramix, 2016. ISBN: 2399973567770;

Budapest, 2024

Dr. Krasznay Csaba, PhD, egyetemi docens

Nemzeti Közszolgálati Egyetem
Államtudományi és Nemzetközi Tanulmányok
Kar

TANTÁRGYI PROGRAM

ÁISZLM201 Szaknyelvi ismeretek I. - Hatékony előadás és tárgyalás technika

1. A tantárgy kódja: ÁISZLM201

2. A tantárgy megnevezése (magyarul): Szaknyelvi ismeretek I. - Hatékony előadás és tárgyalás technika

3. A tantárgy megnevezése (angolul): LSP I. - Effective presentation and negotiation skills

4. Kreditérték és képzési karakter:

4.1. 2 kredit

4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 100 % gyakorlat, 0 % elmélet

4.3. Az értékelés: gyakorlati jegy

5. A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):

5.1. fejlesztéspolitikai programmenedzsment mesterképzési szak;5.2. International Public Service Relations mesterképzési szak;5.3. kiberbiztonsági mesterképzési szak;5.4. kommunikáció- és médiatudomány mesterképzési szak / valamennyi specializáció;5.5. kormányzás és vezetés mesterképzési szak;5.6. közgazdálkodás és közpolitika mesterképzési szak;5.7. közigazgatási mesterképzési szak;5.8. nemzetközi közszolgálati kapcsolatok mesterképzési szak / valamennyi szakirány;5.9. nemzetközi tanulmányok mesterképzési szak / valamennyi specializáció;5.10. nemzetközi tanulmányok mesterképzési szak (angol nyelven) / valamennyi specializáció;

6. Az oktatásért felelős oktatási szervezeti egység megnevezése:

Idegennyelvi és Szaknyelvi Lektorátus

7. A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:

Miklósy Hajnalka

8. A tanórák száma és típusa

8.1.össz óraszám/félév:

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

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

8.2.heti óraszám - nappali munkarend: 2

8.3.Az ismeret átadásában alkalmazandó további sajátos módok, jellemzők:
Interaktív online oktatási platformok használata a hallgatók és az oktató által az élményalapú oktatás biztosítása és a hallgatói autonómia fejlesztésének érdekében, pl. Kahoot, Quizlet, Mentimeter. A hallgatók quizeket, szókincsgyűjteményeket és

kérdőíveket készítenek önmaguk és egymás számára. Az oktató ezeket ellenőrzi és kiegészíti és integrálja az oktatási folyamatba.

9. A tantárgy szakmai tartalma (magyarul):

Az ismeretanyag a hatékony szóbeli kommunikáció és prezentáció nyelvi/szaknyelvi eszközeit öleli fel. Az ismeretanyag kiterjed az előadástartás módszertanának idegennyelven történő megismerésére, elemzésére, angol nyelven tartott előadások, megbeszélések, tárgyalások és írásbeli kommunikáció nyelvének elsajátítására. A kurzus teljesítésével jártasságot szereznek az alapvető kommunikációs készségek használatában és képesek lesznek ezeket megfelelően alkalmazva a fent említett témákban írásban és szóban egyaránt megnyilvánulni.

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

The course aims to provide students with the relevant vocabulary of effective communication within the organization, such as presentation. Students study the theoretical and practical background of presentation, meetings, negotiations and written communication. By completing the course, students will become acquainted basic communication skills and will be able to exchange ideas about them both in written and oral forms.

10. Elérendő kompetenciák (magyarul):

Tudása

Rendelkezik a szakmai feladatellátásához szükséges idegennyelv tudással legalább egy idegen nyelven.Rendelkezik a közigazgatási területre jellemző szaknyelvi ismeretekkel.

Alapvetően érti a társadalmi problémákat.Részletesen ismeri a hatékony szóbeli és írásbeli hivatalos kommunikáció eszköztárát.Összefüggéseiben látja és csoportosítani tudja a különböző társadalmi problémák lehetséges megoldásait.

Képességei

Szakmai feladatellátása során megfelelően alkalmaz legalább egy idegennyelvet.Rendelkezik a közigazgatási szakterületre jellemző szaknyelvi kommunikációs készségekkel.

Szakszerűen és komplex módon használja a szóbeli és írásbeli kommunikációs eszközöket.Munkahelyi feladatokat végez nemzetközi, multikulturális közegben.Képes idegen nyelven munkahelyi környezetben szakmai témákban hatékonyan kommunikálni szóban és írásban.Prezentációkat és összefoglalókat készít.

Attitűdje

-

Törekszik a megszerzett átfogó ismeretek rendszerszintű alkalmazására, idegen nyelvű környezetben is.Nyitottá válik a szakmai diskurzusokra idegen nyelven is.Kritikusan gondolkodik saját szakterületén idegen nyelven is.Törekszik a nyelvi pontosságra, igényességre.

Autonómiája és felelőssége

-

Önállóan előadást készít és tart idegen nyelven.Másokkal együttműködve kifejti álláspontját, reagál más résztvevő véleményére és döntéseket hoz idegen nyelven.Segítséggel idegen nyelvű összefoglalókat készít.

Elérendő kompetenciák (angolul) (Competences – English):
Knowledge:

The student has the necessary foreign language skills in at least one foreign language to fulfil his/her professional duties.He/she is familiar with the technical language specific to the administrative area.

He/She fundamentally understands social problems.He/She has a variety of tools how to communicate in formal writing and speaking.He/She understands the complexity of different solutions to social problems and is able to group them.
Capabilities:

During the performance of his/her professional duties, the student is able to apply at least one foreign language properly.He/she is capable of using his/her professional language communication skills typical of the public administration field.

He/She uses written and oral tools of communication accurately and professionally.He/She works in an international and multicultural environment.He/She communicates efficiently about professional topics at his/her workplace both in oral and written forms in foreign languages.He/She makes and gives presentations.
Attitude:
-

He/She intends to apply the comprehensive knowledge acquired systematically in a foreign environment.He/She becomes open to professional discourses in a foreign language as well.He/She thinks critically on his/her own professional field in a foreign language as well.He/She intends to become critical and accurate regarding his/her language skills.
Autonomy and responsibility:
-

He/She prepares and holds presentations on his/her own in a foreign language.He/She expresses his/her opinion, reacts to others' opinion and makes decisions by collaborating with others in a foreign language.He/She prepares summaries with help.

11. Előtanulmányi követelmények:

nincs

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

12.1. Bevezetés (Introduction)12.2. Látogatók fogadása, az együttműködés megfelelő kereteinek kialakítása (Welcoming visitors, setting the tone)12.3. Ajánlatok, meghívások, felkérések elfogadása, udvarias visszautasítása. Email írás (Accepting and rejecting offers and invitations appropriately. Writing emails.)12.4. Hatékony kérdésfeltevés, megfelelő reagálás. (Effective questioning, appropriate reactions.)12.5. Együttműködő magatartásformák kialakítása, a beszélgetés menetének fenntartása. (Cooperation, keeping the discussion going.)12.6. Búcsúzás, a kapcsolatok megerősítése. (Farewell, strengthening connections.)12.7. Zárthelyi dolgozat. Téma 1-6. (Test I. Unit 1-6.)12.8. A hatékony értekezlet legfontosabb ismérvei. (Effective meetings.)12.9. Értekezlet megnyitása: célkitűzések, eljárás menete, tisztségviselők, résztvevők. (Opening a meeting: goals, process, participants.)12.10. Értekezlet napirendjének, struktúrájának folyamatos kontrollja. (Setting and keeping to the agenda.)12.11. Érveléstechnika, problémamegoldás. (Argumentation and problem-solving.)12.12. Közbeszólások, eltérés a tárgytól; udvarias visszautasítási formulák. (Interruptions, digressions, polite rejections.)12.13. Felhívás ötletbörzére – új ötletek ösztönzése, visszajelzések. Notórius közbeszólókkal, domináns felszólalókkal való megfelelő bánásmód. (Brainstorming - encouraging ideas, feedback. Dealing with problematic people.)12.14. Zárthelyi dolgozat. Téma 8-13. (Test II. Unit 8-13.)

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

bármely félévben;

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

A hallgató köteles a foglalkozások min. 75%-án részt venni, rövid/tartós távolmaradás indokolt esetben (orvosi, szolgálati) pótolható, amely pótlás egyéni megbeszélés szerint történik. Egyéb esetből fakadó több mint 25%-os hiányzás esetén, a félév teljesítése nem írható alá.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje

Két zárthelyi dolgozat /időpontja a tantárgyi tematikában látszik/Egy nyelvi portfólió létrehozása a félév folyamán, melynek elemei:- egy prezentáció tartása (szinttől függően 5-10 perces idegen nyelvű prezentáció tartása, melyet az oktatóval a félév elején egyeztetnek a hallgatók. Témája: a tantárgyi tematika egyik témájának altémája, a tematika által meghatározott héten.)- egy cikk összefoglalása 6-8 mondatban;legalább kettő interaktív feladat készítése (kahoot, quizlet gyűjtemény);Osztályzat ötfokozatú skálán / 50% elégséges, 60% közepes, 75% jó, 90%tól jeles/Dolgozatok pótlása a dolgozat utáni legelső alkalommal.

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

16.1. Az aláírás megszerzésének feltételei:
Részvétel a tanórák minimum 75%-án. Két zárthelyi dolgozat megírása. Nyelvi portfólió elemeinek elkészítése.

16.2. Az értékelés:
Gyakorlati jegy(GYJ). Osztályzat ötfokozatú skálán / 50% elégséges, 60% közepes, 75% jó, 90%tól jeles/. Zárthelyi dolgozatok 20-20%-ot, míg a nyelvi portfólió 60%-át teszi ki a gyakorlati jegynek.

