CTI elemzés

Kiberbiztonsági képzések Magyarországon

1996

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERBIZTONSÁGI INTÉZET

Tartalomjegyzék

Bevezető

Ez az írás a magyarországi, iskolarendszerű kiberbiztonsági képzési kínálatot tekinti át: felsőfokú szakképzési és felsőoktatási (alap- és mesterképzési), valamint releváns szakirányú továbbképzési programokat gyűjt össze, különös tekintettel azokra, ahol a kiberbiztonság / IT-biztonság nem mellékszál, hanem a képzés egyik szervező elve. A cél kettős: egyrészt gyors eligazodást adni a döntéshozóknak és képzésszervezőknek, másrészt pályatérképet adni a jelentkezőknek és munkaadóknak.

Az összehasonlításban kiemelt szerepet kap, hogy az egyes képzések milyen fókuszúak (mérnöki, vezetői/GRC - Irányítás, Kockázat és Megfelelőség, jogi–humán), milyen tipikus belépői háttérrel érdemes rájuk jelentkezni, illetve hogyan illeszthetők egy közös, európai kompetencianyelvhez: az ENISA European Cybersecurity Skills Framework (ECSF) szerepkör-profiljaihoz.

Miért válasszuk a kiberbiztonságot szakmaként?

A kiberbiztonság ma már nem szűk IT-részterület, hanem üzletmenet-, szolgáltatás- és társadalombiztonsági kérdés: a szervezetek működésének folyamatos digitális kitettsége miatt a védelem, az incidenskezelés, a kockázatkezelés és a megfelelés egyszerre vált mindennapi feladattá. Európai szinten a szakemberhiány és a készségrések tartósan jelen vannak; az ENISA kifejezetten a munkaerőhiányt és a képzettségi hiátust (skills gap) nevezi meg az ECSF létrejöttének egyik fő mozgatójaként.

Emellett a kiberbiztonság multidiszciplináris szemléletű tudományág. Stabil karrierutat kínál nemcsak informatikusoknak és mérnököknek, hanem jogi, menedzsment, audit, kommunikációs, vagy akár oktatási hátterű szakembereknek is. Az ENISA ECSF szemlélete is erre épít. A különböző szerepkörök (pl. CISO, auditor, jogi/megfelelési szakértő, incidens-reakció) együtt adják ki a szervezeti védelmi ökoszisztémát, és az oktatás is akkor lesz hatékony, ha ezekhez a valós szerepekhez illeszkedő kompetenciákat fejleszt.

Van, akinek kötelező

A 2024. évi LXIX. törvény 11. § (3) bekezdése kimondja, hogy az elektronikus információs rendszer biztonságáért felelős személy (IBF) feladatait – meghatározott szervezeti körben – csak olyan személy végezheti, aki cselekvőképes, büntetlen előéletű, és rendelkezik a feladatellátáshoz szükséges, a miniszteri rendeletben (képzési és továbbképzési kötelezettségeket a 17/2025. (VII. 24.) EM rendelet) előírt végzettséggel, valamint a nemzeti koordinációs központ által közzétett szakképzettséggel, akkreditált nemzetközi képzettséggel, vagy az előírt szakterületen szerzett szakmai tapasztalattal. Az írás főként ebben a körben releváns szakképzésekről igyekszik átfogó képet nyújtani.

Az ECSF szerepe és jelentősége az oktatásban

Az ENISA ECSF egy európai szintű, gyakorlati keretrendszer: közös fogalmi alapot ad a kiberbiztonsági szerepkörök, feladatok, készségek és tudáselemek leírására, és segít összekötni a munkaerőpiaci elvárásokat a képzési programok tanulási kimeneteivel. Az ENISA célként nevesíti, hogy az ECSF közös európai nyelvet adjon a szereplők (munkáltatók, egyének, képzők) között, és támogassa a képzések tervezését, a kompetenciák közti választás megkönnyítését.

Oktatási szempontból az ECSF akkor különösen hasznos, amikor egy képzés fókuszát és mélységét kell pontosan pozicionálni: ugyanaz a kiberbiztonság címke mást jelent egy mérnöki (architektúra/implementáció), egy vezetői (stratégia/kockázat/irányítás) vagy egy jogi-humán (compliance, szabályozás, adatvédelem) programban.

Az ECSF szerepkör-profiljai ezt a különbséget strukturáltan láthatóvá teszik, és támogatják a tantervi lefedettség (mit tanítunk?) és a karrierkimenetek (milyen munkakörre készít fel?) összerendelését. Éppen ezért ez az írás kísérletet tesz a különböző képzések ECSF kompetenciáinak feltárására is.

Végül az ECSF a minőség és az összehasonlíthatóság felől is értelmezhető: ha egy képzés nyíltan vállalja, hogy mely szerepkörökhöz fejleszt kompetenciákat, az segíti a jelentkezőket a tudatos választásban, a munkáltatókat pedig a valós tudástartalom megértésében. Az ENISA kiemeli, hogy az ECSF az EU referencia-pontja a releváns készségek meghatározására és értékelésére, és hozzájárul a készséghiányok célzott kezeléséhez.

Fontos kiemelni, hogy az anyagban szereplő ENISA ECSF besorolások tájékoztató jellegűek, nem minősülnek hivatalos, akkreditált megfeleltetésnek, és nem jelentenek ENISA által jóváhagyott tanúsítást vagy minősítést egyetlen képzésre nézve sem. A mappingek a nyilvánosan elérhető képzésleírások, célok és (ahol hozzáférhető) tantárgyi tematikák alapján készültek, annak érdekében, hogy közös európai szerepkör-nyelven összehasonlíthatóvá váljon, mely programok milyen típusú kompetenciákat fejlesztenek; a végleges, intézményi szintű megfeleltetéshez minden esetben részletes tantervi és tanulási kimenet (learning outcomes) elemzés, illetve a képző intézmény hivatalos állásfoglalása szükséges.

