Óbudai Egyetem
Neumann János Informatikai Kar

Kiberbiztonsági szakmérnök/szakember szakirányú továbbképzés

Budapest, 2020.

I. A szakindítási kérelem indoklása

Napjainkban, az informatikai rendszerek életünk minden területén teret hódítanak, aminek következtében a kevésbé érzékeny mindennapi adatainktól kezdve, a legkényesebb személyes adatainkig minden információ továbbításra vagy tárolásra kerül. Mind az ipari vagy vállalati kutatások, mind a különböző tudományterületek számára nélkülözhetetlenné váltak a felhő alapú lehetőségek és szolgáltatások. Okos városokban és okos otthonokban élünk, különböző mobil platformokról vagy az internetről intézzük hivatalos ügyeinket és közösségi alkalmazásokon keresztül érintkezünk kollégáinkkal, ismerőseinkkel és barátainkkal. Mivel minden rendszer csak annyira biztonságos, amennyire a leggyengébb láncszeme, teljes körű, mindenre kiterjedő védelemre lenne szükség, de éppen ez jelenti ma világszerte a legnagyobb kihívást.

A továbbképzés célja megismertetni a hallgatókkal az IT rendszerek biztonsággal kapcsolatos problémáit és hiányosságait, az azok megoldására alkalmazott korszerű módszereket és technológiákat, mindezt gyakorlati és praktikus készségekkel és alkalmazásokkal kiegészítve. Olyan mérnök-informatikusok képzésére törekszünk, akik képesek a modern IT rendszerekben felmerülő biztonsági problémák azonosítására, feltárására, a problémák megoldásához szükséges praktikus tervezési és fejlesztési feladatok elvégzésére, valamint a mélyebb elméleti alapokra (pl. kriptográfiára) épülő módszerek és rendszerek megértésére és alkalmazására.

A szakirányú továbbképzés a fentiekből következően Kiberbiztonsági szakmérnök szakon indul.

II. A szak tanterve és a tantárgyi programok leírása

1. Tanterv

	Kredit	Óraszám	Követelmény
I. félév			
Informatikai biztonság alapjai (elektronikus elméleti tananyaggal támogatott labor)	6	28	Vizsga
Adatvédelmi és információbiztonsági jogszabályok	6	28	Vizsga
IT hálózati alapismeretek	10	44	Évközi jegy
Felhasználói információbiztonsági szabályok	2	12	Évközi jegy
Projektlabor 1	7	60	Évközi jegy
I. félév összesen	**31**	**172**	
II. félév			
Informatikai rendszerek üzemeltetésének biztonsága	7	36	Vizsga
Logelemzés	4	20	Évközi jegy
Integrált vállalatirányítási rendszerek	3	12	Évközi jegy
Fizikai védelem / vagyonvédelmi rendszerek és módszerek	6	28	Évközi jegy
Felhőszolgáltatások biztonsági kérdései	4	20	Évközi jegy
Projektlabor 2	7	60	Évközi jegy
II. félév összesen	**31**	**176**	

	Kredit	Óraszám	Követelmény
III. félév			
Virtuális hálózatok és adatközpontok biztonsága	8	36	Vizsga
IT hálózatbiztonság	14	56	Évközi jegy
Projektlabor 3	8	80	Évközi jegy
III. félév összesen	**30**	**172**	
IV. félév			
Intézményi informatikai biztonság	9	36	Vizsga
Hacker eszközök, technikák	2	12	Évközi jegy
IT auditálás	7	30	Évközi jegy
Záródolgozati projekt	10	100	Évközi jegy
IV. félév összesen	**28**	**178**	

Képzési forma:
Szakirányú továbbképzés

Képzési cél:
Egymásra épülő, aktuális szakmai ismeretanyagot és piacképes tudást biztosítani azoknak a szakembereknek, akik az informatikai biztonság területeihez kapcsolódó munkakörökben dolgoznak.

Képzés helye:
Óbudai Egyetem, Neumann János Informatikai Kar,
1034 Budapest, Bécsi út 96/B.

