Óbudai Egyetem
Bánki Donát Gépész- és Biztonságtechnikai Mérnöki Kar

INFORMÁCIÓBIZTONSÁGI SZAKMÉRNÖK/SZAKEMBER
szakirányú továbbképzés

Budapest, 2017.

I. A szakindítási kérelem indoklása

Magyarországon napról-napra, szinte robbanásszerűen nő az igény az információbiztonság és az információbiztonsági rendszerek használata iránt. A vállalatoknál már elképzelhetetlen az üzleti folyamatok működtetése különböző informatikai rendszerek és infokommunikációs eszközök támogatásai nélkül. A vállalatoknak alapvető érdekük folyamataik megbízható működését garantálni, ami megköveteli a támogató informatika folyamatos rendelkezésre állását, megbízható és biztonságos üzemeltetését. Az internet és az infokommunikáció fejlődésével a vállalatok nyitottsága az internet irányában is jelentősen megnőtt, ami romahosan megnövelte a kiberbűnözés veszélyeinek való kitettséget. Ezek azok a fő indokok, amelyek miatt az információbiztonság általánosan egy kiemelt kulcskérdéssé vált és válik a gazdaság minden ágazatának szereplői körében. Kiemelt jelentősége van mind a versenyszférában, ahol egyre több multi és cégcsoport vezeti be és tanúsíttatja az átfogó információbiztonsági irányítási rendszerét, és követeli ezt meg a beszállítóitól és alvállalkozóitól is. Az állami szférában az információbiztonsági követelményeket külön jogszabályok írják elő kötelezően, amelyek nemcsak a legtöbb állami szférába tartozó intézményre (kiemelten beleértve a kritikus infrastruktúrákat üzemeltető létesítményeket is) vonatkoznak, hanem azok fontosabb beszállítóira, azok informatikai rendszereinek fejlesztőire és üzemeltetőire is.

A továbbképzés célja ezért az, hogy az információbiztonságról és annak alkalmazásáról magas szintű, korszerű elméleti és gyakorlati ismereteket nyújtson a gazdaság minden ágazatában azoknak a szakembereknek, akik a korábban megszerzett szakképzettségük és felsőfokú szakismeretük birtokában képesek a szakterületükön belül felmerülő problémák megoldására, és ezen új ismeretekkel képesek legyenek ezt az információbiztonság különböző területein felmerülő problémákra is kiterjeszteni.

A szakirányú továbbképzés a fentiekből következően ***Információbiztonsági szakmérnök/ szakember*** szakon indul.

A szak tanterve és a tantárgyi programok leírása

1. Tanterv

	Kredit	Óraszám	Követelmény
I. félév			
Információbiztonság alapjai	8	28	Vizsga
Adatvédelmi és információbiztonsági jogszabályok	8	28	Vizsga
Vállalati informatikai rendszerek	3	12	Évközi jegy
IT hálózati alapismeretek	4	16	Évközi jegy
ITIL alapismeretek	5	20	Évközi jegy
Üzletmenet folytonosság, katasztrófahelyzetek kezelése	2	8	Aláírás
I. félév összesen	**30**	**112**	
II. félév			
Vállalati irányítási rendszerek ismeretek	8	28	Évközi jegy

	Kredit	Óraszám	Követelmény
Információbiztonsági / IBIR releváns szabványok	4	16	Évközi jegy
Információbiztonsági kockázatmenedzsment	3	12	Évközi jegy
Fizikai védelem / vagyonvédelmi rendszerek és módszerek	8	28	Évközi jegy
Humán biztonság és iratok és hagyományos adathordozók biztonsága	5	20	Évközi jegy
Szoftverfejlesztési életciklus és módszerek	2	8	Aláírás
II. félév összesen	**30**	**112**	
III. félév			
Az információbiztonság kiépítése, szabályozása	9	36	Vizsga
IT rendszerek üzemeltetésének fizikai biztonsági követelményei	4	12	Évközi jegy
IT rendszerek üzemeltetésének logikai biztonsági követelményei	9	36	Vizsga
IT hálózatbiztonság	6	20	Évközi jegy
Információs rendszerek biztonsági követelményei	2	8	Aláírás
III. félév összesen	**30**	**112**	
IV. félév			
IBIR auditálása	9	36	Vizsga
Felhasználói információbiztonsági szabályok	2	12	Évközi jegy
Szoftverfejlesztés IB követelményei, aspektusai	2	12	Aláírás
Sebezhetőségi és törés-vizsgálatok	7	36	Évközi jegy
Záró-dolgozati projekt	10	16	
IV. félév összesen	**30**	**112**	

Képzési forma:
Szakirányú továbbképzés.

