06135013 számú Szoftverbiztonsági szakember megnevezésű

szakképesítés megszerzésére irányuló szakmai képzéseket megalapozó programkövetelmény

1. A programkövetelmény, illetve az ennek alapján szervezhető szakmai képzés

1.1 Megnevezése: Szoftverbiztonsági szakember

1.2 Ágazat megnevezése: Informatika és távközlés

1.3 Besorolása a képzési területek egységes osztályozási rendszere (KEOR) szerinti kód alapján: 0613 Szoftverek és alkalmazások fejlesztése és elemzése

2. A programkövetelmény alapján szervezhető szakmai képzéssel megszerezhető szakképesítés

2.1 Megnevezése: Szoftverbiztonsági szakember

2.2 Szintjének besorolása

2.2.1 Az Európai Képesítési Keretrendszer (EKKR) szerint: 5

2.2.2 A Magyar Képesítési Keretrendszer (MKKR) szerint: 5

2.2.3 A Digitális Kompetencia Keretrendszer szerint: 8

3. A programkövetelmény alapján szervezhető szakmai képzéssel megszerezhető szakképesítés és az azzal betölthető munkakör vagy végezhető tevékenység kapcsolata, összefüggése[1]:

3.1 A szakmai képzéshez kapcsolódóan megszerezhető szakképesítéshez szükséges kompetenciákkal szakmajegyzékben szereplő szakma körébe vonható munkaterület, tevékenység vagy munkakör magasabb szinten gyakorolható, vagy a szakmai képzés szakmajegyzékben szereplő szakma képzési és kimeneti követelményeiben meg nem határozott speciális szakmai ismeretek és szakmai készségek megszerzésére irányul.

3.2 A szakmai képzéshez kapcsolódóan megszerezhető szakképesítés jogszabályban meghatározott képesítési követelmény munkakör betöltéséhez vagy tevékenység folytatásához.

A képesítési követelményt előíró jogszabály:

4. A programkövetelmény alapján szervezhető szakmai képzéshez kapcsolódóan megszerezhető szakképesítéssel ellátható legjellemzőbb munkaterület, tevékenység vagy munkakör leírása:

Az Szoftverbiztonsági szakember olyan szakember, aki ismeri a biztonságos kód fogalmát és alkalmazza az általa használt programozási nyelvek biztonsági funkcióit. Tisztában van az információbiztonság alapelveivel, elsajátítja a biztonságtudatos gondolkodást.

[1] A megfelelő elem kiválasztandó.

Az általa készített kódok, asztali és mobil alkalmazások, valamint a weboldalak biztonságossá tételéhez megfelelő technológiákat alkalmaz. Ismeri a leggyakrabban használt web-es biztonsági ellenőrző szoftvereket. Képes komplett szoftverrendszerre sérülékenységi teszteket végezni, valamint azokat kiértékelni.
Tesztelési terv készítésekor külön figyelmet fordít a biztonsági teszteknek. Az alkalmazás kódban megfelelő minőségű, mennyiségű és szintű logolást alkalmaz.
Mások kódjában észreveszi az alapvető biztonsági hibákat, képes érvelni a megfelelő biztonsági eszközök mellett, és alternatívákat mutatni a nem biztonságos kódokra.
Az új technológiák alkalmazására nyitott, tudását folyamatosan fejleszti.

5. A programkövetelmény alapján szervezhető szakmai képzéssel megszerezhető szakképesítéshez szükséges képzési tartalom szabadalmi vagy szerzői jogi oltalom alatti állása:

5.1 Szabadalmi vagy szerzői jogi oltalom alatt áll:

5.1.1 Az oltalom típusának megjelölése:

5.1.2 Nyilvántartó hatóság:

5.1.3 Azonosító vagy nyilvántartásba vételi száma:

6. A programkövetelmény alapján szervezhető szakmai képzés megkezdéséhez szükséges bemeneti feltételek:

6.1 Iskolai előképzettség[2]:

- érettségi végzettség

6.2 Szakmai előképzettség: -

6.3 Egészségügyi alkalmassági követelmény: -

6.4 Szakmai gyakorlat területe és időtartama: -

6.5 Egyéb feltételek:

A képzésben résztvevőnek az alábbi tudással és gyakorlati készségekkel kell rendelkeznie a képzés kezdetekor:

- alapszintű tudással rendelkezik a hálózati ismeretek terén
  - forgalomirányítási alapokkal rendelkezik
  - ismeri a statikus forgalomirányítást
  - ismeri a IPv4-es és IPv6-os címzést
  - alapszintű hálózatbiztonsági ismeretekkel rendelkezik
  - ismeri a HTTP protokoll részleteit (sütik, SSL)
- a hálózati operációs rendszerekkel kapcsolatban alapszintű tudással rendelkezik
  - Ismeri a virtualizációt és a konténereket
- alapszintű tudással rendelkezik a modern verziókezelő rendszerek használatával kapcsolatban

[2] A megfelelő elem kiválasztandó.