További információ az ENISA ECSF-ről az alábbi linken érhető el.

ENISA ECSF – kompetenciák/ szerepkörök

Az ENISA az ECSF-ben 12 tipikus kiberbiztonsági szakmai szerepkört ír le, mely segít a szereplőknek eligazodni a képzések és kompeteicák kiberbiztonsági tengerében.

- **Chief Information Security Officer (CISO):** A szervezet kiberbiztonsági stratégiáját, irányítási rendszerét (pl. ISMS) és erőforrásait fogja össze. Kockázati döntéseket készít elő vezetői szinten, és biztosítja, hogy a biztonsági célok illeszkedjenek az üzleti célokhoz.

- **Cyber Incident Responder:** A kibertámadások és incidensek észlelésében, elemzésében, elhárításában és a működés helyreállításában kulcsszereplő. Tipikusan SOC/CSIRT együttműködésben dolgozik, és a tanulságokat visszacsatornázza a megelőzésbe.

- **Cyber Legal, Policy & Compliance Officer:** A jogszabályi és belső szabályozási megfelelést (compliance) és a policy-k kialakítását viszi; hidat képez a technológia és a jogi követelmények között. Erős fókusz a felelősségek, kötelezettségek, dokumentáció és auditálhatóság terén.

- **Cyber Threat Intelligence Specialist:** Fenyegetési információkat gyűjt, értékel és kontextusba helyez (TTP-k, kampányok, fenyegetői motivációk). A cél, hogy a védelem proaktívabb legyen: priorizált kockázati képet adjon a döntésekhez és a technikai védekezéshez.

- **Cybersecurity Architect:** Biztonságos rendszerek és szolgáltatások tervezéséért felel, „security-by-design” szemlélettel. Követelményeket, architekturális megoldásokat és kontrollokat alakít ki, és gondoskodik arról, hogy a technológiai döntések fenyegetési modellhez illeszkedjenek.

- **Cybersecurity Auditor:** A kontrollkörnyezet és a biztonsági intézkedések megfelelőségét és hatékonyságát ellenőrzi, hiányosságokat tár fel, javaslatokat ad a javításra. Erős kapcsolódás a bizonyíték-alapú értékeléshez, auditjelentésekhez és a követelményrendszerekhez.

- **Cybersecurity Educator:** Tudatossági és képzési programokat tervez és valósít meg, a célcsoporthoz illesztett tananyaggal. A hangsúly azon van, hogy a szervezetben és a társadalomban mérhetően javuljon a biztonságtudatos viselkedés és az alapvető „cyber hygiene”.

- **Cybersecurity Implementer:** Konkrét védelmi megoldásokat (eszközöket, konfigurációkat, kontrollokat) vezet be és üzemeltet – a tervezett követelmények „lefordítása” a működő védelemre. Tipikus területek: hardening, hozzáférés-kezelés, hálózatvédelem, naplózás/monitoring.

- **Cybersecurity Researcher:** Új módszerek, technológiák és védelmi megközelítések kutatásán dolgozik, eredményeit publikálja vagy prototípusokban hasznosítja. Különösen fontos, ahol gyorsan változó fenyegetések és új technológiák (pl. AI, IoT) jelennek meg.

- **Cybersecurity Risk Manager:** A kiberkockázatok azonosítását, elemzését, értékelését és kezelését vezeti, jellemzően üzleti

prioritásokhoz kötötten. Az eredmény gyakran kockázatértékelési riport és kockázatcsökkentési intézkedési terv, amely összhangot teremt a vezetői döntések és a technikai megvalósítás között.

- **Digital Forensics Investigator:** Digitális bizonyítékokat gyűjt, megőriz és elemez incidensek, visszaélések vagy jogviták esetén. A fókusz a bizonyítékok integritásán, az elemzés szakszerűségén és azon van, hogy az eredmény felhasználható legyen szervezeti és (adott esetben) jogi eljárásokban.

- **Penetration Tester:** A biztonsági kontrollok hatékonyságát vizsgálja, sérülékenységeket tár fel és értékel a tényleges kihasználhatóság szempontjából. Célja, hogy a szervezet még a támadók előtt azonosítsa a kritikus gyengeségeket, és a javítások priorizálhatók legyenek.

További információk a szerepkörökről és kompetenciákról az alábbi linken érhető el.

Felsőoktatási képzések

Óbudai Egyetem: Kiberbiztonsági mérnöki BSc

A Kiberbiztonsági mérnöki alapképzés célja kiberbiztonsági mérnökök képzése, akik képesek szervezetek működését támogató információbiztonsági rendszerek és infokommunikációs eszközök biztonságos üzemeltetésére, illetve az üzletmenet-folytonosság támogatására. Ez a célmeghatározás már alapszinten is erősen védelmi irányt jelez, nem pusztán általános informatikai alapozást.

A BSc-szint sajátossága, hogy a hallgatóknak egyszerre kell felépíténiük magukban a klasszikus informatikai törzsanyagot (programozás, adatbázisok, hálózatok, operációs rendszerek) és a kiberbiztonsági látásmódot. A program célja alapján hangsúlyosak azok az alapfogalmak és technikák, amelyek átjárót képeznek az általános informatika és a kibervédelem között: például jogosultságkezelés, hálózati szegmentáció, hardening, alap kriptográfiai megoldások és incidensek felismerésének módszertana.