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

Képzés helye:
Óbudai Egyetem, Bánki Donát Gépész- és Biztonságtechnikai Mérnöki Kar,
1081 Budapest, Népszínház utca 8.

Képzési idő:
4 félév, összesen 448 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 (150.000 Ft/félév)

Megszerezhető végzettség:
Eredményes záróvizsga esetén hallgatóink oklevelet kapnak: **Információbiztonsági szakmérnök/szakember** megnevezéssel.

Megszerzendő 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 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:
- Az információbiztonság kiépítése, szabályozása;
- IT rendszerek üzemeltetésének logikai biztonsági követelményei;
- IBIR auditálása.

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

Információbiztonság alapjai

Áttekintés az információbiztonság, az információbiztonsági irányítási rendszer (IBIR) fogalmáról, területeiről, és ezeken keresztül magáról az információbiztonsági szakirányról:

- Információbiztonság fogalma, jelentősége, szerepe.
- az információbiztonság megvalósításának gyakorlati szakmai területei.
- Az IBIR fogalma, céljai, ...
- Az információbiztonság jogi követelményei.
- Az információbiztonsági vagyonleltár és kockázatmenedzsment témái és módszerei.
- A fizikai védelem (őrzés védelem, vagyonvédelem) feladatai.
- A humánbiztonság feladatai.
- A dokumentumbiztonság (papír és elektronikus iratok védelme) feladatai.
- Az informatikai biztonság területei és feladatai.
- A katasztrófahelyzetek IB-vonatkozású feladatai.
- Az információbiztonság megvalósításának gyakorlati szakmai területeinek kapcsolata az ISO/IEC 27001 szabvány struktúrájához.

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.).
- Személyes adatok kezelsének új, európai irányelvei, követelményei (GDPR)
- 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.

Vállalati informatikai rendszerek

- Az informatika alkalmazásának szintjei.
- Informatikai alkalmazások tipikus munkahelyi területei (irodai informatika; könyvelés és gazdasági tevékenységek, kontrolling, humánerőforrás menedzsment tevékenységek, tervezés, termelés, termelésirányítás, ügyfélkapcsolatok menedzselése, értékesítés, beszerzés, logisztika, stb. támogatása; CRM, ERP, MIS rendszerek).

- Folyamatok és projektek támogatási rendszerei, tevékenységek, dokumentumok és termékek nyomon követése, workflow rendszerek.
- Infokommunikációs új eszközök, lehetőségek. Felhő alapú szolgáltatások jellemzése és fajtái. Internet és közösségi médiák az üzleti életben.

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

ITIL alapismeretek

- Az ITIL fogalma, kialakulása, jellemzői.
- Az ITIL v2. folyamatstruktúrája.
- Az ITIL v3 folyamatstruktúrája.
- Az IT szolgáltatások jellemzése. Az IT szolgáltatásmenedzsment jellemzése.
- Az informatikai szolgáltatásmenedzsment életciklusa.
- Az IT szolgáltatások üzemeltetése. (Célok, feladatok és tevékenységek.)
- Az IT szolgáltatások bevezetése. (Célok, feladatok és tevékenységek.)
- Az IT szolgáltatások tervezése. (Célok, feladatok és tevékenységek.)
- Az IT szolgáltatási stratégia. (Célok, feladatok és tevékenységek.)
- Állandó szolgáltatásfejlesztés. (Célok, feladatok és tevékenységek.)

Üzletmenet folytonosság, katasztrófahelyzetek kezelése

- Természeti / társadalmi katasztrófahelyzetek – jelentősége a vállalatok számára (példák). Ezek információbiztonsági vonatkozásai. IT rendszerek részleges vagy teljes működésképtelenné válása.
- Információbiztonság folytonossága a BCP/DRP alatt
- Üzleti BCP/DRP fogalma, célja, általános alapelve.
- IT BCP/DRP működésének életciklusa, fázisai, lépései. IT BCP/DRP készítésének lépései.
- IT BCP/DRP készítése – üzleti megközelítés, folyamatalapú.
- IT BCP/DRP készítése – IT megközelítés, IT szolgáltatás alapú. Szükséges redundanciák fogalma, módszerei.