- magabiztos programozási alapismeretek legalább egy magasszintű programozási nyelven (pl. C#, Java, C++):
    - egyszerű és összetett adatszerkezetek
    - vezérlési szerkezetek
    - függvények és eljárások
    - egyszerű algoritmusok alkalmazása
    - kivétel kezelési alapismeretek
- magabiztos objektumorientált programozási ismeretek (OOP) és azok alkalmazása
- HTML5 alapismeretek és azok alkalmazása
- JavaScript alapismeretek és azok alkalmazása
- magabiztos tesztelési ismeretekkel rendelkezik a következő területeken
    - tesztek fogalma, tesztelés alapelvei
    - funkcionális és nemfunkcionális tesztek különbségeit ismeri
    - tesztjegyzőkönyvet vezet
    - unit tesztet készít

A fenti tudás és készségek ellenőrzése előzetes tudásfelméréssel történik, mely során a résztvevőnek az alábbi feladatot kell megoldania:

1. Egy tesztet kell kitöltenie, mely az alapszintű tudását és ismereteit méri.
2. Egyszerű programozási feladatot megvalósító konzolos alkalmazást kell létrehoznia a választott magas szintű programozási nyelven. A feladatnak mérnie kell az OOP ismereteket is, ennek megfelelően legalább egy osztálydefiníciót, illetve egy osztály példányosítását meg kell valósítania, és az osztályhoz unit teszteket készítenie.

Az előzetes tudásmérés alól mentesül, aki a (5 0613 12 03) Szoftverfejlesztő és tesztelő végzettséggel rendelkezik.

7. A programkövetelmény alapján szervezhető szakmai képzés elvégzéséhez szükséges foglalkozások minimális és maximális óraszáma (Amennyiben a programkövetelmény modulszerű felépítésű, a minimális óraszám a <u>modulonként</u> meghatározott minimális, a maximális óraszám a modulonként meghatározott maximális óraszámok összege):

7.1 Minimális óraszám: 400

7.2 Maximális óraszám: 550

8. A szakmai követelmények leírása:

8.1 Modulszerű felépítés esetén[3]

8.1.1 Programkövetelmény-modul neve: Általános információbiztonsági alapok

8.1.1.1 Programkövetelmény-modul sorszáma: 1.

[3] Legalább két modul esetén modulonként szükséges meghatározni a tanulási eredményeket! A sablont a modulok számának függvényében további táblázatokkal ki lehet egészíteni a modulra vonatkozó információk megjelenítésével.

8.1.1.2 Programkövetelmény-modul tanulási eredményeinek elsajátításához szükséges foglalkozások minimális és maximális óraszáma:

8.1.1.2.1 Minimális óraszám: 72
8.1.1.2.2 Maximális óraszám: 108

Készségek, képességek	**Ismeretek**	**Elvárt viselkedésmódok, attitűdök**	**Önállóság és felelősség mértéke**
Megfelelően használja az információbiztonság alapfogalmait.	Ismeri a biztonság általános informatikai és információbiztonsági definícióját, az információbiztonság három alappillérét.	Az egyes szituációkban képes felismerni, hogy a biztonság melyik alappillére sérül. Meg tudja határozni, hogy az adott intézkedés melyik alappillérre lesz hatással.	Felméri a tevékenységéből adódó kockázatokat, felelősséggel végzi a munkáját.
Eligazodik az információbiztonság jogszabályi környezetében, kapcsolódó szabványokban.	Ismeri az információbiztonságra vonatkozó hazai és nemzetközi jogszabályokat, szabványokat.	Képes különbséget tenni a jogszabályok és szabványok között. Figyelmet fordít rá, hogy tisztában legyen a releváns jogszabályok főbb tartalmi elemeivel.	Önállóan képes jogszabályi hivatkozásokat kezelni.
Ismeri a biztonságot támogató dokumentációk követelményeit, ezek tartalmi és formai elvárásait.	Ismeri a jogszabályok által elvárt információbiztonsági dokumentumokat, ezek főbb tartalmi elemeit.	Fontosnak tartja, hogy betartsa a dokumentációs elvárásokat napi munkavégzése során.	A rendelkezésére bocsátott sablon alapján képes azt releváns információkkal feltölteni.
Átlátja az információbiztonság főbb területeit.	Tisztában van az információbiztonsági irányítási rendszer működésével, főbb elemeivel és ezek szerepeivel.	Törekszik arra, hogy az információbiztonság minden területéről rendelkezzen átfogó ismeretekkel.	Önállóan képes az egyes területekhez kontrollokat megfogalmazni.