A tematikai fókusz sokszor gyakorlati kompetenciákban mérhető: egy végzett BSc-s kiberbiztonsági mérnöktől a munkaerőpiac tipikusan azt várja, hogy (felügyelet mellett) képes legyen biztonsági szempontból helyesen konfigurálni és üzemeltetni rendszereket, naplókat értelmezni, alapvető kockázatokat felismerni, és incidens esetén a „first responder” jellegű teendőket strukturáltan végrehajtani. A képzés célmondataiban megjelenő üzletmenet-folytonosság pedig arra utal, hogy a technikai tudás mellé a működési folyamatok és a helyreállítási logika is beépül.

A képzés karaktere a leírás alapján erősen mérnöki, ugyanakkor a BSc-szint miatt jellemzően nem mély-specialista területekre, hanem stabil alapokra és széles spektrumú üzemeltetési biztonságra épít. Ez akkor különösen értékes, ha a hallgató később MSc-n, vagy munkahelyi specializációval szeretne továbblépni például tesztelés, incidenskezelés vagy architektúra irányba.

Jelentkezni azoknak érdemes, akik már a pályaválasztás elején tudják, hogy az informatikán belül a védekezési oldal érdekli őket: SOC, üzemeltetésbiztonság, biztonságos hálózatok, security engineering, vagy később akár kritikus infrastruktúrák védelme. A képzés előnye lehet, hogy a biztonság, mint fő fókusz identitást ad, ami a belépő pozícióknál (junior security engineer, SOC analyst,

CTI elemzés NEMZETI KIBERBIZTONSÁGI INTÉZET

security operations) egyértelmű versenyelőnyt jelenthet a kiválasztási folyamat során.

ENISA ECSF-lefedettség oldalról a képzés tipikusan a Cybersecurity Implementer és a Cyber Incident Responder belépő feladatköreihez ad alapokat, és részben előkészíti a Cybersecurity Architect (junior) szemléletet is. A későbbi specializáció függvényében a tanult alapok átvihetők a Penetration Tester vagy a Digital Forensics Investigator szerepkörök irányába is, de ezek általában MSc-n vagy célzott gyakorlati pályán válnak teljes értékűvé.

További információk a képzésről az alábbi linken érhető el.

Óbudai Egyetem: Kiberbiztonsági mérnöki MSc

A kiberbiztonsági mérnöki (MSc) képzést az Óbudai Egyetem Neumann János Informatikai Kara hirdeti, a képzés telephelye Budapest, a szak 4 féléves, magyar nyelvű, és a meghirdetésben levelező munkarend is szerepel.

A képzés logikája tipikusan mérnöki: nem pusztán biztonsági szemléletet ígér, hanem olyan rendszerszintű tudást, amelynek középpontjában információbiztonsági követelményekre tervezett és üzemeltetett infokommunikációs és IT-rendszerek állnak. A kiberbiztonsági mérnöki szakleírásokban általában hangsúlyos a fenyegetések és sérülékenységek megértése, a védelmi kontrollok kiválasztása és bevezetése, valamint a biztonság „beépítése" (security-by-design) az életciklus különböző pontjain.

Tematikailag ez a típusú MSc jellemzően három nagy blokkra osztható: az első a biztonságtechnológiai alapozás (kriptográfiai alapok, hálózati és rendszerbiztonság, autentikáció/azonosítás, naplózás és monitorozás), a második alkalmazás- és fejlesztésbiztonság (biztonságos szoftvertervezés, sebezhetőségi mintázatok, tesztelési és verifikációs megközelítések), a harmadik üzemeltetési és incidenskezelési témák (detektálás, reagálás, helyreállítás, üzletmenet-folytonosság). A képzési célokból következően a hallgató nem „egy eszközre" tanul rá, hanem arra, hogy különböző szervezeti környezetekben tudjon biztonsági döntéseket hozni, és azt műszaki kontrollokban is lefordítani.

A fókusz egyértelműen mérnöki/technikai, ugyanakkor a munkaerőpiaci realitás miatt a képzésben jellemzően megjelenik a biztonságirányítási és megfelelési szemlélet (például auditálhatóság, biztonsági követelményrendszerek, kockázatalapú gondolkodás). Ez a kettősség fontos: a kibervédelem nemcsak „tűzfal és EDR", hanem tervezési döntések, üzemeltetési fegyelem és folyamatos javítási ciklus.

Jelentkezni azoknak érdemes, akik informatikai/műszaki alapképzettséggel rendelkeznek, és a karrierjükben biztonsági mérnöki, védelmi architektúra, SOC/IR vagy biztonságos fejlesztés irányba szeretnének lépni. A levelező jelleg különösen releváns lehet már dolgozó üzemeltetőknek, fejlesztőknek, rendszermérnököknek, akik meglévő szakmai tudásukat kiberbiztonsági kompetenciákkal kívánják kiegészíteni.

ENISA ECSF-lefedettség szempontból egy ilyen MSc tipikusan erős alapot ad a Cybersecurity Implementer, Cybersecurity Architect és részben a Penetration Tester szerepkörhöz, valamint – az üzemeltetési/reakciós komponensek arányától függően – a Cyber Incident Responder profilhoz is. Kiegészítő (részleges) lefedettség szokott lenni a Cybersecurity Risk Manager és Cybersecurity Auditor irányok felé, amennyiben a képzés kockázatmenedzsmentet és kontrollrendszer-szemléletet is tanít.

További információk a képzésről az alábbi linken érhető el.

Nemzeti Közszolgálati Egyetem: Kiberbiztonsági MA

A Nemzeti Közszolgálati Egyetem a kiberbiztonsági mesterképzést az Államtudományi és Nemzetközi Tanulmányok Kar keretében hirdeti, Budapest telephellyel, 4 féléves képzési idővel, nappali és levelező munkarendi formákkal.