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

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. Adrian Wallwork: Business Options, Oxford University Press, 2000. ISBN: 0-19-457234-X;2. Frances Eales - Steve Oakes: Speakout, Pearson, Harlow 2012.. ISBN: ISBN13: 9781408276099 ;3. Jeremy Comfort: Effective Presentations, Oxford University Press, 1996. ISBN: 13 9780194570657;

17.2. Ajánlott irodalom:

1. Oxford Advanced Learner's Dictionary, Oxford University Press, 2010. ISBN: 9780194799027;2. Berridge, Geoff R. – Lloyd, Lorna: The Palgrave Macmillan Dictionary of Diplomacy, Palgrave Macmillan, New York 2012.. ISBN: 9780230302983 ;

Budapest, 2024

Miklósy Hajnalka

Nemzeti Közszolgálati Egyetem
Államtudományi és Nemzetközi Tanulmányok
Kar

TANTÁRGYI PROGRAM

ÁISZLM202 Szaknyelvi ismeretek II. - Európai Uniós szakpolitikák

1. A tantárgy kódja: ÁISZLM202

2. A tantárgy megnevezése (magyarul): Szaknyelvi ismeretek II. - Európai Uniós szakpolitikák

3. A tantárgy megnevezése (angolul): LSP II. - EU policies

4. Kreditérték és képzési karakter:

4.1. 2 kredit

4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 100 % gyakorlat, 0 % elmélet

4.3. Az értékelés: gyakorlati jegy

5. A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):

5.1. fejlesztéspolitikai programmenedzsment mesterképzési szak;5.2. International Public Service Relations mesterképzési szak;5.3. kiberbiztonsági mesterképzési szak;5.4. kommunikáció- és médiatudomány mesterképzési szak / valamennyi specializáció;5.5. kormányzás és vezetés mesterképzési szak;5.6. közgazdálkodás és közpolitika mesterképzési szak;5.7. közigazgatási mesterképzési szak;5.8. nemzetközi közszolgálati kapcsolatok mesterképzési szak / valamennyi szakirány;5.9. nemzetközi tanulmányok mesterképzési szak / valamennyi specializáció;5.10. nemzetközi tanulmányok mesterképzési szak (angol nyelven) / valamennyi specializáció;

6. Az oktatásért felelős oktatási szervezeti egység megnevezése:

Idegennyelvi és Szaknyelvi Lektorátus

7. A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:

Nagy Zsuzsanna

8. A tanórák száma és típusa

8.1.össz óraszám/félév:

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

8.1.2.levelező munkarend: 28 (0 EA + 0 SZ + 28 GY)

8.2.heti óraszám - nappali munkarend: 2

8.3.Az ismeret átadásában alkalmazandó további sajátos módok, jellemzők:
Az ismeret átadásában alkalmazandó további sajátos módok, jellemzők: Az ismeret átadásában alkalmazandó további sajátos módok, jellemzők: Interaktív online oktatási platformok használata a hallgatók és az oktató által az élményalapú oktatás biztosítása és a hallgatói autonómia fejlesztésének érdekében, pl. Kahoot, Quizlet, Mentimeter. A

hallgatók quizeket, szókincsgyűjteményeket és kérdőíveket készítenek önmaguk és egymás számára. Az oktató ezeket ellenőrzi és kiegészíti és integrálja az oktatási folyamatba.

9. A tantárgy szakmai tartalma (magyarul):

Az ismeretanyag az EU történetén, intézményin, politikáin keresztül megismereteti a hallgatókat az EU speciális szókincsével. A szókincsfejlesztésen túl különös hangsúlyt kap az olvasás-, írás-, beszédkészség és a beszédértés fejlesztése. A kurzus teljesítésével jártasságot szereznek az EU alapvető fogalmainak körében és képesek lesznek ezeket megfelelően alkalmazva a fent említett témákban írásban és szóban egyaránt megnyilvánulni.

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

The course covers the special vocabulary of the European Union through the topics of EU history, institutions and different policies. Besides expanding their vocabulary, students improve their reading, writing, speaking and listening skills. By completing the course, students will become acquainted with the concepts and notions of the EU and will be able to exchange ideas about them both in written and oral forms.

10. Elérendő kompetenciák (magyarul):

Tudása

Rendelkezik a szakmai feladatellátásához szükséges idegennyelv tudással legalább egy idegen nyelven.Rendelkezik a közigazgatási területre jellemző szaknyelvi ismeretekkel.

Alapvetően érti az történetét és intézményrendszerét.Részletesen ismeri az EU döntéshozatali mechanizmusát és törvényhozását.Összefüggéseiben látja és csoportosítani tudja az EU különböző szakpolitikáit.

Képességei

Szakmai feladatellátása során megfelelően alkalmaz legalább egy idegennyelvet.Rendelkezik a közigazgatási szakterületre jellemző szaknyelvi kommunikációs készségekkel.

Szakszerűen és komplex módon használja a az EU szókincsét.Munkahelyi feladatokat végez nemzetközi, multikulturális közegben.Képes idegen nyelven munkahelyi környezetben szakmai témákban hatékonyan kommunikálni szóban és írásban.Prezentációkat és összefoglalókat készít.

Attitűdje

-

Törekszik a megszerzett átfogó ismeretek rendszerszintű alkalmazására, idegen nyelvű környezetben is.Nyitottá válik a szakmai diskurzusokra idegen nyelven is.Kritikusan gondolkodik saját szakterületén idegen nyelven is.Törekszik a nyelvi pontosságra, igényességre.

Autonómiája és felelőssége

-

Önállóan előadást készít és tart idegen nyelven.Másokkal együttműködve kifejti álláspontját, reagál más résztvevő véleményére és döntéseket hoz idegen nyelven.Segítséggel idegen nyelvű összefoglalókat készít.

Elérendő kompetenciák (angolul) (Competences – English):
Knowledge:

The student has the necessary foreign language skills in at least one foreign language to fulfil his/her professional duties.He/she is familiar with the technical language specific to the administrative area.

He/She fundamentally understands the history and the institutions of the EU.He/She has detailed information about decision-making and legislation in the EU.He/She understands the complexity of different electoral systems and is able to group them.
Capabilities:

During the performance of his/her professional duties, the student is able to apply at least one foreign language properly.He/she is capable of using his/her professional language communication skills typical of the public administration field.

He/She uses EU terminology professionally.He/She works in an international and multicultural environment.He/She communicates efficiently about professional topics at his/her workplace both in oral and written forms in foreign languages.He/She makes and gives presentations.
Attitude:
-

He/She intends to apply the comprehensive knowledge acquired systematically in a foreign environment.He/She becomes open to professional discourses in a foreign language as well.He/She thinks critically on his/her own professional field in a foreign language as well.He/She intends to become critical and accurate regarding his/her language skills.
Autonomy and responsibility:
-

He/She prepares and holds presentations on his/her own ina foreign language.He/She expresses his/her opinion, reacts to others' opinion and makes decisions by collaborating with others in a foreign language.

11. Előtanulmányi követelmények:

nincs

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

12.1. Bevezetés (Introduction);12.2. Munkavállalás az EU-ban (Working in the EU);12.3. EPSO (EPSO);12.4. Döntéshozatal az EU-ban (Decision-making in the EU);12.5. Törvényhozás az EU-ban (Legislation in the EU);12.6. Főigazgatóságok (Directorate Generals);12.7. Külügyi és biztonságpolitikai főképviselő (High Representative for Foreign Affairs and Security Policy);12.8. Zárthelyi dolgozat I. (Test I.);12.9. Az EU tanácsadó szervei (Advisory bodies of the EU);12.10. Kohéziós politika (Cohesion policy);12.11. Agrárpolitika (CAP);12.12. Szociálpolitika (Social policy);12.13. Biztonság és rendvédelem az EU-ban (Security and Law enforcement in the EU);12.14. Zárthelyi dolgozat II. (Test II.);

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

bármely félévben;

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

A hallgató köteles a foglalkozások min. 75%-án részt venni. Rövid/tartós távolmaradás indokolt esetben (orvosi, szolgálati) pótolható, amely pótlás egyéni megbeszélés szerint történik. Egyéb esetből fakadó több mint 25%-os hiányzás esetén, a félév teljesítése nem írható alá.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje

Két zárthelyi dolgozat /időpontja a tantárgyi tematikában látszik/.Egy nyelvi portfólió létrehozása a félév folyamán, melynek elemei:- egy prezentáció tartása (szinttől függően 5-10 perces idegen nyelvű prezentáció tartása, melyet az oktatóval a félév elején egyeztetnek a hallgatók. Témája: a tantárgyi tematika egyik témájának altémája, a tematika által meghatározott héten.)- egy cikk összefoglalása 6-8 mondatban;- legalább kettő interaktív feladat készítése (kahoot, quizlet gyűjtemény);Osztályzat ötfokozatú skálán / 50% elégséges, 60% közepes, 75% jó, 90% jeles/. Dolgozatok pótlása a dolgozat utáni legelső alkalommal.

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

16.1. Az aláírás megszerzésének feltételei:
Részvétel a tanórák minimum 75%-án. Két zárthelyi dolgozat megírása. Nyelvi portfólió elemeinek elkészítése.

16.2. Az értékelés:
Gyakorlati jegy(GYJ). Osztályzat ötfokozatú skálán / 50% elégséges, 60% közepes, 75% jó, 90%-tól jeles/. Zárthelyi dolgozatok 20-20%-ot, míg a nyelvi portfólió 60%-át teszi ki a gyakorlati jegynek.

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

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. Colm Downes: A Practical Guide to the European Union, British Council, 2011.2. Pascal Fontaine: Europe in 12 lessons, European Commission , 2017. ISBN: 978-92-79-53577-2;

17.2. Ajánlott irodalom:

1. Adrian Wallwork: Business Options, Oxford University Press, 2000. ISBN: 0-19-457234-X;

Budapest, 2024

Nagy Zsuzsanna

Nemzeti Közszolgálati Egyetem
Államtudományi és Nemzetközi Tanulmányok
Kar

TANTÁRGYI PROGRAM

ÁISZLM203 Szaknyelvi ismeretek III. - Gazdasági szaknyelv

1. A tantárgy kódja: ÁISZLM203

2. A tantárgy megnevezése (magyarul): Szaknyelvi ismeretek III. - Gazdasági szaknyelv

3. A tantárgy megnevezése (angolul): LSP III. - Business English

4. Kreditérték és képzési karakter:

4.1. 2 kredit

4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 100 % gyakorlat, 0 % elmélet

4.3. Az értékelés: gyakorlati jegy

5. A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):

5.1. fejlesztéspolitikai programmenedzsment mesterképzési szak;5.2. International Public Service Relations mesterképzési szak;5.3. kiberbiztonsági mesterképzési szak;5.4. kommunikáció- és médiatudomány mesterképzési szak / valamennyi specializáció;5.5. kormányzás és vezetés mesterképzési szak;5.6. közgazdálkodás és közpolitika mesterképzési szak;5.7. közigazgatási mesterképzési szak;5.8. nemzetközi közszolgálati kapcsolatok mesterképzési szak / valamennyi szakirány;5.9. nemzetközi tanulmányok mesterképzési szak / valamennyi specializáció;5.10. nemzetközi tanulmányok mesterképzési szak (angol nyelven) / valamennyi specializáció;

6. Az oktatásért felelős oktatási szervezeti egység megnevezése:

Idegennyelvi és Szaknyelvi Lektorátus

7. A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:

Szekrényesné Dr. Rádi Éva Ágota, PHD, adjunktus

8. A tanórák száma és típusa

8.1.össz óraszám/félév:

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

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

8.2.heti óraszám - nappali munkarend: 2

8.3.Az ismeret átadásában alkalmazandó további sajátos módok, jellemzők:
Interaktív online oktatási platformok használata a hallgatók és az oktató által az élményalapú oktatás biztosítása és a hallgatói autonómia fejlesztésének érdekében, pl. Kahoot, Quizlet, Mentimeter. A hallgatók quizeket, szókincsgyűjteményeket és kérdőíveket készítenek önmaguk és egymás számára. Az oktató ezeket ellenőrzi és kiegészíti és integrálja az oktatási folyamatba.