Elvégzi a sérülékenység vizsgálat eredményének kiértékelését..	Átfogó ismeretekkel rendelkezik a sérülékenység vizsgáló eszközök működéséről. Tisztában van a sérülékenység feltáró manuális és automata megoldások különbségével. Ismeri a leggyakoribb sérülékenység fajtákat és az ezekre adott válaszokat.	Magabiztosan értelmezi a sérülékenység vizsgálatok eredményét.	Önállóan azonosítja az illetékességi területéhez tartozó rendszer/alkalmazás tekintetében a legsúlyosabb sérülékenységet.
Képes önállóan elvégezni egy kisebb szervezet vagy egy komplex informatikai rendszer kockázatelemzését.	Ismeri a fenyegetések, sérülékenységek leggyakoribb fajtáit és tisztában van a kockázatkezelési eljárások típusaival. Ismeri a kockázati étvágy fogalmát és a kockázatok kezelésének módjait.	Törekszik arra, hogy egyes kockázatokra alternatív intézkedéseket is meg tudjon fogalmazni.	A lehetséges fenyegetések felmérése során képes megfelelő kockázatcsökkentő intézkedéseket javasolni.
Tisztában van a jogosultságkezelési rendszer szerepével, a kialakításkor alkalmazandó alapelvekkel.	Ismeri a jogosultsági rendszert, a hozzáférés azonosítás szerepét. Tisztában van a jogosultság kialakítás alapelveivel, az elemi jogosultságok és szerepkörök fogalmával.	Igyekszik az adott felhasználási területnek leginkább megfelelő jogosultsági rendszert kialakítani a biztonsági alapelvek maximális szem előtt tartása mellett.	Önállóan képes az összeférhetetlen szerepkörök felismerésére. Tisztában van a helytelen jogosultsági rendszerből adódó kockázatokkal.
Képes a megfelelő hitelesítő eszköz kiválasztására.	Ismeri a hitelesítés szerepét, a hitelesítő eszközök típusait, főbb jellemzőit.	Törekszik az adott alkalmazás/szolgáltatás/rendszer számára az ideális hitelesítési	Képes a felelősségi körébe tartozó információs rendszerben

	Tisztában van a többtényezős hitelesítés szerepével. Ismeri az elavult hitelesítési eszközök jelentette veszélyeket.	mód megtalálására. Nyitott a többtényezős hitelesítés alkalmazására.	biztonságos jelszó házirend kialakítására.

8.1.2 Programkövetelmény-modul neve: Biztonságos szoftverfejlesztés

8.1.2.1 Programkövetelmény-modul sorszáma: 2.

8.1.2.2 Programkövetelmény-modul tanulási eredményeinek elsajátításához szükséges foglalkozások minimális és maximális óraszáma:

8.1.2.2.1 Minimális óraszám: 328 óra
8.1.2.2.2 Maximális óraszám:442 óra

Készségek, képességek	**Ismeretek**	**Elvárt viselkedésmódok, attitűdök**	**Önállóság és felelősség mértéke**
Mások kódjában észrevesz alapvető biztonsági hibákat.	Ismeri a biztonságos kód fogalmát, ismeri a tanult nyelv biztonsági funkcióit. Ismeri az adott nyelv eszközeit az intervallum problémára, párhuzamos végrehajtásra. Régi (deprecated) könyvtárakra, függvényekre ismeri a modern alternatívákat.	Érvel a megfelelő biztonsági eszközök mellett, alternatívákat mutat fel nem biztonságos kódokra.	Saját kódjára értékelést kér, mások kódjára konstruktívan reagál.
	Ismeri a web alapvető biztonsági funkcióit.	Törekszik a saját weboldalának biztonságossá tételére a megfelelő technológiák alkalmazásával.	Nem használ "any bound" portokat.