Az NKE képzésének intézményi célmeghatározása kifejezetten jelzi, hogy a szak elsődleges célcsoportja a közszolgálatban kiberbiztonságért felelős szakemberek köre, akik a nemzetközi kapcsolatok, az állami/önkormányzati szervezetek információbiztonsága és a létfontosságú informatikai rendszerek védelme területén terveznek dolgozni – ugyanakkor a hallgatók piaci kihívásokra is felkészülnek. Ez a pozicionálás már önmagában eltér a klasszikus tisztán mérnöki MSc-k logikájától: erősebb benne a kormányzati/államigazgatási környezet és a kritikus infrastruktúrák szemlélete.

Tematikailag az NKE-s megközelítés tipikusan ott erős, ahol a kiberbiztonság nem csupán technológiai, hanem intézményi és társadalmi funkció: állami rendszerek, közszolgáltatások, létfontosságú rendszerelemek, valamint a kibertérrel összefüggő nemzetközi dimenziók. A kiberbiztonsági kockázatok értelmezése itt gyakran összekapcsolódik a szabályozással, a szervezeti felelősségi körökkel, az együttműködéssel (például incidensek koordinációja) és a döntéshozatali mechanizmusokkal.

A képzés vezérfonalát ezért érdemes vezetői–kormányzási és humán irányból megfogni: a hallgató nem csak eszközöket, hanem rendszerszintű működést és felelősségi viszonyokat is tanul. Ez azoknak különösen releváns, akik információbiztonsági felelősként,

kiberbiztonsági koordinátorként, szabályozási vagy stratégiai szerepben dolgoznak, vagy ilyen irányba szeretnének lépni – akár közigazgatásban, akár nagyvállalati környezetben.

Jelentkezni azoknak érdemes, akik már rendelkeznek valamilyen informatikai, műszaki, jogi vagy közigazgatási háttérrel, és a kiberbiztonságot szervezeti–irányítási kérdésként is szeretnék érteni: hogyan lesz egy intézmény komplex módon reziliens, milyen döntések és folyamatok kellenek a védekezéshez, és miként kapcsolódik ehhez a nemzetközi környezet. A nappali és levelező forma párhuzamos jelenléte jó jelzés arra, hogy a szak egyszerre célozhat frissen végzetteket és már dolgozó szakembereket is.

ENISA ECSF-lefedettség tekintetében az NKE-s kiberbiztonsági MA különösen jól illeszkedik a CISO (vezetői/stratégiai), a Cybersecurity Risk Manager, valamint a Cyber Legal, Policy & Compliance Officer szerepkörök feladatvilágához; ezek mellett – a technikai komponensek arányától függően – részleges lefedettséget adhat a Cyber Incident Responder és a Cyber Threat Intelligence Specialist profilokhoz is.

További információk a képzésről az alábbi linken érhető el.

Nemzeti Közszolgálati Egyetem: International Cybersecurity Studies (MA)

Az NKE International Cybersecurity Studies elnevezésű mesterképzése budapesti telephellyel, angol nyelven, 2 féléves képzési idővel, és nappali-blended munkarenddel indul.

A 2 féléves struktúra jelzésértékű: ez tipikusan egy kompakt, fókuszált, gyakran policy- és stratégiai szemléletű programformát jelent, amely nem feltétlenül a mély műszaki laborokra, hanem

a kiberbiztonság nemzetközi, intézményi és kormányzási összefüggéseire épít. Az angol nyelvűség pedig a nemzetközi diskurzushoz (EU-s és globális kiberpolitika, nemzetközi együttműködések, normák) illeszkedő tananyag-felépítést tesz lehetővé, ezt erősíti.

A program értéke abban áll, hogy a kiberbiztonságot nem csupán IT-alrendszerként, hanem közpolitikai és nemzetközi biztonsági kérdésként kezeli: hogyan hat a kiber a diplomáciára, a nemzetbiztonságra, a kritikus infrastruktúrákra, illetve a köz- és magánszféra kapcsolatrendszerére. Ezzel együtt a tananyagban jellemzően megjelenik az a minimális technológiai műveltség, amely nélkül stratégiai döntéseket sem lehet hozni (alapfogalmak, tipikus támadási mintázatok, kockázat és védelmi logika).

A képzés vezérfonala emiatt elsősorban vezetői/humán, azon belül is nemzetközi és stratégiai. Különösen releváns lehet olyan jelentkezőknek, akik kormányzati, szabályozói, nemzetközi szervezeti, vagy vállalati nemzetközi kapcsolati környezetben dolgoznak, és a kibertérrel összefüggő döntéseket, kockázatokat és szabályozási dilemmákat szeretnék professzionálisan kezelni.

Jelentkezni azoknak érdemes, akiknek a célja nem feltétlenül a technikai specializáció, hanem az, hogy képesek legyenek kiberbiztonsági programokat, együttműködéseket és szabályozási/stratégiai kezdeményezéseket átlátni és támogatni. A nemzetközi fókusz a későbbi pályák között reálisan megnyitja a kiberpolitikai elemző, kiberbiztonsági tanácsadó, kockázatkezelési vagy megfelelőségi irányokat.

ENISA ECSF-lefedettség szempontjából ez a program jellemzően legerősebben a CISO, a Cybersecurity Risk Manager és a Cyber Legal, Policy & Compliance Officer profilok kompetenciaigényeihez illeszkedik, és részlegesen támogathatja a Cyber Threat Intelligence Specialist (stratégiai/elemző oldal) szerepkört is.

További információk a képzésről az alábbi linken érhető el.