9. A tantárgy szakmai tartalma (magyarul):

A diákok a kurzus során elsajátítják a gazdasági élet alapjait, alapszókincsét idegen nyelven. A kurzus teljesítésével jártasságot szereznek az alapvető gazdasági fogalmak körében és képesek lesznek ezeket megfelelően alkalmazva a fent említett témákban írásban és szóban egyaránt megnyilvánulni.

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

Students become familiar with the basics and the terminology of the economy. By completing the course, students will become acquainted with the concepts and notions of governance systems and will be able to exchange ideas about them both in written and oral forms.

10. Elérendő kompetenciák (magyarul):

Tudása

Rendelkezik a szakmai feladatellátásához szükséges idegennyelv tudással legalább egy idegen nyelven.Rendelkezik a közigazgatási területre jellemző szaknyelvi ismeretekkel.

Alapvetően érti a gazdasági mechanizmusokat.Részletesen ismeri a hatékony szóbeli és írásbeli hivatalos kommunikáció eszköztárát.Összefüggéseiben látja és csoportosítani tudja a különböző gazdasági események lehetséges hatásait.

Képességei

Szakmai feladatellátása során megfelelően alkalmaz legalább egy idegennyelvet.Rendelkezik a közigazgatási szakterületre jellemző szaknyelvi kommunikációs készségekkel.

Szakszerűen és komplex módon használja a szóbeli és írásbeli kommunikációs eszközöket.Munkahelyi feladatokat végez nemzetközi, multikulturális közegben.Képes idegen nyelven munkahelyi környezetben szakmai témákban hatékonyan kommunikálni szóban és írásban.Prezentációkat és összefoglalókat készít.

Attitűdje

-

Törekszik a megszerzett átfogó ismeretek rendszerszintű alkalmazására, idegen nyelvű környezetben is.Nyitottá válik a szakmai diskurzusokra idegen nyelven is.Kritikusan gondolkodik saját szakterületén idegen nyelven is.Törekszik a nyelvi pontosságra, igényességre.

Autonómiája és felelőssége

-

Önállóan előadást készít és tart idegen nyelven.Másokkal együttműködve kifejti álláspontját, reagál más résztvevő véleményére és döntéseket hoz idegen nyelven.Segítséggel idegen nyelvű összefoglalókat készít.

Elérendő kompetenciák (angolul) (Competences – English):
Knowledge:

The student has the necessary foreign language skills in at least one foreign language to fulfil his/her professional duties.He/she is familiar with the technical language specific to the administrative area.

He/She fundamentally understands economic operations.He/She has a variety of tools how to communicate in formal writing and speaking.He/She understands the effects of different economic mechanisms and is able to group them.
Capabilities:

During the performance of his/her professional duties, the student is able to apply at least one foreign language properly.He/she is capable of using his/her professional language communication skills typical of the public administration field.

He/She uses written and oral tools of communication accurately and professionally.He/She works in an international and multicultural environment.He/She communicates efficiently about professional topics at his/her workplace both in oral and written forms in foreign languages.He/She makes and gives presentations.
Attitude:
-

He/She intends to apply the comprehensive knowledge acquired systematically in a foreign environment.He/She becomes open to professional discourses in a foreign language as well.He/She thinks critically on his/her own professional field in a foreign language as well.He/She intends to become critical and accurate regarding his/her language skills.
Autonomy and responsibility:
-

He/She prepares and holds presentations on his/her own in a foreign language.He/She expresses his/her opinion, reacts to others' opinion and makes decisions by collaborating with others in a foreign language.He/She prepares summaries with help.

11. Előtanulmányi követelmények:

nincs

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

12.1. Bevezetés (Introduction);12.2. Kapcsolattartás partnerekkel (Keeping contact with business partners);12.3. Interkulturális management (Intercultural management);12.4. Külkereskedelem (Foreign trade);12.5. Piaci elemzés, grafikon leírás (Market and graph analysis);12.6. Értékesítés (Sales);12.7. Befektetések (Investments);12.8. Zárthelyi dolgozat 1 (Test 1);12.9. A környezetvédelem gazdasági vonatkozásai (Economic aspects

of environmental protection);12.10. Logisztika (Logistics);12.11. Az EU gazdasága (The economy of the EU);12.12. A gazdasági válság hatása az EU gazdaságára (The effects of the economic crisis on the EU);12.13. Célnyelvi országok gazdasága (The economy of leading countries);12.14. Zárthelyi dolgozat 2 (Test 2);

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

bármely félévben;

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

A hallgató köteles a foglalkozások min. 75%-án részt venni.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje

Két zárthelyi dolgozat /időpontja a tantárgyi tematikában látszik/Egy nyelvi portfólió létrehozása a félév folyamán, melynek elemei:- egy prezentáció tartása (szinttől függően 5-10 perces idegen nyelvű prezentáció tartása, melyet az oktatóval a félév elején egyeztetnek a hallgatók. Témája: a tantárgyi tematika egyik témájának altémája, a tematika által meghatározott héten.)- egy cikk összefoglalása 6-8 mondatban;- legalább kettő interaktív feladat készítése (kahoot, quizlet gyűjtemény);Osztályzat ötfokozatú skálán / 50% elégséges, 60% közepes, 75% jó, 90% -tól jeles/Dolgozatok pótlása a dolgozat utáni legelső alkalommal.

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

16.1. Az aláírás megszerzésének feltételei:
Részvétel a tanórák minimum 75%-án. Két zárthelyi dolgozat megírása. Nyelvi portfólió elemeinek elkészítése.

16.2. Az értékelés:
Gyakorlati jegy(GYJ). Osztályzat ötfokozatú skálán / 50% elégséges, 60% közepes, 75% jó, 90%tól jeles/. Zárthelyi dolgozatok 20-20%-ot, míg a nyelvi portfólió 60%-át teszi ki a gyakorlati jegynek.

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

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. Jeremy Comfort: Effective Presentations, Oxford University Press, 1996. ISBN: 13 9780194570657;2. Jon Wortmann: Mastering Communication at Work, McGraw-Hill Education, 2021. ISBN: 1260474127;

17.2. Ajánlott irodalom:

1. Oxford Advanced Learner’s Dictionary, Oxford University Press, 2010. ISBN: 9780194799027;2. Adrian Wallwork: Business Options, Oxford University Press, 2000. ISBN: 0-19-457234-X;

Budapest, 2024

Szekrényesné Dr. Rádi Éva Ágota, PHD, adjunktus

Nemzeti Közszolgálati Egyetem
Államtudományi és Nemzetközi Tanulmányok
Kar

TANTÁRGYI PROGRAM

ÁISZLM204 Szaknyelvi ismeretek IV. - Jogi szaknyelv

1. A tantárgy kódja: ÁISZLM204

2. A tantárgy megnevezése (magyarul): Szaknyelvi ismeretek IV. - Jogi szaknyelv

3. A tantárgy megnevezése (angolul): LSP IV. - Legal English

4. Kreditérték és képzési karakter:

4.1. 2 kredit

4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 100 % gyakorlat, 0 % elmélet

4.3. Az értékelés: gyakorlati jegy

5. A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):

5.1. fejlesztéspolitikai programmenedzsment mesterképzési szak;5.2. International Public Service Relations mesterképzési szak;5.3. kiberbiztonsági mesterképzési szak;5.4. kommunikáció- és médiatudomány mesterképzési szak / valamennyi specializáció;5.5. kormányzás és vezetés mesterképzési szak;5.6. közgazdálkodás és közpolitika mesterképzési szak;5.7. közigazgatási mesterképzési szak;5.8. nemzetközi közszolgálati kapcsolatok mesterképzési szak / valamennyi szakirány;5.9. nemzetközi tanulmányok mesterképzési szak / valamennyi specializáció;5.10. nemzetközi tanulmányok mesterképzési szak (angol nyelven) / valamennyi specializáció;

6. Az oktatásért felelős oktatási szervezeti egység megnevezése:

Idegennyelvi és Szaknyelvi Lektorátus

7. A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:

Nagy Zsuzsanna

8. A tanórák száma és típusa

8.1.össz óraszám/félév:

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

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

8.2.heti óraszám - nappali munkarend: 2

8.3.Az ismeret átadásában alkalmazandó további sajátos módok, jellemzők:
Interaktív online oktatási platformok használata a hallgatók és az oktató által az élményalapú oktatás biztosítása és a hallgatói autonómia fejlesztésének érdekében, pl. Kahoot, Quizlet, Mentimeter. A hallgatók quizeket, szókincsgyűjteményeket és kérdőíveket készítenek önmaguk és egymás számára. Az oktató ezeket ellenőrzi és kiegészíti és integrálja az oktatási folyamatba.

9. A tantárgy szakmai tartalma (magyarul):

A tantárgy oktatásának célja, átfogó jogi szaknyelvi ismeretek elsajátítása. Jogágak (pl. tulajdonjog, szerződési jog, vállalati jog, kártérítési jog) szókincse, kapcsolódó készségek fejlesztése: olvasott szöveg értése, hallott szöveg értése, beszédkészség, levél-, jelentésírás. A kurzus teljesítésével jártasságot szereznek az alapvető jogi fogalmak körében és képesek lesznek ezeket megfelelően alkalmazva a fent említett témákban írásban és szóban egyaránt megnyilvánulni.

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

Students become familiar with the special vocabulary of various legal fields. Students gain knowledge of legal terminology of different fields (such as titles, contract law, company law, torts). Also, their related skills are developed such as reading and listening comprehension, speaking and writing skills. By completing the course, students will become acquainted with the concepts and notions of legal terminology and will be able to exchange ideas about them both in written and oral forms.

10. Elérendő kompetenciák (magyarul):

Tudása

Rendelkezik a szakmai feladatellátásához szükséges idegennyelv tudással legalább egy idegen nyelven.Rendelkezik a közigazgatási területre jellemző szaknyelvi ismeretekkel.