Vállalati irányítási rendszerek ismeretek

- A vállalati irányítási rendszer jelentése és fogalma, és kapcsolódó fogalmak.
- Áttekintés az ISO tanúsítható irányítási rendszerekről (MIR, KIR, IBIR, MEBIR, EIR, ...).
- A tanúsítható irányítási rendszerek egységes struktúrája (HLS).
- Az integrált irányítási rendszer fogalma, és a közös elemek.
- Az ISO 9001 struktúrája, felépítése és követelményei.
- Az általános (minden szervezetre használható) irányítási rendszerek különbségei az ISO 9001 szerinti minőségirányítási rendszerhez.

Információbiztonsági / IBIR releváns szabványok

- Információbiztonság irányításával kapcsolatos szabványok: ISO/IEC 27000-es szabványcsoport fontosabb szabványainak áttekintése. Cobit 5 áttekintése. NIST releváns szabványok.
- Termékekre vonatkozó IT biztonsági követelmény-szabványok: Common Criteria – IT termékek biztonsági követelményeinek szintjei, struktúrája, elvárások és tanúsítások. Szoftverek minőségjellemzői, és közülük a security-re vonatkozó követelmények (ISO/IEC 9126-1,2,3,4 illetve ISO/IEC 25000-es csoport)
- Különböző IT biztonsági eljárásokra, részterületekre vonatkozó (ISO/IEC …) követelményszabványok áttekintése. (pl. incidenskezelés, üzletmenet folytonosság, hálózatbiztonság, kiberbiztonság, stb.)

Információbiztonsági kockázatmenedzsment

- Kockázatmenedzsment általános fogalma, alapelve, életciklusa és módszerei.
- Kockázatmenedzsment tárgya, célja az információbiztonságban.
- Kockázatelemzési módszerek és használatuk (alapvető, informális, részletes, kombinált, …).
- CRAMM módszer alapelve.
- Védendő adatvagyon fogalma, helye, kategorizálása.
- Védendő vagyonelemek fogalma, kategóriái, strukturálása.
- Adatvagyon és vagyonelemek osztályozása, követelmények, felelősségek.
- Skálázások módjai.
- Vagyonelemek sebezhetőségei és fenyegetései.
- Információbiztonsági kockázatok fajtái, felvétele, elemzése és értékelése.
- Kockázatok kezelésének módjai, és IB-gyakorlata.
- Kockázatok karbantartása, felügyelete, aktualizálása.

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

Humán biztonság és iratok és hagyományos adathordozók biztonsága

- A humán biztonság célja, feladatai az információbiztonságban.
- Az ember, mint adathordozó védelme – miért kell védeni, milyen veszélyek ellen, hogyan…
- A humán tényező, mint a leggyengébb biztonsági láncszem. A humán tényezőre visszavezethető jellemző fenyegetések.
- A "social engineering" (SE) fogalma, jellemzése, veszélyei.

- Az SE jellemző technikái, módszerei. Védekezési módok, lehetőségek az SE ellen. Tudatosítás, képzés (mit, hogyan, …).
- Humánbiztonsági eljárások munkatársak felvételekor. Humánbiztonsági eljárások munkaviszony alatt. Humánbiztonsági eljárások munkaviszony megszűnésekor és utána.
- Iratok biztonsági osztályba sorolása. Biztonsági osztályokhoz tartozó biztonsági követelmények kialakítása.
- Titkos ügyirat-kezelési (TÜK) alapok
- Iratok életciklusa. Papíralapú iratok, dokumentumok, adatok kezelésének elvárásai – az életciklus során, különböző esetekben, előfordulási helyeken.
- Irattárazás követelményei, irattárak (dokumentumtárak) műszaki, biztonsági, szervezési, szabályozási követelményei, alkalmazott módszerek.
- Iratok selejtezésének biztonsági követelményei, módszerei
- Elektronikus iratkezelés követelményei. Átjárás elektronikus és papíralapú iratok között, erre vonatkozó biztonsági követelmények.

Szoftverfejlesztési életciklus és módszerek

- A szoftverfejlesztési projekt életciklusa, fázisai és feladatai.
- A szoftverfejlesztés ellenőrzései (review és teszt).
- A konfiguráció-menedzsment (CM) jelentése és követelményei.
- Szoftverfejlesztési módszertanok: Vízesés modell, V-Modell, Scrum, CMMI.
- A Scrum és a Vízesés modell módszertanok összehasonlítása, rövid áttekintése.
- A követelménykezelés jelentősége, lépései. (Meghatározások, funkcionális és nem funkcionális követelmények. Biztonsági követelmények.)
- A tesztelés fázisai, lépései, problémái. (Speciális biztonsági szempontú követelmények.)