Széchenyi István Egyetem: Modern technológiák és kiberbiztonság joga MA

A Széchenyi István Egyetem modern technológiák és kiberbiztonság joga címmel hirdet 4 féléves mesterképzést, Győr telephellyel, magyar nyelven, nappali és levelező munkarendben. A képzés magyar és angol nyelven is meghirdetésre kerül.

A szak lényegi sajátossága, hogy a kiberbiztonságot jogi és szervezeti oldalról értelmezi, miközben a képzési cél alapján az itt végzetteknek két nyelvet kell beszélniük: érteniük kell a kiberbiztonsági folyamatok informatikai logikáját, és ugyanakkor képesnek kell lenniük a kapcsolódó jogi szabályozás és belső szervezeti szabályok (policyk, eljárásrendek) kialakítására. A képzés célja, hogy az okleveles modern technológiai és kiberbiztonsági jogi szervezők képesek legyenek kiberbiztonsági támogató informatikai feladatok menedzselésére, folyamatok modellezésére és a legjobb gyakorlatok beépítésére, valamint a jogi szabályozás ismeretére és belső szabályozók elkészítésére.

Tematikailag ez az interdiszciplináris képzés tipikusan olyan tárgyköröket emel be, amelyek a tisztán jogi képzésekből hiányoznak, a tisztán műszaki képzésekben viszont nem kapnak elég mély szabályozási kontextust. A modern technológiák (digitális platformok, adatvezérelt rendszerek, felhő, automatizáció) kiberkockázatai itt nem önmagukban jelennek meg, hanem mint szabályozási és szervezetirányítási kérdések: milyen kötelezettségek, felelősségi körök, bizonyítási és

auditálási elvárások keletkeznek, és ezek hogyan fordíthatók le működő vállalati/állami gyakorlatra.

A képzés iránya ezért egyszerre vezetői és humán/jogi, de nem tisztán jogi: a kiberbiztonsági informatikai folyamatok modellezése, tervezése és a támogató feladatok menedzselése kifejezetten interdiszciplináris profilt jelez. Ez a kombináció különösen értékes lehet azoknál a szervezeteknél, ahol a jogi megfelelés, az IT-üzemeltetés és a biztonság „tulajdonosa" több különböző egység, és szükség van olyan szakemberekre, akik ezek között képesek közvetíteni.

Jelentkezni tipikusan azoknak érdemes, akik kiberbiztonságban governance, risk, compliance (GRC), adatkezelési és szabályozási, vagy belső kontrollrendszeri területen szeretnének elhelyezkedni, és ehhez egy jogilag megalapozott, de technológiailag is értelmezhető tudáscsomagot keresnek. A levelező munkarend arra utal, hogy a célközönségben erős lehet a már dolgozó jogász, megfelelőségi szakember, IT-vezetői környezetben dolgozó szakértő.

ENISA ECSF-lefedettség szerint ez a mesterképzés különösen jól illeszkedik a Cyber Legal, Policy & Compliance Officer profilhoz, és a szervezeti folyamat- és programmenedzsment fókusz miatt erős kapcsolódása lehet a CISO és a Cybersecurity Risk Manager szerepkörökhöz is. A „támogató informatikai feladatok menedzselése" miatt részleges lefedettség adódhat a Cybersecurity Auditor irányába (kontrollok, megfelelés és ellenőrizhetőség), valamint a Cybersecurity Architect profil felé.

További információk a képzésről az alábbi linken érhető el.

Szakirányú továbbképzések

Széchenyi István Egyetem: Kiberbiztonsági szakjogász

A kiberbiztonsági szakjogász 2 féléves szakirányú továbbképzés célja, hogy a végzettek alkalmasak legyenek a kibertér és kapcsolódó technológiák által generált, állami–gazdasági–társadalmi alrendszerekre veszélyt jelentő folyamatok felismerésére, a kapcsolódó jogi szabályozás ismeretére, valamint a szervezeten belüli szabályozók megalkotásának felismerésére és – adott esetben – elkészítésére. Ez a célkép nagyon világosan egy jogi–szabályozási kiberbiztonsági szerepet ír le.

A 2 félév során jellemzően havonta és online formában kerül lebonyolításra a képzés. Ez a konstrukció tipikusan azt szolgálja, hogy dolgozó jogászok és jogi területen mozgó szakemberek a munkájuk mellett is elvégezhessék.

Tematikailag egy kiberbiztonsági szakjogász képzés jellemzően a kiberbiztonság azon jogterületi metszeteit rendezi össze, amelyek a szervezeti gyakorlatban naponta megjelennek: információbiztonsági kötelezettségek és felelősség, szerződéses és felelősségi kérdések, incidensek jogi kezelése, bizonyítás, auditálhatóság, belső szabályozás, valamint az adatkezeléshez és digitális szolgáltatásokhoz kapcsolódó compliance. A képzési célban hangsúlyos belső szabályozók kifejezetten policy-alkotási és szervezeti normaképzési kompetenciát jelent.

A képzés fő iránya alapvetően humán/jogi, ugyanakkor a célleírásból következően szükségszerűen érinti a technológiai alapokat is

– nem mérnöki mélységben, hanem annyiban, hogy a jogi szabályozás és a kiberkockázat megértése a tárgy technikai természetének ismerete nélkül nem reális. A kiberbiztonsági szakjogász szerepe a szervezetekben tipikusan akkor válik kulccsá, amikor a biztonság már nem csak egy IT probléma, hanem szerződéses, felelősségi, reputációs és hatósági dimenzióval is bír.