Képzési idő:
4 félév, összesen 698 kontaktóra

Jelentkezés feltétele:
Szakmérnöki képzés: mérnöki BSc, vagy MSc, (korábbi egyetemi vagy főiskolai) oklevél
Szakember képzés: bármely felsőoktatási szakon szerzett BSc, vagy MSc, (korábbi egyetemi vagy főiskolai) oklevél

Finanszírozási forma:
Önköltséges (280.000 Ft/félév)

Megszerezhető végzettség:
Eredményes záróvizsga esetén hallgatóink oklevelet kapnak: **Kiberbiztonsági szakmérnök/szakember** megnevezéssel.
A szak angol nyelvű megjelölése: **Cybersecurity Engineering**
A szakképzettség angol nyelvű megjelölése: **Cybersecurity Engineer/Cybersecurity specialist**

Megszerezhető kreditek száma:
120 kredit

A képzés főbb területei:

Tárgyak jellege	Kredit
Alapismeretek és szakmai törzsanyag	60
Speciális szakismeretek	50
Szakdolgozat	10
Összesen	120

Értékelési és ellenőrzési módszerek, eljárások:
A tantárgyak vizsgával, illetve évközi jeggyel zárulnak. A vizsgára bocsátás feltétele tantárgyanként különböző: írásbeli, gyakorlati dolgozat, illetve egyéni feladat beadása egyaránt lehetséges.
A vizsga írásbeli vagy szóbeli lehet. A negyedik félév teljesítése során szakdolgozatot kell készíteni, majd az abszolutórium megszerzése után azt a záróvizsgán meg kell védeni, és a záróvizsga tárgyakból eredményes vizsgát kell tenni.

A korábban szerzett ismeretek, gyakorlatok beszámítási rendje:
A korábban, hasonló témában szerzett érdemjegyet az egyetem általános eljárási rendje szerint számítjuk be, azaz a félév kezdetén, index alapján és megfelelő tematika alapján a tantárgyfelelős oktató tesz javaslatot a beszámítás lehetőségére.

A záróvizsgára bocsátás feltételei:
A záróvizsgára bocsátás feltétele a végbizonyítvány (abszolutórium) megszerzése. Végbizonyítványt a felsőoktatási intézmény annak a hallgatónak állít ki, aki a tantervben előírt tanulmányi és vizsgakövetelményeket – szakdolgozat elkészítése kivételével – teljesítette és az előírt krediteket megszerezte.

A záróvizsga részei:
A záróvizsga a szakdolgozat védéséből és a tantervben előírt tárgyakból tett szóbeli vizsgákból áll. A záróvizsgát a hallgatónak egy napon, folyamatosan kell letenni. A záróvizsga szóbeli vizsgából áll, a felkészülési idő tantárgyanként legalább 20 perc.

A záróvizsga tárgyai:
- Informatikai rendszerek üzemeltetésének biztonsága;
- IT hálózatbiztonság;
- Intézményi informatikai biztonság.

A záróvizsga eredménye:
A szakdolgozatra és a záróvizsga szóbeli részére kapott érdemjegyek – a vizsgatárgyak számát figyelembe vevő – átlaga az alábbiak szerint:

$$Z=(SZD+Z1+Z2+..+Zm)/(1+m).$$

Az oklevél minősítése:
A záróvizsga eredménye alapján az oklevelet a következők szerint kell minősíteni:

kiváló	5,00
jeles	4,51 - 4,99
jó	3,51 - 4,50
közepes	2,51 - 3,50
elégséges	2,00 - 2,50

2. Tantárgyi programok

Informatikai biztonság alapjai

Áttekintés az informatikai biztonság területeiről, az egyes területek bevezető jellegű bemutatásával, és ezeken keresztül magáról a képzésről:

- Az informatikai biztonság fogalma, jelentősége, szerepe, rövid történeti áttekintése.
- Az informatikai biztonság jogi követelményei.
- Etikai kérdések, motivációk, célpontok. biztonságtudatosság, szabályozások.
- Kockázatelemzés/ kockázatkezelés, kockázatmenedzsment témái és módszerei.
- Munkaállomások, szerverek, hálózatok és infrastruktúrák sérülékenysége.
- Rosszindulatú szoftverek (malwerek).
- Felhasználó hitelesítés, jogosultság- és hozzáférés kezelés.
- A humánbiztonság feladatai. Operációs rendszerek jelszókezelése. Jelszó választás problémái, jelszótörés.
- Hálózati határvédelem (tűzfalak, IDS/IPS).
- PKI infrastruktúra.
- Biztonságos levelezés és adattárolás.
- Mobil platformok és felhő alapú rendszerek biztonsága.
- Alkalmazások sérülékenysége.
- Az üzletmenet-folytonosság.
- Kriptológia, kriptográfiai algoritmusok és alapprotokollok.