Az információbiztonság kiépítése, szabályozása

- Vállalat működtetésének, irányításának részei, szervezete, szabályozó rendszere.
- IBIR-rel szembeni külső és belső elvárásoknak való megfelelés.
- IBIR – Információbiztonsági irányítási rendszer részei, működésének keretei.
- IBIR működtetés témái, helye a vállalat folyamatszabályozásában.
- IBIR működtetés területei, folyamatai.
- IBIR működtetés miatti elvárások felhasználóktól (munkatársak, bedolgozók).
- IBIR működtetés miatti elvárások külső felektől – IB követelmények a szerződésekben.
- IBIR működtetés feladatai, irányítása és szervezete.
- IBIR működtetés szabályozása, dokumentumai.
- IBIR működtetés ellenőrzési mechanizmusai, mérése, hatékonyság figyelése.
- IBIR kialakításának, szabályozásának lehetőségei - példák, gyakorlatok: különböző vállalati méretekben, kultúrában, különböző ágazati szektorokban (versenyszféra, ipari, tervezés, ipari termelés, IT szolgáltatások, pénzügyi szektor, állami szektor, kritikus infrastruktúrák üzemeltetői, stb.).

IT rendszerek üzemeltetésének fizikai biztonsági követelményei

- IT eszközök, berendezésének fizikai biztonságának területei, céljai.
- IT eszközök, berendezések biztonságos elhelyezésének kritériumai, szempontjai.
- IT eszközök, berendezések biztonságos és megbízható üzemeltetési körülményeinek biztosítása: áramellátás stabilitása, megfelelő klimatizálás, kábelezés biztonsága, közművek üzemének biztonsága, stb.
- IT eszközök és berendezések megfelelő és biztonságos karbantartása.
- IT eszközök és berendezések selejtezésének biztonsági aspektusai

- IT eszközök és berendezések telephelyen kívül.
- Munkavégzés különleges helyeken: biztonsági területeken, rakodási / szállítási területeken, külső helyszíneken (ügyfélnél, vásáron, nyilvános területeken, otthon, …).
- Felhasználók eszközeinek biztonsága a munkavégzés helyszínén, őrizetlenül hagyott eszközök és adathordozók kérdése, „clear desk policy”.

IT rendszerek üzemeltetésének logikai biztonsági követelményei

- Üzemeltetési rendszeres és ad-hoc feladatok – szerver-üzemeltetés, hálózat üzemeltetése, alkalmazás és DB üzemeltetése és desktop-üzemeltetés.
- Konfiguráció-kezelés, kapacitás-kezelés, változás-kezelés.
- Kérés-, esemény-kezelés. Incidens- és problémamenedzsment.
- Telepítések rendje, jogosultságai, lehetőségei – biztonsági aspektusok, lehetséges módok.
- Üzemelő szoftverek felügyelete, biztonsága, frissítések és azok biztonsága.
- Mentések és archiválások módszerei, eszközei, technikái.
- Vírusvédelem (és kártékony kódoktól védelem) technikái.
- Éles-, teszt- és fejlesztői környezetek elkülönítése.
- Mobil eszközök és adathordozók szabályozása, biztonságos használata.
- Céges vs. magán-tulajdonú eszközök használata – céges vs. magán-célú használatának engedélyezése, kezelése, módok a megengedhető használat mellett a biztonságra.
- Monitoring, naplózás és naplóelemzés (mit, hogyan, milyen sűrűn, mentések hol, kiértékelések hogyan, …).
- IT audit esetén biztonság megtartása.
- Titkosítás alapjai: A kriptográfia matematikai alapjai. A napjainkban használt szimmetrikus kódoló algoritmusok működése. Aszimmetrikus kódolás menete. Hibrid titkosítás, HTTPS, tanúsítványkezelés.
- Titkosítás használata és eszközei: Merevlemez, partíció, könyvtárstruktúra illetve fájl titkosítási módszerei és eszközei. Alkalmazásokba épített titkosítások módszerei, erőssége.
- Hálózati kommunikáció titkosítása, eszközei.
- Digitális aláírás.
- Titkosításkor kulcsok tárolása, kezelése, eszközei. Jelszavak biztonságos tárolása, kezelése, eszközei.
- Gyakorlati szempontok - titkosítási igény vs. alkalmazott technika erősségének összhangjára
- Hozzáférések szabályozása, központi (üzleti, vezetői) elvárások rendje, kialakításhoz szükséges, ajánlott irányelvek, szempontok. Hozzáférési szabályok kialakításának elvei – hálózatokhoz, alkalmazásokhoz, rendszerekhez.
- Hozzáférési jogosultságmenedzselő eszközök, rendszerek, illetve adatok hozzáférését menedzselő rendszerek (pl. IRM), adatlopás elleni védelmi rendszerek (pl. DLP).
- Hozzáférések szabályainak beállítása, megvalósítása.
- Felhasználók regisztrációja, ill. törlése, jogainak beállítása. Felhasználói jogok módosításának, nyilvántartásának lehetőségei, alapelvei. Kiemelt felhasználói jogok korlátozása, kontrollja.
- Felhasználók authentikálási módszerei, hitelesítési (titkos) információk kezelési módjai.
- Felhasználói hozzáférési jogok felülvizsgálati módszerei, jogosultsági audit.
- Felhasználói hozzáférések használata, kontrolljának lehetőségei, módszerei.