Jelentkezni azoknak érdemes, akik jogászként, compliance szakemberként, adatvédelmi és információbiztonsági feladatok közelében dolgoznak, és a klasszikus jogi háttér mellé szeretnének kiberbiztonsági szaknyelvet és gyakorlati szervezeti szabályozási képességet. Különösen hasznos lehet közintézményeknél, kritikus infrastruktúrák közelében, pénzügyi szektorban, nagyvállalati környezetben, illetve beszállítói láncok jogi támogatásában.

ENISA ECSF-lefedettség alapján a kiberbiztonsági szakjogász képzés legerősebben a Cyber Legal, Policy & Compliance Officer profilhoz illeszkedik, és részben a Cybersecurity Risk Manager és Cybersecurity Auditor szerepkörök „jogi-megfelelési” oldala felé is ad releváns kompetenciákat (szabályozók, eljárásrendek, auditálhatóság, incidensek jogi kezelése).

További információk a képzésről az alábbi linken érhető el.

Milton Friedman Egyetem: ICT Biztonsági Szakember

A képzés deklarált célja olyan szakemberek felkészítése, akik vállalati ICT-biztonsági rendszerek létrehozására és működtetésére, illetve ICT-biztonsági feladatokat ellátó csoportok szakmai munkájára és irányítására képesek, továbbá támogatni tudják az üzleti döntéselőkészítést információgyűjtéssel és -feldolgozással. A képzés egy

tipikusan gyakorlati hasznosságra hangolt posztgraduális konstrukció: nem alapképzést vált ki, hanem már meglévő diplomára épít. A program 3 féléves, és a tájékoztató szerint az oktatás 7 hétvégén (péntek–szombat) zajlik.

A tematikai fókusz egyszerre technikai és irányítási jellegű. A fő témakörök között külön nevesítik az ICT-biztonsági jogi ismereteket, a biztonságmenedzsmentet, az etikus hackelést, az informatikai rendszerek ellenőrzését, a kockázatelemzést és a forenzikus vizsgálatot. Ez a kombináció tipikusan úgy áll össze egy szerves egésszé, hogy a hallgató egyrészt érti a védelmi intézkedések logikáját (kontrollok, audit, risk), másrészt képes technikai oldalról is rálátni (tesztelés, incidens- és bizonyítékkezelés).

Profilját tekintve a képzés mérnöki és vezetői/GRC képességek keverékét nyújtja. A biztonságmenedzsment és jogi ismeretek a megfelelőségi és szervezeti dimenziót erősítik, míg az etikus hackelés, ellenőrzés és forenzika a technikai készségterületeket támogatja. Jelentkezni ezért tipikusan azoknak érdemes, akik IT/üzemeltetés/fejlesztés felől érkeznek és fókuszuk a security, vagy információbiztonsági feladatkörben dolgoznak és szeretnék strukturáltan összeépíteni a kockázat–kontroll–incidenskezelés–vizsgálat láncot.

Az ECSF logikája szerint ez a tananyag tipikusan több profilt is érint. Elsődlegesen: Cybersecurity Implementer / Operator (ellenőrzés, tesztelés, üzemeltetéshez kötődő kontrollok), Cybersecurity Auditor (rendszerellenőrzés, megfelelőség-ellenőrzés), Digital Forensics Investigator (forenzika), valamint részben Cybersecurity Risk Manager / CISO (kockázatelemzés, biztonságmenedzsment). A jogi ismeretek miatt kis részben érinti a Cyber Legal, Policy and Compliance Officer profilt is.

További információk a képzésről az alábbi linken érhető el.

Nemzeti Közszolgálati Egyetem: Elektronikus információbiztonsági vezető

Ez a képzés erősen „szabályozási és közszolgálati logikára” épül: a célját kifejezetten úgy határozzák meg, hogy a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvényben nevesített, elektronikus információs rendszer biztonságáért felelős személyek feladatellátásához szükséges kompetenciákat adja át, és biztonságtudatos szemléletet alakítson ki. A végzett hallgató szerepe nem csak technikai: a szervezet információbiztonsági rendszerének kialakítása és fenntartása mellett a munkatársak szemléletformálása is feladat.

A kompetencialista kimondottan részletes, és szépen kirajzolja a „vezetői információbiztonság” profilját: szabályozási előírások értelmezése, kibertámadások elleni védelmi megoldások és eljárások ismerete, létfontosságú rendszerelemek fogalma, belső szabályzatalkotás szükségessége, emberi tényező, kártékony kódok, állami kibervédelmi rendszer – és mindezek szervezeti alkalmazása. Képességszinten külön kiemelik a vezetői támogatás megszerzését a megfelelőséghez, a humán kockázatok csökkentését célzó intézkedéseket, és a támadási lánc (cyber kill chain) elemeihez kapcsolódó technológiai intézkedéseket.

A tantárgylista is jelzi, hogy ez GRC, technikai alapozás és vezetés kombinációjának tekinthető: információbiztonsági és adatvédelmi szabályozás, információbiztonsági szabványok, kockázatértékelés, incidensmenedzsment, biztonsági tesztelés, információbiztonsági stratégia és vezetés, európai kiberbiztonsági szabályozás, válságmenedzsment és kommunikáció, hálózatbiztonság. A két féléves képzés a módszertan alapján levelező rendszerű, e-learning támogatással.

A belépés feltétele legalább alapképzésben szerzett oklevél, és külön jelzik, hogy a felhasznált szakirodalmak, szabványok, esettanulmányok jelentős része angol nyelvű, ezért elvárt a szakmai angol ismerete. Emellett (hallgatói jogviszony létesítéséhez) előfeltétel a büntetlen előélet igazolása.