Alapvetően érti a polgári és büntető jog közti különbséget.Részletesen ismer olyan jogágakat mint a tulajdonjog, szerződési jog vagy a vállalati jog.Összefüggéseiben látja és csoportosítani tudja a büntető és a polgári peres eljárásokat.

Képességei

Szakmai feladatellátása során megfelelően alkalmaz legalább egy idegennyelvet.Rendelkezik a közigazgatási szakterületre jellemző szaknyelvi kommunikációs készségekkel.

Szakszerűen és komplex módon használja a különböző jogágakhoz kapcsolódó terminológiát.Munkahelyi feladatokat végez nemzetközi, multikulturális közegben.Képes idegen nyelven munkahelyi környezetben szakmai témákban hatékonyan kommunikálni szóban és írásban.Prezentációkat és összefoglalókat készít.

Attitűdje

-

Törekszik a megszerzett átfogó ismeretek rendszerszintű alkalmazására, idegen nyelvű környezetben is.Nyitottá válik a szakmai diskurzusokra idegen nyelven is.Kritikusan gondolkodik saját szakterületén idegen nyelven is.Törekszik a nyelvi pontosságra, igényességre.

Autonómiája és felelőssége

-

Autonómiája és felelőssége:Önállóan előadást készít és tart idegen nyelven.Másokkal együttműködve kifejti álláspontját, reagál más résztvevő véleményére és döntéseket hoz idegen nyelven.Segítséggel idegen nyelvű összefoglalókat készít.

Elérendő kompetenciák (angolul) (Competences – English):
Knowledge:

The student has the necessary foreign language skills in at least one foreign language to fulfil his/her professional duties.He/she is familiar with the technical language specific to the administrative area.

He/She fundamentally understands the difference between civil and criminal law.He/She has detailed information about the following branches of law: titles, contract law, company law, torts.He/She understands the complexity of civil and criminal cases and is able to group them.

Capabilities:

During the performance of his/her professional duties, the student is able to apply at least one foreign language properly.He/she is capable of using his/her professional language communication skills typical of the public administration field.

He/She adopts and uses the terminology of different branches of law.He/She works in an international and multicultural environment.He/She communicates efficiently about professional topics at his/her workplace both in oral and written forms in foreign languages.He/She makes and gives presentations.

Attitude:

-

He/She intends to apply the comprehensive knowledge acquired systematically in a foreign environment.He/She becomes open to professional discourses in a foreign language as well.He/She thinks critically on his/her own professional field in a foreign language as well.He/She intends to become critical and accurate regarding his/her language skills.

Autonomy and responsibility:

-

He/She prepares and holds presentations on his/her own in a foreign language.He/She expresses his/her opinion, reacts to others' opinion and makes decisions by collaborating with others in a foreign language.He/She prepares summaries with help.

11. Előtanulmányi követelmények:

nincs

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

12.1. Bevezetés (Introduction);12.2. Karrier a jog területén (Careers in law);12.3. Szerződési jog alapjai (Contract Law);12.4. Szerződésszegés jogorvoslata (Breaches of contract);12.5. Kártérítési jog (Torts);12.6. Bevezetés a büntetőjogba (Introduction into criminal law);12.7. Zárthelyi dolgozat 1 (Test 1);12.8. Elkövetők és bűncselekmények fajtái (Perpetrators and crimes);12.9. Bűncselekmények és bűntetés (Crime and punishment);12.10. Társasági jog (Company law);12.11. Társasági törvény megszegése (Breach of Company law);12.12. A társasági törvény megszegésének jogkövetkezményei (Breach and consequences of Company Law);12.13. Ismétlés (Revision);12.14. Zárthelyi dolgozat 2 (Test 2);

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

bármely félévben;

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

A hallgató köteles a foglalkozások min. 75%-án részt venni.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje

Két zárthelyi dolgozat /időpontja a tantárgyi tematikában látszik/Egy nyelvi portfólió létrehozása a félév folyamán, melynek elemei:- egy prezentáció tartása (szinttől függően 5-10 perces idegen nyelvű prezentáció tartása, melyet az oktatóval a félév elején egyeztetnek a hallgatók. Témája: a tantárgyi tematika egyik témájának altémája, a tematika által meghatározott héten.)- egy cikk összefoglalása 6-8 mondatban;legalább kettő interaktív feladat készítése (kahoot, quizlet gyűjtemény);Osztályzat ötfokozatú skálán / 50% elégséges, 60% közepes, 75% jó, 90%tól jeles/Dolgozatok pótlása a dolgozat utáni legelső alkalommal.

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

16.1. Az aláírás megszerzésének feltételei:
Részvétel a tanórák minimum 75%-án. Két zárthelyi dolgozat megírása. Nyelvi portfólió elemeinek elkészítése.

16.2. Az értékelés:
Gyakorlati jegy(GYJ). Osztályzat ötfokozatú skálán / 50% elégséges, 60% közepes, 75% jó, 90%tól jeles/. Zárthelyi dolgozatok 20-20%-ot, míg a nyelvi portfólió 60%-át teszi ki a gyakorlati jegynek.

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

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. Catherine Mason: Advanced legal English, Global Legal English, 2020. ISBN: 9781800680951;2. Catherine Mason: The Lawyer’s English Language Coursebook, Global English Ltd, 2010. ISBN: 0-19-457234-X;

17.2. Ajánlott irodalom:

1. Adrian Wallwork: Business Options, Oxford University Press, 2000. ISBN: 0-19-457234-X;

Budapest, 2024

Nagy Zsuzsanna

Nemzeti Közszolgálati Egyetem
Államtudományi és Nemzetközi Tanulmányok
Kar

TANTÁRGYI PROGRAM

ÁISZLM205 Szaknyelvi ismeretek V. - Nemzetközi kapcsolatok

1. A tantárgy kódja: ÁISZLM205

2. A tantárgy megnevezése (magyarul): Szaknyelvi ismeretek V. - Nemzetközi kapcsolatok

3. A tantárgy megnevezése (angolul): LSP V. - International relations

4. Kreditérték és képzési karakter:

4.1. 2 kredit

4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 100 % gyakorlat, 0 % elmélet

4.3. Az értékelés: gyakorlati jegy

5. A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):

5.1. fejlesztéspolitikai programmenedzsment mesterképzési szak;5.2. International Public Service Relations mesterképzési szak;5.3. kiberbiztonsági mesterképzési szak;5.4. kommunikáció- és médiatudomány mesterképzési szak / valamennyi specializáció;5.5. kormányzás és vezetés mesterképzési szak;5.6. közgazdálkodás és közpolitika mesterképzési szak;5.7. közigazgatási mesterképzési szak;5.8. nemzetközi közszolgálati kapcsolatok mesterképzési szak / valamennyi szakirány;5.9. nemzetközi tanulmányok mesterképzési szak / valamennyi specializáció;5.10. nemzetközi tanulmányok mesterképzési szak (angol nyelven) / valamennyi specializáció;

6. Az oktatásért felelős oktatási szervezeti egység megnevezése:

Idegennyelvi és Szaknyelvi Lektorátus

7. A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:

Miklósy Hajnalka

8. A tanórák száma és típusa

8.1.össz óraszám/félév:

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

8.1.2.levelező munkarend: 28 (0 EA + 0 SZ + 28 GY)

8.2.heti óraszám - nappali munkarend: 2

8.3.Az ismeret átadásában alkalmazandó további sajátos módok, jellemzők:
Interaktív online oktatási platformok használata a hallgatók és az oktató által az élményalapú oktatás biztosítása és a hallgatói autonómia fejlesztésének érdekében, pl. Kahoot, Quizlet, Mentimeter. A hallgatók quizeket, szókincsgyűjteményeket és kérdőíveket készítenek önmaguk és egymás számára. Az oktató ezeket ellenőrzi és kiegészíti és integrálja az oktatási folyamatba.

9. A tantárgy szakmai tartalma (magyarul):

Az ismeretanyag a világ vezető országai, a főbb nemzetközi szervezetek, a fejlődő országok, valamint a globalizáció főbb területein keresztül megismerteti a hallgatót a nemzetközi kapcsolattartás szakmai nyelvhasználatával, terminológiájával idegennyelven. A szókincsfejlesztésen túl különös hangsúlyt kap az olvasás-, írás-, beszédkészség és a beszédértés fejlesztése. A kurzus teljesítésével jártasságot szereznek a nemzetközi szervezetek alapvető fogalmainak körében és képesek lesznek ezeket megfelelően alkalmazva a fent említett témákban írásban és szóban egyaránt megnyilvánulni.

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

The course makes students familiar with the professional language of international communication in English or German through the topics of leading nations, international organizations, developing countries and globalization. Besides expanding their vocabulary, students improve their reading, writing, speaking and listening skills. By completing the course, students will become acquainted with the concepts and notions of international organizations and will be able to exchange ideas about them both in written and oral forms.

10. Elérendő kompetenciák (magyarul):

Tudása

Rendelkezik a szakmai feladatellátásához szükséges idegennyelv tudással legalább egy idegen nyelven.Rendelkezik a közigazgatási területre jellemző szaknyelvi ismeretekkel.

Alapvetően érti a nemzetközi szervezetek történetét és intézményrendszerét.Részletesen ismeri Magyarország és a világ vezető hatalmainak nemzetközi kapcsolatait.Összefüggéseiben látja és csoportosítani tudja a 21. század társadalmi problémáit.

Képességei

Szakmai feladatellátása során megfelelően alkalmaz legalább egy idegennyelvet.Rendelkezik a közigazgatási szakterületre jellemző szaknyelvi kommunikációs készségekkel.

Szakszerűen és komplex módon használja a nemzetközi szervezetek, kapcsolatok szókincsét.Munkahelyi feladatokat végez nemzetközi, multikulturális közegben.Képes idegen nyelven munkahelyi környezetben szakmai témákban hatékonyan kommunikálni szóban és írásban.Prezentációkat és összefoglalókat készít.

Attitűdje

-

Törekszik a megszerzett átfogó ismeretek rendszerszintű alkalmazására, idegen nyelvű környezetben is.Nyitottá válik a szakmai diskurzusokra idegen nyelven is.Kritikusan gondolkodik saját szakterületén idegen nyelven is.Törekszik a nyelvi pontosságra, igényességre.

Autonómiája és felelőssége

-

Önállóan előadást készít és tart idegen nyelven.Másokkal együttműködve kifejti álláspontját, reagál más résztvevő véleményére és döntéseket hoz idegen nyelven.Segítséggel idegen nyelvű összefoglalókat készít.