Adatvédelmi és információbiztonsági jogszabályok

- Az információbiztonsággal kapcsolatos, releváns jogszabályok csoportosítása, áttekintése. (Törvények és hozzá kapcsolódó egyéb jogszabályok, kormányrendeletek, stb.)
- Személyes adatok kezelésére vonatkozó követelmények (infotv.).
- Közérdekű adatok kezelésére vonatkozó követelmények (infotv.).
- Üzleti titok fogalma és védelme (PTK része).
- Nemzeti minősített adatok kezelésére vonatkozó követelmények (2009/CLV tv.).
- A nemzeti adatvagyon védelme (2010/CLII.tv.).
- Állami és önkormányzati szervek információbiztonsága (2013/L.tv.).
- Létfontosságú létesítmények és rendszerek követelményei (2012/CLXVI.tv.).
- Pénzügyi szektor IB követelményei (hpt. - 2013/CCXXVII.tv).
- Vétkezések az információbiztonság ellen, szabályok megsértése, visszaélések … (BTK részei).
- Vagyonvédelem és magánnyomozói tevékenység (2005/CXXIII.tv.) – és a megfigyelésekre vonatkozó jogszabályok is ebben.

IT hálózati alapismeretek

- A kommunikáció alapjai, topológiák, protokollok.
- Számítógépes hálózatok felépítése, működése. OSI rétegek.
- Keretek, csomagok fogalma, felépítése, enkapszuláció.
- Elterjedtebb L1 és L2 megoldások, vezetékes és vezeték nélküli kapcsolatok.
- L3 és L4 a gyakorlatban: TCP/IP modell (IP, TCP, UDP, stb.).
- Útválasztók működése, biztonsági lehetőségek.
- Alap hálózati szolgáltatások: DHCP, DNS.
- Hálózati referencia modellek.

- Internet alapelvek, az Internet címzési és névkezelési rendszere, az IP protokoll működési módja.
- kapcsolatmentes és kapcsolat-orientált adatátvitel jellemzői, szállítási protokollok.
- Vezetékes és rádiós lokális hálózati technikák, Ethernet hálózatok, kapcsolás (switching) és útválasztás (routing) működése.

Felhasználói információbiztonsági szabályok

- Számítógép használata.
- Mobil eszközök és adathordozók használata.
- Céges vs. magán-tulajdonú eszközök használata – cége vs. magán-célú használata.
- Céges hálózat használatának szabályai (inc. WiFi, távoli munka, VPN, etc…).
- Céges alkalmazások használata.
- Internet és E-mail használata.
- Jelszóhasználat.
- Titkosítások használata.
- Vírusvédelem használata, teendők vírus észlelésekor.
- Teendők információbiztonsági incidensek észlelésekor.
- Vállalati munkahely és helyszínek biztonságos használata.
- Fax és telekommunikációs eszközök használata.
- Biztonságos viselkedés munkahelyen és azon kívül.

Informatikai rendszerek üzemeltetésének biztonsága

- A vállalati biztonságfelügyelet és jellemző problémái.
- Az operációs rendszerekkel szemben támasztott alapvető elvárások.
- A felügyelet infrastruktúrájának tervezése.
- A címtár biztonságának védelme.
- Szerverek és ügyfélgépek ellenállóvá tétele, vírus-, behatolás védelme és központi menedzsmentje.
- Felhasználók hitelesítése. Felhasználó-nyilvántartási adatforrások valós idejű szinkronizációja.
- Felhasználó- és hozzáférés menedzsment.
- Biztonságos kapcsolat kialakítása a szolgáltatások igénybevételéhez.
- Nyilvános kulcsú infrastruktúra tervezése és megvalósítása.
- A leggyakoribb, interneten/intraneten/felhőben biztosított vállalati informatikai szolgáltatások biztonsági kérdései.
- Szoftverek sérülékenységéből származó kockázatok csökkentése.
- A webalkalmazások/webszolgáltatások alapvető fejlesztési hibáinak kiküszöbölése.
- Adatvédelem, adatmentés-visszaállítás, adatmentési rendszerek.

Logelemzés

- Hálózati forgalom monitorozása és rögzítése. Hálózati logelemzés célja, elvi háttere és eszközei.
- Naplógyűjtő és -elemző rendszerek, logelemző megoldások bemutatása.