Az ENISA ECSF szerepkörök közül itt nagyon erős a CISO / Information Security Officer jelleg (stratégia, vezetés, ISMS, döntéstámogatás), a Cyber Legal, Policy and Compliance Officer (szabályozás, megfelelőség, belső szabályzatok), valamint a Cybersecurity Risk Manager (kockázatértékelés, kockázatmenedzsment). Másodlagosan érintheti a Cybersecurity Incident Responder és Cybersecurity Auditor profilokat (incidensmenedzsment, tesztelés, audit-logika), de a hangsúly szemmel láthatóan a szervezeti és kormányzati beágyazottságon van.

További információk a képzésről az alábbi linken érhető el.

Óbudai Egyetem: Információbiztonsági szakmérnök/szakember

A 4 féléves, levelező munkarendű, Budapesten zajló szakirányú képzés indoklása klasszikus üzemmenet-folytonosság és megbízhatóság narratívára épül, mivel folyamatosan nő az igény az információbiztonság és az információbiztonsági rendszerek használata iránt, ezért olyan már diplomás szakembereket képeznek, akik a tudást az információbiztonsági területeken alkalmazni tudják, tekintettel a folyamatos rendelkezésre állás és a biztonságos üzemeltetés üzleti fontosságára. A pozicionálás ezzel inkább enterprise security engineering / security operations jellegű, mintsem kizárólag kutatói.

A fő tantárgyi pillérek röviden, de beszédesen jelennek meg: információbiztonság alapjai, IT hálózati alapismeretek, vállalati irányítási rendszerek ismeretek, szoftverfejlesztési életciklus és módszerek, IT rendszerek üzemeltetésének fizikai biztonsági követelményei, valamint IT hálózatbiztonság. Ez a mix tipikusan azokat a kompetenciákat célozza, ahol a security nem különálló sziget, hanem beépül az IT működésébe (üzemeltetés, SDLC, szervezeti kontrollok), és gyakorlati hasznosítás technikai szinten is gyorsan végbe tud menni.

Belépési követelményként a képzésoldal legalább BSc oklevelet jelöl, a bemenet mérnöki szakképzettséghez kötött. A program elsősorban mérnöki alapokra épít, és a jelentkezési feltételek pontos értelmezését az intézményi felvételi tájékoztató adja meg.

Profilját tekintve ez a képzés mérnöki-üzemeltetési irányba húz: erős alapot ad ahhoz, hogy valaki infrastruktúra- és hálózati környezetben, illetve fejlesztési folyamatokban biztonsági szempontokat érvényesítsen. A vállalati irányítási rendszere" és a fizikai biztonsági követelmények ugyanakkor arra utalnak, hogy a program tudatosan nyit a GRC és a fizikai/üzemeltetési kontrollok irányába is.

Az ECSF szerepkörök közül itt elsődlegesen a Cybersecurity Implementer / Operator (hálózatbiztonság, üzemeltetés, SDLC-biztonság), valamint részben a Cybersecurity Architect (ha az irányítási rendszerek/tervezés hangsúlyos a tantárgyi kimenetekben) jelennek meg. Másodlagosan Cybersecurity Auditor (kontroll- és irányítási rendszerek logikája) és Incident Responder szerepkörre készít fel a kurzus.

További információk a képzésről az alábbi linken érhető el.

Zárszó

A feltárt képzési kínálat alapján a magyarországi, iskolarendszerű kiberbiztonsági utánpótlás ma már több, egymást kiegészítő „belépési kapun" keresztül érhető el: a mérnöki fókuszú (BSc/MSc) programok a technikai megvalósítás, architektúra és üzemeltetésbiztonság irányába készítenek fel, míg a vezetői/GRC és jogi–humán programok a kockázatkezelés, megfelelőség, szabályozás és szervezeti irányítás dimenzióit erősítik. Ez a többpólusú szerkezet a gyakorlatban előny, mert a kiberbiztonság szervezeti működéséhez egyszerre kell mély technikai kompetencia és olyan „fordítói" képesség, amely a jogi, üzleti és műszaki elvárásokat egy közös működési renddé alakítja.

A jogszabályi környezet közben egyre határozottabban formalizálja a kiberbiztonsági felelősségi szerepek kompetencia-elvárásait: az IBF feladatellátásához kötődő végzettségi és szakképzettségi elvárások, valamint az évenkénti továbbképzés kötelezettsége azt jelzi, hogy a kiberbiztonság nem eseti projekt, hanem folyamatosan fenntartandó szakmai gyakorlat. Ennek megfelelően az egyéni pályaépítésben és a szervezeti képzésmenedzsmentben is felértékelődik a „tanulási út" tervezése: belépés (alapozás), specializáció (mérnöki, incidens, audit, jog), majd folyamatos szinten tartás (továbbképzések, szabályozás- és technológia-követés).

Az ENISA ECSF keretrendszerének bevonása azért különösen hasznos, mert közös európai nyelvet ad a képzések és a munkaerőpiac összekapcsolásához: segít megnevezni, hogy egy program valójában mely szerepkörökhöz (pl. Implementer/Architect vs. CISO/Risk/Compliance) épít kompetenciát, és hol vannak átfedések vagy hiányok. A kompetencia-alapú megközelítés a jövőben kulcs

lehet a képzési portfólió tudatos fejlesztésében is: a technikai mélység, a governance–compliance és az emberi tényező (tudatosság, kommunikáció, válságkezelés) egyensúlya döntően befolyásolja, hogy a végzettek mennyire lesznek képesek a valós szervezeti kiberkockázatok kezelésére.

Források

ENISA

https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf (Letöltve: 2025.01.21.)

ENISA

https://www.enisa.europa.eu/sites/default/files/publications/European%20Cybersecurity%20Skills%20Framework%20Role%20Profiles.pdf (Letöltve: 2025.01.21.)