Elérendő kompetenciák (angolul) (Competences – English):
Knowledge:

The student has the necessary foreign language skills in at least one foreign language to fulfil his/her professional duties.He/she is familiar with the technical language specific to the administrative area.

He/She fundamentally understands the history and the institutions of international organizations.He/She has detailed information about the international relations of Hungary and the world leading powers.He/She understands the complexity of different 21st centiry social problems and is able to group them.

Capabilities:

During the performance of his/her professional duties, the student is able to apply at least one foreign language properly.He/she is capable of using his/her professional language communication skills typical of the public administration field.

He/She uses the terminology of international organizations and relations professionally.He/She works in an international and multicultural environment.He/She communicates efficiently about professional topics at his/her workplace both in oral and written forms in foreign languages.He/She makes and gives presentations.

Attitude:

-

He/She intends to apply the comprehensive knowledge acquired systematically in a foreign environment.He/She becomes open to professional discourses in a foreign language as well.He/She thinks critically on his/her own professional field in a foreign language as well.He/She intends to become critical and accurate regarding his/her language skills.

Autonomy and responsibility:

-

He/She prepares and holds presentations on his/her own ina foreign language.He/She expresses his/her opinion, reacts to others' opinion and makes decisions by collaborating with others in a foreign language.

11. Előtanulmányi követelmények:

nincs

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

12.1. Nemzetközi szervezetek és intézmények (szerepük, funkciójuk, jellemzőik) (International organizations (their role, function and characteristics));12.2. A vezető világhatalmak szerepe (Leading world powers);12.3. A célnyelvi ország(ok) nemzetközi kapcsolatai (International relations of target countries);12.4. Magyarország helyzete a nemzetközi politikában (Hungary on the international stage);12.5. A feltörekvő és fejlődő országok (szerepük és hatásuk a nemzetközi politikában) (Emerging and developing countries ((their role and impact in international politics));12.6. A környezetvédelem nemzetközi aspektusai (International aspects of environmental protection);12.7. Zárthelyi dolgozat (Téma 1-6) (Test I. Unit 1-6);12.8. Népesedés és migráció (nemzetközi demográfiai és migrációs problémák) (Population growth and migration ((international demographic and migartion problems));12.9. Emberi jogok, kisebbségi jogok (Human and minority rights);12.10. Nemzetközi konfliktusok, biztonság- és védelempolitika (International conflicts, security and defence policy);12.11. Válsággócok, nemzetközi terrorizmus (International crisis areas and terrorism);12.12. Nemzetközi és interkulturális kommunikáció (a média és a politika/diplomácia viszonya) (International and intercultural communication ((the relation of media and politics/diplomacy));12.13. Politikai és gazdasági erőviszonyok alakulása a világ egyes térségeiben (Poitical and economic powers in certain regions);12.14. Zárthelyi dolgozat (Téma 8-13) (Test II. Unit 8-13);

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

bármely félévben;

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

A hallgató köteles a foglalkozások min. 75%-án részt venni. Rövid/tartós távolmaradás indokolt esetben (orvosi, szolgálati) pótolható, amely pótlás egyéni megbeszélés szerint történik. Egyéb esetből fakadó több mint 25%-os hiányzás esetén, a félév teljesítése nem írható alá.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje

Két zárthelyi dolgozat /időpontja a tantárgyi tematikában látszik/.Egy nyelvi portfólió létrehozása a félév folyamán, melynek elemei:- egy prezentáció tartása (szinttől függően 5-10 perces idegen nyelvű prezentáció tartása, melyet az oktatóval a félév elején egyeztetnek a hallgatók. Témája: a tantárgyi tematika egyik témájának altémája, a tematika által meghatározott héten.)- egy cikk összefoglalása 6-8 mondatban;- legalább kettő interaktív feladat készítése (kahoot, quizlet gyűjtemény);Osztályzat ötfokozatú skálán / 50% elégséges, 60% közepes, 75% jó, 90% jeles/. Dolgozatok pótlása a dolgozat utáni legelső alkalommal.

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

16.1. Az aláírás megszerzésének feltételei:
Részvétel a tanórák minimum 75%-án. Két zárthelyi dolgozat megírása. Nyelvi portfólió elemeinek elkészítése.

16.2. Az értékelés:
Gyakorlati jegy(GYJ). Osztályzat ötfokozatú skálán / 50% elégséges, 60% közepes, 75% jó, 90%-tól jeles/. Zárthelyi dolgozatok 20-20%-ot, míg a nyelvi portfólió 60%-át teszi ki a gyakorlati jegynek.

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

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. Adrian Wallwork: Business Options, Oxford University Press, 2000. ISBN: 0-19-457234-X;2. Bogár Judit, Erdei József, Robert Thiessen: Crossing Borders, Lexika Kiadó,. ISBN: 978-615-5200-30-4;3. Bogár Judit, Erdei József, Robert Thiessen: Expanding Horizons, Lexika Kiadó,. ISBN: 978-615-5200-82-3;

17.2. Ajánlott irodalom:

1. Ajkay-Nagy Éva, Robin Bellers: Opening Borders, Lexika Kiadó, 2014. ISBN: 978-615-5200-31-1;

Budapest, 2024

Miklósy Hajnalka

Nemzeti Közszolgálati Egyetem
Államtudományi és Nemzetközi Tanulmányok
Kar

TANTÁRGYI PROGRAM

HKHIRA83 Számítógép hálózatok

1. A tantárgy kódja: HKHIRA83

2. A tantárgy megnevezése (magyarul): Számítógép hálózatok

3. A tantárgy megnevezése (angolul): Computer networks

4. Kreditérték és képzési karakter:

4.1. 6 kredit

4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 0 % gyakorlat, 100 % elmélet

4.3. Az értékelés: kollokvium

5. A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):

5.1. kiberbiztonsági mesterképzési szak;

6. Az oktatásért felelős oktatási szervezeti egység megnevezése:

Híradó Tanszék

7. A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:

Dr. Tóth András, PhD, egyetemi docens, tanszékvezető

8. A tanórák száma és típusa

8.1.össz óraszám/félév:

8.1.1.nappali munkarend: 84 (84 EA + 0 SZ + 0 GY)

8.1.2.levelező munkarend: 24 (24 EA + 0 SZ + 0 GY)

8.2.heti óraszám - nappali munkarend: 6

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

9. A tantárgy szakmai tartalma (magyarul):

A tantárgy célja átfogó ismeretek nyújtása a számítógépes hálózatok felépítéséről és működéséről. Ennek során a hallgatók megismerik a hálózati infrastruktúrát, a hálózati protokollokat és kommunikációt, a hálózatokhoz történő kapcsolódást, az OSI modellt, a TCP/IP modellt, az Ethernet szabványt, a hálózati, a szállítási és az alkalmazási réteg funkcióit, az IPv4 és az IPv6 címzést, az IP alhálózatok tervezését és kialakítását. A tananyag tartalmazza a a kapcsolt hálózatokba való bevezetést, a kapcsolás (switching) alapjait és beállítását, a forgalomirányítási (routing) alapokat, a statikus forgalomirányítást, a dinamikus forgalomirányítás, a DHCP, IPv4 hálózati címfordítást (NAT). Kitér a VLAN kialakítási, valamint forgalomirányítási lehetőségeire, az IPv4 és IPv6 hozzáférés vezérlési listák konfigurálására és megvalósítására, különböző WAN technológiák jellemzőinek bemutatására, előnyeik meghatározására, a virtuális magánhálózatok (VPN) működésének leírására. Átfogó elméleti és gyakorlati ismereteket nyújt a hálózati kapcsolatok beállítási és hibaelhárítási lehetőségeiben, különösen a hálózati diagnosztika területén, ismerteti a hitelesítési és titkosítási protokollok alapjait, valamint a proxyk, tűzfalak alkalmazását. Magában foglalja a Windows és Linux operációs rendszerek hálózati szolgáltatásainak és beállításainak megismerését. A hallgatók foglalkoznak a hálózati forgalomelemzés aktív és passzív módszereivel, a vezetéknélküli hálózatok működésének vizsgálatával, az Ethernet szabványok összehasonlító mérésével, a hálózati eszközök (HUB, switch, router, tűzfal,

proxy) működésének protokollanalizátor segítségével végzett vizsgálatával, a hálózati eszközök terheléses vizsgálatával, és a hálózati eszközök funkcionális vizsgálatának lehetőségeivel. Emellett az IP forgalom titkosításának lehetőségeit (hálózati, szállítási, alkalmazás rétegbeli lehetőségek) is bemutatja a tárgy, mely kitér a tűzfalak típusainak és funkcióinak gyakorlati vizsgálatára is.

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

The aim of this course is to provide a comprehensive knowledge of the structure and operation of computer networks. In this course, students will learn about network infrastructure, network protocols and communication, network connectivity, the OSI model, the TCP/IP model, the Ethernet standard, network, transport and application layer functions, IPv4 and IPv6 addressing, IP subnet design and construction. The curriculum includes introduction to switched networks, switching basics and configuration, routing basics, static traffic management, dynamic traffic management, DHCP, IPv4 network address translation (NAT). It covers VLAN design and traffic management options, configuration and implementation of IPv4 and IPv6 access control lists, characteristics of different WAN technologies, their advantages, description of virtual private network (VPN) operation. It provides a comprehensive theoretical and practical understanding of the configuration and troubleshooting of network connections, in particular network diagnostics, the basics of authentication and encryption protocols, and the use of proxies and firewalls. It includes an introduction to the network services and configuration of Windows and Linux operating systems. Students will cover active and passive methods of network traffic analysis, wireless network performance testing, comparative measurement of Ethernet standards, protocol analyzer testing of network devices (HUB, switch, router, firewall, proxy), network device load testing, and functional testing of network devices. In addition, IP traffic encryption options (network, transport, application layer options) will be covered, including a practical examination of firewall types and functions.

10. Elérendő kompetenciák (magyarul):

Tudása

Átlátja, hogy milyen védelmi megoldások vannak a kibertámadás ellen. Ismeri a kibertámadás esetén alkalmazandó eljárásokat.
A tantárgy átfogó ismereteket nyújt a hallgatóknak a különböző védelmi mechanizmusokról, amelyeket a számítógépes hálózatok kibertámadások elleni védelmére használnak. Elméleti ismeretekkel rendelkezik majd a kibertámadásokkal kapcsolatos kockázatok mérséklése érdekében követendő szabványos eljárásokról. Megismeri továbbá a kiberbűnözők által alkalmazott legújabb trendeket és taktikákat, valamint azt, hogy hogyan lehet hatékonyan azonosítani és reagálni ezekre a fenyegetésekre.
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 megfelelően támogatni szervezetét és a külső feleket egy kibertámadás kezelésében.
A tantárgy olyan készségekkel ruházza fel a hallgatókat, amelyek szükségesek a számítógépes hálózatok védelméhez a potenciális emberi fenyegetésekkel szemben. Átfogó képzést nyújt a cyber kill chain-nel kapcsolatos biztonsági intézkedésekről, kitérve az aktuális kiberfenyegetésekre és a hálózatok támadás alatti támogatására irányuló stratégiákra. A hallgatók ismereteket szereznek a kockázatértékelésről, a hatékony biztonsági intézkedések végrehajtásáról és a kiberbiztonság legújabb trendjeinek naprakész követéséről.
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.