Integrált vállalatirányítási rendszerek

A vállalati rendszer, vállalati információs rendszer. Vállalati külső kapcsolatok. Az információs rendszerrel szemben támasztott követelmények. Funkcionális követelmények és alrendszerek: értékesítés, beszerzés, cikk és készletnyilvántartás és - gazdálkodás, pénzügy,

gyártás. Az egyes funkciók üzleti és informatikai folyamatai. Az egyes funkciók kapcsolatai. Az integrált – és a sztenderd rendszer fogalma. Az Enterprise Resource Planning rendszerek. A partnerekkel történő információcsere fejlődése: papír alapú, EDI, e-Business. Az e-Business alapjai: B2C, B2B, B2E. A beszállítói – és ellátási lánc. Vezetés támogatás és működési mértékek. Az integrált rendszerek architektúrája. Rendszerhez jutási lehetőségek: fejlesztés, vásárlás, szolgáltatásként történő igénybevétel. Folyamatok és partner követelmények. Az új rendszer bevezetése.

Fizikai védelem / vagyonvédelmi rendszerek és módszerek

- Az őrzés-védelem célja, feladatai az információbiztonságban. Az őrzésvédelem eszköztára, módszerei.
- Zónamodell – elve és alkalmazása. Kockázatok számítása a zónamodellben. Zónák kialakításának célja, lehetőségei, szempontjai és módszerei.
- Élőerős őrzés-védelem.
- Beléptető technikai rendszerek, módszerek, eszközök.
- Authentikációs módok.
- Határvédelmi eszközök és rendszerek. Érzékelők, detektálók, riasztók. Megfigyelő rendszerek.
- Különböző technikák, rendszerek tulajdonságai, jellemzői, előnyök és hátrányok, alkalmazási területek.
- Védelmi rendszerek tervezésének alapjai.

Felhőszolgáltatások biztonsági kérdései

- Számítási felhő (cloud computing) rendszerek, valamint elterjedt publikus, privát és hibrid felhő platformok felhasználói, és üzemeltetői oldalról.
- A felhők által kínált szolgáltatások fajtái (IaaS/PaaS/SaaS), kialakításuk sajátosságai, jellemző megoldásaik, valamint kapcsolódó menedzsment és automatizálási lehetőségek.
- A publikus felhőszolgáltatások (pl. Amazon Web Services) használata, platformszolgáltatások (pl. Microsoft Azure) kialakítása és különböző interfészeken történő elérése.
- Felhőszolgáltatások biztonsága.

Virtuális hálózatok és adatközpontok biztonsága

- Adatközpontokkal szembeni változó elvárások.
- A hagyományos adatközponti megoldások korlátai.
- Több bérlős (multi-tenant) IaaS szolgáltatást ellátó virtualizált adatközponti megoldások.
- Virtual Multi-Tenant Data Center (VMDC) referencia architektúra bemutatása, az architektúra rétegszerkezete és rétegfunkciói.
- I/O konszolidáció. A VMDC modell rendszertechnikai építőelemei: Point of Delivery (PoD, Integrated Compute Stack (ICS).
- Az egyazon infrastruktúrán, azonos időben megvalósuló, biztonságos, bérlők közti logikai szeparáció megvalósítása. Az infrastruktúra magas szintű rendelkezésre állása.
- Adatközponti hálózat kialakításának lehetősége Cisco alapú eszközökkel.

IT hálózatbiztonság

- Hálózati topológia kialakítása, biztonsági szempontjai. (Hálózati szegmensek, alhálózatok, VLAN-ok, NAT, PAT, …).
- Biztonság az L1 és L2 rétegben (WiFi, 802.1x, ...).

- Biztonság az L3 és L4 rétegekben (routerek, tűzfalak lehetőségei).
- További gyakori biztonsági megoldások az OSI felsőbb rétegeiben (ssh, ssl, proxy megoldások, ...).
- Távoli hálózatok biztonságos elérése (L2 és L3 tunneling, VPN, ...).
- Felhő alapú rendszerek és szolgáltatások biztonsága.
- Néhány tipikus támadási lehetőség és az ellenük történő védekezés módja.
- A hálózatok üzemeltetése, dokumentáltsága, ezek biztonsági aspektusai.