Óbudai Egyetem BGK

https://bgk.uni-obuda.hu/bsc-kepzes-kiberbiztonsagi-mernoki (Letöltve: 2025.01.19.)

Óbudai Egyetem NIK

https://nik.uni-obuda.hu/kiberbiztonsagi-mernoki-msc/ (Letöltve: 2025.01.19.)

Nemzeti Közszolgálati Egyetem ANTK

https://antk.uni-nke.hu/oktatas/mesterkepzes/kiberbiztonsagi-mesterkepzesi-szak (Letöltve: 2025.01.20.)

Nemzeti Közszolgálati Egyetem ANTK

https://antk.uni-nke.hu/oktatas/mesterkepzes/international-cybersecurity-studies-mesterkepzesi-szak (Letöltve: 2025.01.20.)

Széchenyi István Egyetem Felvételi

https://felveteli.sze.hu/modern-technologiak-es-kiberbiztonsag-joga-ma (Letöltve: 2025.01.22.)

Széchenyi István Egyetem Felvételi

https://felveteli.sze.hu/kiberbiztonsagi-szakjogasz (Letöltve: 2025.01.22.)

Milton Friedman Egyetem

https://uni-milton.hu/kepzesek/posztgradualis-kepzesek/ict-biztonsagi-szakerto/ (Letöltve: 2025.01.23.)

Nemzeti Közszolgálati Egyetem KTI

https://kti.uni-nke.hu/szakiranyu-tovabbkepzesek/szakiranyu-tovabbkepzesi-szakok/elektronikus-informaciobiztonsagi-vezeto/altalanos-informaciok (Letöltve: 2025.01.20.)

Óbudai Egyetem

https://uni-obuda.hu/szakok/informaciobiztonsagi-szakmernok-szakember/ (Letöltve: 2025.01.19.)

Összefoglaló táblázat a képzésekről

Intézmény	Képzés neve	Szint/ típus	Félév	Munkarend	Felvételi követelmény	Tematika	Fókusz	ENISA ECSF mapping
ÓE	Kiberbiztonsági mérnöki (BSc) – kiberbiztonsági mérnök	alapképzés	7	nappali és levelező	felvételi (érettségi + pontszámítás)	üzemeltetésbiztonság; hálózatvédelem; IBIR/ ISMS	mérnöki	Implementer; Incident Responder; (junior) Architect
NKE	Kiberbiztonsági mesterképzési szak – okleveles kiberbiztonsági szakértő	mesterképzés	4	nappali és levelező	BA (több belépő háttér); részletszabály intézményi	kritikus rendszerek; kockázat; kiberkormányzás	vezetői + humán/ stratégiai	CISO; Risk Manager; Legal/Policy/Compliance; (részben) CTI
NKE	Cybersecurity Studies – okleveles nemzetközi kiberbiztonsági szakértő	mesterképzés	2	nappali-blended	BA + erős szakmai angol	nemzetközi/policy; stratégia; risk	vezetői + humán	CISO; Risk Manager; Legal/Policy/Compliance; (részben) CTI
ÓE	Kiberbiztonsági mérnöki (MSc) – okleveles kiberbiztonsági mérnök	mesterképzés	4	nappali/ levelező (meghirdetéstől függően)	MSc-belépés + kredit-előfeltételek	védelmi architektúra; secure engineering; kriptográfia	mérnöki	Architect; Implementer; (részben) Penetration Tester; (részben) Incident Responder
SZE	Modern technológiák és kiberbiztonság joga – okleveles modern technológiai és kiberbiztonsági jogi szervező	mesterképzés	4	nappali és levelező	BA (több belépő háttér)	tech governance; kiberjog;	humán/jogi + vezetői	Legal/Policy/Compliance; Risk Manager; (részben) Auditor; (részben) CISO

Intézmény	Képzés neve	Szint/ típus	Félév	Munkarend	Felvételi követelmény	Tematika	Fókusz	ENISA ECSF mapping
MFE	ICT Biztonsági Szakember	szakirányú továbbképzés	3	levelező; hétvégi blokkok	BSc + (infó mérnök -> Szakértő) vagy BSc + igazolt infobizt. tapasztalat -> Szakember	etikus hackelés; kockázatelemzés; forenzika	mérnöki + vezetői/GRC	Implementer; Auditor; Digital Forensics Investigator; (részben) Risk Manager
NKE	Elektronikus információbiztonsági vezető	szakirányú továbbképzés	2	levelező + e-learning	BA/BSc; (jellemzően) szakmai angol; (jogviszonyhoz) büntetlen előélet	ISMS; kockázat;	vezetői + compliance/ GRC	CISO; Risk Manager; Legal/Policy/Compliance; (részben) Incident Responder
ÓE	Információbiztonsági szakmérnök/szakember	szakirányú továbbképzés	4	levelező	min. BSc (a részletszabály gyakran mérnöki előképzettséghez kötött)	hálózatbiztonság; SDLC; fizikai security	mérnöki/ üzemeltetési	Implementer; (részben) Architect; (részben) Auditor
SZE	Kiberbiztonsági szakjogász	szakirányú továbbképzés	2	jellemzően online/blended; havi ütemezés	jogász (állam- és jogtud. egyetemi oklevél)	kiberjog; belső szabályozók; megfelelés	humán/jogi	Legal/Policy/Compliance; (részben) Risk Manager; (részben) Auditor

NEMZETI
KIBERBIZTONSÁGI
INTÉZET

Kibertámadás!
podcast

Nemzetbiztonsági Szakszolgálat
Nemzeti Kiberbiztonsági Intézet

titkarsag@nki.gov.hu

nki.gov.hu

+36 (1) 325 7672

2026