A tantárgy átfogó kiberbiztonsági hozzáállással ruházza fel a hallgatókat, lehetővé téve számukra a sebezhetőségek azonosítását, az iparági szabványos eszközök használatát és a kockázatok csökkentésére irányuló proaktív intézkedések meghozatalát. A hallgatók együttműködő partnerekké válnak a szervezetük hálózatának védelmében, és proaktívan fognak hozzáállni a kiberbiztonsági incidensekhez.

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.
A tantárgy sikeres elvégzése után a hallgató lelkiismeretesen és felelősségteljesen törekszik a számítógépes hálózatok biztonságának rendkívül összetett területével kapcsolatos korszerű ismeretek és gyakorlatok alkalmazására, figyelembe véve mind a nemzeti, mind a nemzetközi kontextus egyedi követelményeit. A hallgató felelősséget vállal a terület szilárd módszertanának és a szakmai gyakorlat kialakításához nélkülözhetetlen elméleti, tudományos és gyakorlati információk megszerzéséért, átfogó értékeléséért és felhasználásáért. A tantárgy célja, hogy a hallgató a megszerzett ismereteket és készségeket hatékonyan és felelősségteljesen alkalmazza a gyakorlatban, és hozzájáruljon a szakterület folyamatos fejlődéséhez.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge:

Defence solutions against cyber attacks.Familiar with the procedures applicable in case of a cyber attack.
This course gives students a comprehensive understanding of the protection mechanisms used to defend computer networks against cyber attacks. They will have a theoretical understanding of the standard procedures to be followed to mitigate cyber-attack risks. Furthermore, they will learn about cybercriminals' latest trends and tactics and how to identify and respond to these threats effectively.

Capabilities:

He/she is capable of taking defensive measures that ensure the reduction of risk resulting from threat against humans. Moreover he/she is capable of taking technological defensive measures related to elements of the cyber kill chain. Furthermore has the capability and understanding of the current threats of cyberspace. He/she is capable of supporting his/her organisation and external parties in handling a cyber attack.
The course equips students with the skills needed to protect computer networks against potential human threats. It provides a comprehensive education on cyber kill chain security measures, covering current cyber threats and strategies to support networks under attack. Students will gain knowledge on risk assessment, implementing effective security measures and keeping up to date with the latest trends in cyber security.

Attitude:

An effort to take effective measures in order to prevent cyber attacks, by this means reducing the exposure of his/her organisation. An ability to cooperate in preventing his/her organisation and him/herself from becoming a victim of a cyber attack.
The course will equip students with a comprehensive cybersecurity attitude, enabling them to identify vulnerabilities, use industry-standard tools and take proactive measures to mitigate risks. Students will become collaborative partners in protecting their organisation's network and take a proactive approach to cyber security incidents.

Autonomy and responsibility:

To implement advanced knowledge characterising cybersecurity on a national and international level. To obtain, evaluate and utilize theoretical, scientific and practical information necessary for the improvement of the field and the methodology of professional practice.
Upon completing the course, the student will conscientiously and responsibly apply state-of-the-art knowledge and practices in the highly complex area of computer network

security, considering the specific requirements of both national and international contexts. The student will take responsibility for acquiring, comprehensively evaluating, and using the theoretical, scientific and practical information necessary to develop a sound methodology and professional practice in the field. This course aims to enable the student to apply the knowledge and skills acquired effectively and responsibly in practice and to contribute to the continuous development of the field.

11. Előtanulmányi követelmények:

nincs

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

12.1. Hálózati protokollok és kommunikáció, Ethernet szabvány (Network protocols and communications, Ethernet standard);12.2. Hálózati és szállítási réteg (Network and transport layer);12.3. Alkalmazási réteg (Application layer);12.4. Kapcsolt hálózatok, a kapcsolás beállításainak alapjai (Switched networks, basics of switching settings);12.5. VLAN-ok (VLANs);12.6. A forgalomirányítás alapjai (The basics of routing);12.7. Statikus, dinamikus forgalomirányítás (Static, dynamic routing);12.8. Hozzáférés vezérlési listák, DHCP, IPv4 hálózati címfordítás (Access control lists, DHCP, IPv4 network address translation);12.9. WAN technológiák jellemzői (Features of WAN technologies);12.10. Virtuális magánhálózatok (VPN) működése (Operation of Virtual Private Networks (VPNs));12.11. Hálózati diagnosztika, a hitelesítési és titkosítási protokollok alapjai (Network diagnostics, basics of authentication and encryption protocols);12.12. A hálózat monitorozása, hálózati hibaelhárítás (Network monitoring, network troubleshooting);12.13. Tűzfalak típusainak és funkcióinak gyakorlati vizsgálata (Practical study of types and functions of firewalls);12.14. Vezetéknélküli hálózatok (Wireless networks);

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

1. félév/ősz;

14. 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.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje

A félév során a hallgatók két zárthelyi dolgozatot írnak. Az első zárthelyi a 13.1-13.7., a második a 13.8-13.14 témákat ellenőrzi. A zárthelyi dolgozat értékelése ötfokozatú skálán történik az alábbiak szerint: 51 %-tól elégséges, 63 %-tól közepes, 75 %-tól jó, 87 %-tól jeles. Sikertelen zárthelyi dolgozatot a félév utolsó tanulmányi hetében lehet pótolni.

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

16.1. Az aláírás megszerzésének feltételei:
Az aláírás megszerzésének feltétele a tanórákon való 70 %-os részvétel és a zárthelyi dolgozatok mindegyikének legalább elégséges osztályzata.

16.2. Az értékelés:

Az írásbeli kollokvium követelménye a tanórákon átadott ismeretekre és a kötelező irodalomra épül. Az írásbeli kollokvium esetében az értékelés a hallgató által 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)

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

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. Andrew S. Tanenbaum: Számítógép hálózatok , Panem Kft., 2013. ISBN: 9789635455294;2. Frész Ferenc, Kálovics Tamás, Puha Gábor: Hálózatok Biztonsága , ÁROP –2.2.21 Tudásalapú közszolgálati előmenetel, Nemzeti Közszolgálati Egyetem 2014.3. James Kurose, Keith Ross : Computer Networking: A Top-Down Approach, A Top-Down Approach, 2016. ISBN: 9780133594140;

17.2. Ajánlott irodalom:

1. Ciprian Adrian Rusen: Számítógépes eszközök hálózatba kötése lépésről lépésre, Szak Kiadó, 2011. ISBN: 9789639863217;2. Dr. Kónya László: Számítógép-hálózatok, LSI OMAK Alapítvány, 2002. ISBN: 96357722X;3. Jill West, Tamara Dean, Jean Andrews: Network+ Guide to Networks, 2018. ISBN: 9781337569330;

Budapest, 2024

Dr. Tóth András, PhD, egyetemi docens, tanszékvezető

Nemzeti Közszolgálati Egyetem
Államtudományi és Nemzetközi Tanulmányok
Kar

TANTÁRGYI PROGRAM

ÁKIBTM011 Végponti biztonsági technológiák alkalmazása

1. A tantárgy kódja: ÁKIBTM011

2. A tantárgy megnevezése (magyarul): Végponti biztonsági technológiák alkalmazása

3. A tantárgy megnevezése (angolul): Application of endpoint security technologies

4. Kreditérték és képzési karakter:

4.1. 4 kredit

4.2. a tantárgy elméleti vagy gyakorlati jellegének mértéke: 100 % gyakorlat, 0 % elmélet

4.3. Az értékelés: beszámoló

5. A szak(ok), szakirányok/specializációk megnevezése (ahol oktatják):

5.1. kiberbiztonsági mesterképzési szak;

6. Az oktatásért felelős oktatási szervezeti egység megnevezése:

Kiberbiztonsági Tanszék

7. A tantárgyfelelős oktató neve, beosztása, tudományos fokozata:

Koczka Ferenc, phd, tanársegéd

8. A tanórák száma és típusa

8.1.össz óraszám/félév:

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

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

8.2.heti óraszám - nappali munkarend: 2

8.3.Az ismeret átadásában alkalmazandó további sajátos módok, jellemzők:
Egyéni felkészülés e-learning segítségével, online gyakorlat formájában.

9. A tantárgy szakmai tartalma (magyarul):

A tantárgy célja olyan gyakorlati ismeretek nyújtása a hallgatók számára, melynek segítségével képessé válnak egy alapfokú végpontvédelmi ismereteket nyújtó, angol nyelvű, nemzetközi, gyártói vagy gyártófüggetlen vizsga megszerzésére. A kurzus folyamán a hallgatók kiválasztják azt a vizsgát, melynek megszerzését célul tűzték ki, önálló felkészüléssel, a képző által nyújtott e-learning rendszerben elsajátítják az ismereteket, melyek elmélyítésére hetente konzultációs lehetőség áll rendelkezésükre.

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

The aim of the course is to provide students with the practical skills to enable them to pass an international, vendor or vendor-independent exam in English, providing a basic level of endpoint security knowledge. During the course, students will choose the exam they wish to take and will learn the skills through self-study and e-learning provided by the trainer, with weekly consultations to reinforce their knowledge.

10. Elérendő kompetenciák (magyarul):

Tudása

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

Ismeri a különböző típusú kibertámadásokat és azok lehetséges következményeit.Tájékozott a hálózati és rendszeres biztonsági protokollok és technológiák terén.Ismeri a kártékony kódok működésének fő irányait.

Képességei

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

Képes azonosítani és elemző eszközökkel vizsgálni a kártékony kódokat.Képes felismerni a kártékony kódok által okozott károkat és azok lehetséges következményeit.Képes meghatározni az informatikai rendszerek védelmi feladatait a újabb biztonsági fenyegetések ellen is.

Attitűdje

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

Incidens bekövetkezésekor gyorsan és helyesen reagál, meghozza a megfelelő védelmi intézkedéseket.Alkalmazza a megfelelő biztonsági protokollokat és eljárásokat a kibertámadások kezelésére és megelőzésére.