A tárgy keretében a hallgatók megismerkednek többek között a Layer 2 (kapcsolók), Layer 3-4 (forgalomirányítók és tűzfalak), valamint a Layer 7 (NextGen tűzfalak, VPN szerverek, behatolásérzékelők, stb.) biztonsági szolgáltatásaival és architektúrális, telepítési modelljeivel. A megszerzett alapismereteket gyakorlati feladatok segítségével sajátítják el, mint például tűzfal szűrők és szabályok konfigurálása, továbbá IDS/IPS rendszerek beállítása és biztonsági tesztelése hálózati sérülékenység vizsgálati szoftverek segítségével. A tárgy részletesen kitér a vezeték nélküli (WLAN) hálózatok biztonságára, a tároló rendszerek biztonságára, a Cisco biztonsági és végpont-végpont VPN megoldásaira, valamint nyílt forrású technológiákra is (pl. pfSense).

Projektlabor 1,2,3

A gyakorlat célja a csapatmunka megismertetése egy önálló, komplex probléma megoldása kapcsán. A hallgatók önálló projektfeladatokat választanak, melyeket 2 fős csapatokba szerveződve oldják meg. Igen indokolt esetben a csapatlétszám lehet 1 vagy 3 fő. A feladatok kidolgozása során, a gyakorlatokon konzultálva ismertetik az elért részeredményeket, illetve a feltárt problémákat. Az elvégzett munkáról és az elért eredményekről a szemeszter végén „minikonferencia” jelleggel számolnak be. Az előadások a hallgatótársak és az oktatók kérdéseire adott válaszokkal fejeződnek be. A sikeresen teljesített féléves feladatokat a hallgatók tovább fejleszthetik és szakdolgozatot készíthetnek belőle.

Intézményi informatikai biztonság

- Esettanulmányok bemutatása, elemzése biztonsági szempontból.
- Vállalati informatikai rendszerek biztonságának tervezése, eszközök konfigurálása, tesztelése.
- Hálózati topológia kialakítása, aktív elemek kiválasztása, biztonsági feladataik meghatározása, konfigurálása.
- Hálózati behatolás védelmi, sérülékenységet vizsgáló eszközök, tűzfalak topológiába illesztése, konfigurálása.
- A szerver és ügyfél operációs rendszerek biztonsági rendszerének installálása és konfigurálása.
- Vírusvédelmi rendszer installálása és központi felügyelete.
- Szolgáltatások biztonsága: Web, FTP, és levelező szerverek biztonsági rendszerének beállítása.
- Dokumentálás, és üzemeltetési terv készítése.

Hacker eszközök, technikák

Az interneten számos hacker eszköz könnyedén elérhető, melyeket a támadók felhasználhatnak rosszindulatú céljaik eléréséhez. A megfelelő védelem kialakításához, fenntartásához elengedhetetlen a védelem oldaláról is megismerni, megérteni ezeket az eszközöket, technikákat, működésüket. A tárgy célja a különféle támadási folyamatok megértésén keresztül megismertetni a hallgatókat ezen eszközök és technikák ellen végrehajtható védelmi lehetőségekkel.

IT auditálás

- Információbiztonság alapelvei. Az informatikai biztonság pillérei: szervezet, szabályozás, technika.
- A hazai és EU-s törvényi követelmények, a különféle iparági szabályozások, és az egyéb szabványok, ajánlások és legjobb gyakorlatok.
- A vállalati-, az informatikai stratégia, és a vállalat üzleti céljainak kapcsolata, biztonsági és informatikai biztonsági következményei. A stratégia és a kockázatkezelés kapcsolata.
- A vállalati informatikai biztonsági szabályzások hierarchiája.
- Az alkalmazói rendszerekkel kapcsolatos biztonsági követelmények az életciklusuk egyes szakaszaiban.
- A sérülékenységek lehetőségének csökkentése a fejlesztés során.
- Az üzletmenet-folytonosság, az informatikai üzletmenet-folytonosság és stratégiai, kockázatkezelési vonatkozásaik.
- Az adatminőség jelentősége és biztosítása.
- Az informatikai ellenőrzés követelményeinek és feladatainak általános áttekintése.
- Az ellenőrzési célok levezetése az intézményi stratégiából, és teljesítésük preventív, detektív és korrektív ellenőrzési intézkedésekkel.
- A vállalati informatikai rendszer infrastruktúrája biztonsági és ellenőrzési szemszögből, az informatikai rendszer auditálás szervezeti és irányítási szempontjai.
- A vállalati vagyon (információ és informatikai rendszer) védelmi és ellenőrzési vonatkozásai.