Információs rendszerek biztonsági követelményei

- Információs rendszerek működtetése biztonsági követelményei, elvárásai, szempontjai.

- IB szempontok figyelembe vétele új rendszerek tervezésekor, régi felújításakor, információs rendszerek beszerzésekor, információs rendszerek beüzemelésekor, információs rendszerek üzemeltetésekor, információs rendszerek fejlesztésekor, módosításakor.
- Internetes szolgáltatások nyújtásának biztonsági szempontjai, védelmének eszközei.
- Internetes szolgáltatások adatainak biztonsági szempontjai, védelmének eszközei.

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.

IBIR auditálása

- Az audit fogalma, csoportosítása, auditok fajtái.
- Az auditok lefolytatásának követelményei (ISO 19011).
- Az információbiztonsági tanúsító szervezetek követelményei (ISO 17011, ISO/IEC 27006).
- Az auditálás folyamata, lépései, szerepei és dokumentumai.
- Auditori viselkedés, kommunikációs technikák.
- Az ISO/IEC 27001 szabvány követelménystruktúrája.
- Az IBIR területeinek követelményei auditori szemmel, hogyan auditáljuk azokat?
- Szituációs játékok

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.

Szoftverfejlesztés IB követelményei, aspektusai

- A szoftverfejlesztői csapatban tudatosság, humán biztonság betartása.
- A szoftver-fejlesztés életciklusa során biztonsági szempontok, fejlesztő eszközök biztonsága.

- Változáskövetés és verziókövetés betartása, biztonsága a fejlesztés és karbantartás alatt. Mindenféle változások esetén biztonsági tulajdonságok megtartásának ellenőrzése. Szabályozott és biztonságos kiadási folyamat, felelősségi kérdések is.
- Jogosultságok, biztonsági funkcionalitások a termékben, specifikációban.
- Webes adatbázisok felépítése, elméleti alapok, normalizáció.
- Adatok védelmi lehetőségei. (SQL injection, helytelen típuskezelés kihasználása. Keyloggerek típusai, Cross Site Scripting. Stb.)
- Kódolási konvenciók figyelemmel a kódban a sebezhetőségek, törési lehetőségek elkerülésére. (Fogalom: biztonságos kód).
- Biztonsági tesztelés, tesztadatok biztonsága.

Sebezhetőségi és törés-vizsgálatok

- Az etikus hackelés elve, módszerei – áttekintése.
- Az etikus hackelés jogi kérdései, aspektusai.
- Az etikus hackelés területeinek, módszereinek áttekintése
- Támadási teszt környezet kialakítása.
- Hardening.
- A sérülékenység vizsgálat eszközei – tool-ok és támogató eszközök.
- Külső sérülékenység vizsgálati módszerek.
- Belső sérülékenység vizsgálati módszerek.
- Web sérülékenység vizsgálati módszerek.
- WiFi sérülékenység vizsgálatok áttekintése.
- Mobil kommunikációs sérülékenység vizsgálatok áttekintése.
- A „kihasználás” módszerei. Social Engineering technikák, a Social Engineering eredményének felhasználása.
- Incidenskezelés tesztelése.

Záró-dolgozati projekt

A témaválasztás megbeszélése. A hipotézis megfogalmazása, adatgyűjtési technikák. Az adatfelvétel és feldolgozás módszerei. A dolgozat szerkezete, főbb részei. Cím, bevezetés, befejezés. Tézismondat. A bekezdés tulajdonságai. Az ellenőrzés. A hatásos fogalmazás és a mondat ereje. Folyamatelemzési módszerek. Érveléstechnika.