Autonómiája és felelőssége

Vállalja a szakterület, a szakmai praxis módszertanának fejlesztéséhez szükséges elméleti, tudományos kutatási és gyakorlati információk beszerzésének, értékelésének és hasznosításának végrehajtását. Önállóan és pontosan vesz részt a kiberbiztonsági fenyegetések technológiai, politikai és adminisztratív megoldásában. Együttműködik más szakemberekkel a biztonsági eszközök telepítésében, karbantartásában és frissítésében.

Elérendő kompetenciák (angolul) (Competences – English):

Knowledge:

Defence solutions against cyber attacks. The concept and mode of action of malware codes.

Knowledge of the different types of cyber-attacks and their possible consequences.Knowledge of network and system security protocols and technologies.Knowledge of the main ways malicious code works.

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.

Ability to identify and analyse malicious code with analytical tools.Ability to recognise the damage caused by malicious code and its possible consequences.The ability to define the protection of IT systems against new security threats.

Attitude:

An ability to cooperate in preventing his/her organisation and him/herself from becoming a victim of a cyber attack.

In case of an incident, reacts quickly and correctly, taking appropriate protective measures.Apply appropriate security protocols and procedures to manage and prevent cyber-attacks.

Autonomy and responsibility:
To obtain, evaluate and utilize theoretical, scientific and practical information necessary for the improvement of the field and the methodology of professional practice. To take part in providing technological, political and administrative solutions to cyber threats. Collaborates with other professionals to install, maintain and update security tools.

11. Előtanulmányi követelmények:

nincs

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

12.1. Windows alapú végponti biztonsági megoldások I. (Endpoint Security-Windows Systems I.)12.2. Windows alapú végponti biztonsági megoldások II. (Endpoint Security-Windows Systems II.)12.3. Windows alapú végponti biztonsági megoldások III. (Endpoint Security-Windows Systems III.)12.4. Linux alapú végponti biztonsági megoldások I. (Endpoint Security-Linux Systems I.)12.5. Linux alapú végponti biztonsági megoldások II. (Endpoint Security-Linux Systems II.)12.6. Mobilrendszerek végponti biztonsági megoldásai I. (Endpoint Security- Mobile Devices I.)12.7. Mobilrendszerek végponti biztonsági megoldásai II. (Endpoint Security- Mobile Devices II.)12.8. Mobilrendszerek végponti biztonsági megoldásai III. (Endpoint Security- Mobile Devices III.)12.9. IoT rendszerek végponti biztonsági megoldásai I. (Endpoint Security-IoT Devices I.)12.10. IoT rendszerek végponti biztonsági megoldásai II. (Endpoint Security-IoT Devices II.)12.11. Adminisztratív alkalmazásbiztonság I. (Administrative Application Security I.)12.12. Adminisztratív alkalmazásbiztonság II. (Administrative Application Security II.)12.13. Adatbiztonság I. (Data Security I.)12.14. Adatbiztonság II. (Data Security II.)

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

2. félév/tavasz;

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

A hallgató önálló felkészüléssel teljesíti a féléves követelményeket, így a tanórákon a részvétel nem kötelező. Az órarendben meghatározott időpontokon az előadó online gyakorlat formájában konzultációs lehetőséget biztosít.

15. Félévközi feladatok, ismeretek ellenőrzésének rendje

A félév során a hallgatók egyénileg, angol nyelvű e-learning segítségével készülnek fel egy, az oktató által ajánlott listából választott, nemzetközileg elismert kiberbiztonsági vizsgára.

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

16.1. Az aláírás megszerzésének feltételei:
Az aláírás megszerzésének feltétele az oktató által kijelölt e-learning modulok sikeres teljesítése.

16.2. Az értékelés:

A tantárgy beszámolóval zárul és értékelése háromfokozatú jeggyel történik, melynek minősítései:- kiválóan megfelelt (5), amennyiben a hallgató a megadott vizsgaidőpontban sikeresen megszerzi a nemzetközi kiberbiztonsági vizsgát.- megfelelt (3), amennyiben a hallgató a megadott vizsgaidőpontban megkísérli megszerezni a nemzetközi kiberbiztonsági vizsgát, de nem jár sikerrel.nem felelt meg (1), amennyiben a hallgató megszerzi az aláírást, de a vizsgaidőszakban nem próbálkozik meg a nemzetközi kiberbiztonsági vizsga megszerzésével.

16.3. A kreditek megszerzésének feltételei:
A kreditek megszerzésének feltétele az aláírás megszerzése és legalább megfelelt beszámoló (B).

17. Irodalomjegyzék:

17.1. Kötelező irodalom:

1. Abraham Silberschatz, Greg Gagne, Peter B. Galvin: Operating System Concepts, 10th Edition, John Wiley & Sons, 2018. ISBN: 978-1119439257;2. Koczka Ferenc: Operációs rendszerek online tananyag,.

17.2. Ajánlott irodalom:

1. Microsoft MD-102 Explore endpoint management,.2. Andrew S. Tanenbaum: Operációs rendszerek, Panem, Budapest 2007. ISBN: 9789635451761;3. Emmett Dulaney: Linux, Taramix, 2016. ISBN: 2399973567770;

Budapest, 2024

Koczka Ferenc, phd, tanársegéd

TANÓRA-, KREDIT- ÉS VIZSGATERV
KIBERBIZTONSÁGI MESTERKÉPZÉSI SZAK
érvényes 2024/2025-ös tanévtől felmenő rendszerben.
teljes idejű képzésben, nappali munkarend szerint tanuló hallgatók részére

tantárgy kódja	tantárgy jellege	tanulmányi terület/tantárgy	félév/szemeszter																				összesen						TÁRGYFELELŐS SZERVEZETI EGYSÉG	TÁRGYFELELŐS SZEMÉLY
			1.						2.						3.						4.											
			elm.		gyak.				elm.		gyak.				elm.		gyak.				elm.		gyak.				elm.		gyak.			
			heti tanóra	félévi tanóra	heti tanóra	félévi tanóra	kredit	számonkérés	heti tanóra	félévi tanóra	heti tanóra	félévi tanóra	kredit	számonkérés	heti tanóra	félévi tanóra	heti tanóra	félévi tanóra	kredit	számonkérés	heti tanóra	félévi tanóra	heti tanóra	félévi tanóra	kredit	számonkérés	heti tanóra	félévi tanóra	heti tanóra	félévi tanóra	kredit	elmélet + gyakorlat heti összes tanóra		
		Törzsanyag tárgyai																														
ÁKIBTM001	K	A kiberbiztonság jogi és szervezeti alapjai Magyarországon	4	56			6	K																			4	56			6	4	Kiberbiztonsági Ta	Dr. Szádeczky Tamás
ÁKIBTM002	K	Bevezetés a kiberbiztonság szakterületi ismereteibe			6	84	6	GYJ																					6	84	6	6	Kiberbiztonsági Ta	Dr. Krasznay Csaba
HKHIRA83	K	Számítógép hálózatok	6	84			6	K																			6	84			6	6	Híradó Tanszék	Dr. Tóth András
ÁKIBTM004	K	Hálózati biztonsági technológiák alkalmazása			2	28	4	B																					2	28	4	2	Kiberbiztonsági Ta	Dr. Orbók Ákos
ÁAÖKTM07	K	Adatvédelem	4	56			4	K																			4	56			4	4	Alkotmányjogi és G	Dr. Téglásiné dr. Kovács Júlia
ÁKIBTM006	K	Kiberbiztonsági stratégia és vezetés			2	28	4	GYJ																					2	28	4	2	Kiberbiztonsági Ta	Dr. Krasznay Csaba
RBGVB183	K	Kiberbűnözés és kibernyomozás							4	56			6	K													4	56			6	4	Bűnügyi, Gazdasá	Dr. Gyaraki Réka Eszter
HKEHVM68	K	Nemzetállamok a kibertérben									6	84	6	GYJ															6	84	6	6	Elektronikai Hadvis	Prof. Dr. Kovács László
ÁKIBTM009	K	Kritikus információs infrastruktúra védelem							4	56			4	K													4	56			4	4	Kiberbiztonsági Ta	Dr. Szádeczky Tamás
ÁKIBTM010	K	Operációs rendszerek							4	56			6	K													4	56			6	4	Kiberbiztonsági Ta	Dr. Krasznay Csaba
ÁKIBTM011	K	Végponti biztonsági technológiák alkalmazása									2	28	4	B															2	28	4	2	Kiberbiztonsági Ta	Koczka Ferenc
ÁKIBTM007	K	Kockázatértékelés és kockázatmenedzsment															2	28	4	GYJ									2	28	4	2	Kiberbiztonsági Ta	Dr. Krasznay Csaba
ÁKIBTM008	K	Közszolgálati információs rendszerek védelme															4	56	6	GYJ									4	56	6	4	Kiberbiztonsági Ta	Dr. Bányász Péter
ÁKIBTM003	K	Felhőalapú rendszerek biztonsága															2	28	4	B									2	28	4	2	Kiberbiztonsági Ta	Koczka Ferenc
NPNBM51	K	A kiberbiztonság humán tényezői															2	28	4	K									2	28	4	2	Polgári Nemzetbizt	Dr. Dobák Imre
ÁKIBTM005	K	Incidensmenedzsment																					4	56	6	K			4	56	6	4	Kiberbiztonsági Ta	Dr. Krasznay Csaba
HKKNBM15	K	Hírszerzés a kibertérben																					2	28	4	GYJ			2	28	4	2	Nemzetbiztonsági	Dr. Magyar Sándor
HKHIRA84	K	Biztonsági tesztelés																					4	56	6	GYJ			4	56	6	4	Híradó Tanszék	Dr. Tóth András
	KV	Kötelezően választható szaknyelv									2	28	2																2	28	2	2		
	SZV	Szabadon választható 1.									2	28	2																2	28	2	2		
	SZV	Szabadon választható 2.															2	28	2										2	28	2	2		
	SZV	Szabadon választható 3.																					2	28	2				2	28	2	2		
	SZV	Szabadon választható 4.																					2	28	2				2	28	2	2		
		TÖRZSANYAG ÖSSZESEN	**14**	**196**	**10**	**140**	**30**	**x**	**12**	**168**	**12**	**168**	**30**	**x**	**0**	**0**	**12**	**168**	**20**	**x**	**0**	**0**	**14**	**196**	**20**	**x**	**26**	**364**	**48**	**672**	**100**	**74**		
		Kreditet nem képező tantárgyak																																
LFSZE01	KR	Ludovika Fesztivál Szabadegyetem			0	4	x						x						x						x				0	4	x	0		
ÁKIBERMSZGY001	KR	Szakmai gyakorlat																	0	A														
		Kreditet nem képező tantárgyak összesen:	**0**	**0**	**0**	**4**	**x**	**x**	**0**	**0**	**0**	**0**	**x**	**x**	**0**	**0**	**0**	**0**	**x**	**x**	**0**	**0**	**0**	**0**	**x**	**x**	**0**	**0**	**0**	**4**	**x**	**0**		
		Szakdolgozat/Diplomamunka tantárgya																																
ÁKIBERM001	K	Diplomamunka-tervezés 1.															6	84	10	GYJ									6	84	10	6	Kiberbiztonsági Ta	Dr. Krasznay Csaba
ÁKIBERM002	K	Diplomamunka-tervezés 2.																					6	84	10	GYJ			6	84	10	6	Kiberbiztonsági Ta	Dr. Krasznay Csaba
		Szakdolgozat/Diplomamunka tantárgyak összesen:	**0**	**0**	**0**	**0**	**0**	**x**	**0**	**0**	**0**	**0**	**0**	**x**	**0**	**0**	**6**	**84**	**10**	**x**	**0**	**0**	**6**	**84**	**10**	**x**	**0**	**0**	**12**	**168**	**20**	**12**		
		ÖSSZES TANÓRARENDI TANÓRA	**14**	**196**	**10**	**144**	**30**	**x**	**12**	**168**	**12**	**168**	**30**	**x**	**0**	**0**	**18**	**252**	**30**	**x**	**0**	**0**	**20**	**280**	**30**	**x**	**26**	**364**	**60**	**844**	**120**	**86**		
		SZÁMONKÉRÉSEK ÖSSZESÍTŐ																																
		Aláírás (A)																		1												1		
		Beszámoló (B)					1						1							1												3		
		Évközi értékelés (ÉÉ)																																
		Évközi értékelés (((záróvizsga tárgy((ÉÉ(Z)))																																
		Gyakorlati jegy(GYJ)					2						1							3						3						9		
		Gyakorlati jegy (((záróvizsga tárgy((GYJ(Z)))																																
		Kollokvium (K)					3						3							1						1						8		
		Kollokvium (((záróvizsga tárgy((K(Z)))																																
		Alapvizsga (AV)																																
		Komplex vizsga (KV)																																
		Szigorlat (SZG)																																
		Záróvizsga tárgy(ZV)																																
		FÉLÉVENKÉNT SZÁMONKÉRÉSEK ÖSSZESEN:					6						5							6						4						21		

TANÓRA-, KREDIT- ÉS VIZSGATERV

KIBERBIZTONSÁGI MESTERKÉPZÉSI SZAK

érvényes 2024/2025-ös tanévtől felmenő rendszerben.

részidejű képzésben, levelező munkarend szerint tanuló hallgatók részére

tantárgy kódja	tantárgy jellege	tanulmányi terület/tantárgy	félév/szemeszter																				összesen						TÁRGYFELELŐS SZERVEZETI EGYSÉG	TÁRGYFELELŐS SZEMÉLY
			1.						2.						3.						4.											
			elm.		gyak.				elm.		gyak.				elm.		gyak.				elm.		gyak.				elm.		gyak.			
			heti tanóra	félévi tanóra	heti tanóra	félévi tanóra	kredit	számonkérés	heti tanóra	félévi tanóra	heti tanóra	félévi tanóra	kredit	számonkérés	heti tanóra	félévi tanóra	heti tanóra	félévi tanóra	kredit	számonkérés	heti tanóra	félévi tanóra	heti tanóra	félévi tanóra	kredit	számonkérés	heti tanóra	félévi tanóra	heti tanóra	félévi tanóra	kredit	elmélet + gyakorlat heti összes tanóra		
		Törzsanyag tárgyai																														
ÁKIBTM001	K	A kiberbiztonság jogi és szervezeti alapjai Magyarországon	4	16			6	K																			4	16			6	4	Kiberbiztonsági Ta	Dr. Szádeczky Tamás
ÁKIBTM002	K	Bevezetés a kiberbiztonság szakterületi ismereteibe			6	24	6	GYJ																					6	24	6	6	Kiberbiztonsági Ta	Dr. Krasznay Csaba
HKHIRA83	K	Számítógép hálózatok	6	24			6	K																			6	24			6	6	Híradó Tanszék	Dr. Tóth András
ÁKIBTM004	K	Hálózati biztonsági technológiák alkalmazása			2	8	4	B																					2	8	4	2	Kiberbiztonsági Ta	Dr. Orbók Ákos
ÁAÖKTM07	K	Adatvédelem	4	16			4	K																			4	16			4	4	Alkotmányjogi és (	Dr. Téglásiné dr. Kovács Júlia
ÁKIBTM006	K	Kiberbiztonsági stratégia és vezetés			2	8	4	GYJ																					2	8	4	2	Kiberbiztonsági Ta	Dr. Krasznay Csaba
RBGVB183	K	Kiberbűnözés és kibernyomozás							4	16			6	K													4	16			6	4	Bűnügyi, Gazdasá	Dr. Gyaraki Réka Eszter
HKEHVM68	K	Nemzetállamok a kibertérben									6	24	6	GYJ															6	24	6	6	Elektronikai Hadvis	Prof. Dr. Kovács László
ÁKIBTM009	K	Kritikus információs infrastruktúra védelem							4	16			4	K													4	16			4	4	Kiberbiztonsági Ta	Dr. Szádeczky Tamás
ÁKIBTM010	K	Operációs rendszerek							4	16			6	K													4	16			6	4	Kiberbiztonsági Ta	Dr. Krasznay Csaba
ÁKIBTM011	K	Végponti biztonsági technológiák alkalmazása									2	8	4	B															2	8	4	2	Kiberbiztonsági Ta	Koczka Ferenc
ÁKIBTM007	K	Kockázatértékelés és kockázatmenedzsment															2	8	4	GYJ									2	8	4	2	Kiberbiztonsági Ta	Dr. Krasznay Csaba
ÁKIBTM008	K	Közszolgálati információs rendszerek védelme															4	16	6	GYJ									4	16	6	4	Kiberbiztonsági Ta	Dr. Bányász Péter
ÁKIBTM003	K	Felhőalapú rendszerek biztonsága															2	8	4	B									2	8	4	2	Kiberbiztonsági Ta	Koczka Ferenc
NPNBM51	K	A kiberbiztonság humán tényezői															2	8	4	K									2	8	4	2	Polgári Nemzetbiz	Dr. Dobák Imre
ÁKIBTM005	K	Incidensmenedzsment																					4	16	6	K			4	16	6	4	Kiberbiztonsági Ta	Dr. Krasznay Csaba
HKKNBM15	K	Hírszerzés a kibertérben																					2	8	4	GYJ			2	8	4	2	Nemzetbiztonsági	Dr. Magyar Sándor
HKHIRA84	K	Biztonsági tesztelés																					4	16	6	GYJ			4	16	6	4	Híradó Tanszék	Dr. Tóth András
	KV	Kötelezően választható szaknyelv									2	8	2																2	8	2	2		
	SZV	Szabadon választható 1.									2	8	2																2	8	2	2		
	SZV	Szabadon választható 2.															2	8	2										2	8	2	2		
	SZV	Szabadon választható 3.																					2	8	2				2	8	2	2		
	SZV	Szabadon választható 4.																					2	8	2				2	8	2	2		
		TÖRZSANYAG ÖSSZESEN	**14**	**56**	**10**	**40**	**30**	**x**	**12**	**48**	**12**	**48**	**30**	**x**	**0**	**0**	**12**	**48**	**20**	**x**	**0**	**0**	**14**	**56**	**20**	**x**	**26**	**104**	**48**	**192**	**100**	**74**		
		Kreditet nem képező tantárgyak																																
ÁKIBERMSZGY001	KR	Szakmai gyakorlat																	0	A												x		
		Kreditet nem képező tantárgyak összesen:	**0**	**0**	**0**	**0**	**x**	**x**	**0**	**0**	**0**	**0**	**x**	**x**	**0**	**0**	**0**	**0**	**x**	**x**	**0**	**0**	**0**	**0**	**x**	**x**	**0**	**0**	**0**	**0**	**x**	**0**		
		Szakdolgozat/Diplomamunka tantárgya																																
ÁKIBERM001	K	Diplomamunka-tervezés 1.															6	24	10	GYJ									6	24	10	6	Kiberbiztonsági Ta	Dr. Krasznay Csaba
ÁKIBERM002	K	Diplomamunka-tervezés 2.																					6	24	10	GYJ			6	24	10	6	Kiberbiztonsági Ta	Dr. Krasznay Csaba
		Szakdolgozat/Diplomamunka tantárgyak összesen:	**0**	**0**	**0**	**0**	**0**	**x**	**0**	**0**	**0**	**0**	**0**	**x**	**0**	**0**	**6**	**24**	**10**	**x**	**0**	**0**	**6**	**24**	**10**	**x**	**0**	**0**	**12**	**48**	**20**	**12**		
		ÖSSZES TANÓRARENDI TANÓRA	**14**	**56**	**10**	**40**	**30**	**x**	**12**	**48**	**12**	**48**	**30**	**x**	**0**	**0**	**18**	**72**	**30**	**x**	**0**	**0**	**20**	**80**	**30**	**x**	**26**	**104**	**60**	**240**	**120**	**86**		
		SZÁMONKÉRÉSEK ÖSSZESÍTŐ																																
		Aláírás (A)																	1													1		
		Beszámoló (B)					1						1						1													3		
		Évközi értékelés (ÉÉ)																																
		Évközi értékelés (((záróvizsga tárgy((ÉÉ(Z)))																																
		Gyakorlati jegy(GYJ)					2						1						3						3							9		
		Gyakorlati jegy (((záróvizsga tárgy((GYJ(Z)))																																
		Kollokvium (K)					3						3						1						1							8		
		Kollokvium (((záróvizsga tárgy((K(Z)))																																
		Alapvizsga (AV)																																
		Komplex vizsga (KV)																																
		Szigorlat (SZG)																																
		Záróvizsga tárgy(ZV)																																
		FÉLÉVENKÉNT SZÁMONKÉRÉSEK ÖSSZESEN:					6						5						6						4							21		

2. számú melléklet: Előtanulmányi rend

A KIBERBIZTONSÁGI MESTERKÉPZÉSI SZAK AJÁNLOTT TANTERVE
ELŐTANULMÁNYI REND

Kódszám	Tantárgy	Előtanulmányi követelmény		Egyidejű felvétel megengedett (IGEN/NEM)
		Kódszám	Tantárgy	