	Ismeri a leggyakrabban használt web-es biztonsági ellenőrző szoftvereket.	Titkosított adatátvitelt használ, használja a tanított "best practive" eszközöket web-en.	Komplett webalkalmazásra sérülékenységi teszteket végez és értékel ki.
	Ismeri egy szoftverrendszer biztonsági korlátait, beleértve, hogy a biztonság növelése milyen használhatósági akadályokat okoz a szoftverrendszerben.	Tesztelési terv készítésekor külön figyelmet fordít a biztonsági teszteknek.	
	Ismeri a saját szoftverrendszerének bemeneti és kimeneti interfészeinek lehetséges sérülékenységeit. Ismeri a skálázhatóság fogalmát.	Az interfészét teszteli konstruktív és destruktív módokon. (Túlterhelés, DoS, DDoS, Fuzz)	Méri a rendelkezésreállást a saját szoftverrendszerén.
	Ismeri a sérülékenységek adatbázisait.	Meg tudja állapítani egy szoftverrendszerről, hogy az milyen ismert sérülékenységekkel rendelkezik, a sérülékenységi adatbázis alapján mitigációt javasol azok megoldására.	
Alkalmazás kódban megfelelő minőségű, mennyiségű, és szintű logolást alkalmaz. Biztonságosan, megfelelő	Ismeri a logok AAA lehetőségeit, szintjeit, és a logolás erőforrás használatát.	Logokat megfelelő keretrendszerrel használ, az érzékeny adatokat szűri belőlük. Logok törlésére nem ad lehetőséget. A	

redundanciával tárol adatokat.		logokat több helyre replikálja, azokról biztonsági mentést készít.	
Képes biztonságos 3PP, FOSS komponenseket használni a szoftverrendszeréhez.	Ismeri a 3PP, FOSS fogalmakat. Ismeri ezek biztonsági kockázatait.		
El tudja különíteni teszt és éles rendszeren végrehajtható műveleteket.	Ismeri a Hardening fogalmát.		Dokumentációt készít a saját szoftverrendszerének biztonságosabbá tételéhez. Ezt a dokumentumot teszteli.

8.2 A szakmai képzés megszervezhető kizárólag távoktatásban: igen/nem[4]

9. A programkövetelmény alapján szervezhető szakmai képzéssel megszerezhető szakképesítés társadalmi-gazdasági hasznosíthatóságának bemutatása (munkaerő-piaci relevanciája):

A szoftverfejlesztés területén számos olyan alkalmazástípus van, ahol kiemelten fontos biztonságos kód készítése, az alkalmazások külső támadások elleni védelme, a támadások következményeinek csökkentése, az adatok védelme, helyreállíthatósága. Az Szoftverbiztonsági szakember képzésben résztvevők olyan ismereteket és gyakorlati tudást szereznek meg, mellyel egyaránt képesek asztali, mobil, valamint web alkalmazások sérülékenységét vizsgálni, a szoftverrendszer biztonsági korlátait felismerni, az alapvető biztonsági hibák kiküszöbölésére javaslatot tenni, és a kódot a biztonságosság érdekében megfelelően javítani. A képzés a szoftverfejlesztő és –tesztelő technikus képzés által megszerzett tudást egészíti ki kibervédelmi ismeretekkel, de a képzés nyitva áll azok számára is, akik hasonló szintű programozási ismereteket önállóan vagy más képzések során szereztek meg.

10. A képesítő vizsga megszervezéséhez szükséges feltételek és a képesítő vizsga vizsgatevékenységeinek részletes leírása:

10.1 A képesítő vizsgára bocsátás feltétele:

[4] A megfelelő válasz aláhúzandó.

A szakmai képzés követelményeinek igazolásáról a képző intézmény által kiállított tanúsítvány.

Egyéb feltételek:

10.2 Írásbeli vizsga

10.2.1 A vizsgatevékenység megnevezése: Általános információbiztonsági alapok

10.2.2 A vizsgatevékenység, vagy részeinek leírása:

Az írásbeli vizsga kérdéseit a következők szerint kell összeállítani:

- Kérdések: 20 db feleletválasztásos tesztkérdés
- A feleletválasztós tesztkérdéseket úgy kell kialakítani, hogy egyetlen helyes válaszlehetőség legyen lehetséges
- A teszt témaköreit és az egyes témakörökhöz tartozó kérdésszámot az alábbi táblázat tartalmazza:

Témakör	Kérdések száma
Információbiztonsági alapfogalmak	3
Információbiztonsági jogszabályok, szabványok	3
Információbiztonsági dokumentációk	1
Információbiztonsági irányítási rendszer elemei, főbb feladatai	2
Sérülékenység-vizsgálat	3
Kockázatelemzés, kockázatkezelés	3
Jogosultságkezelés	2
Hitelesítés folyamata, hitelesítőeszközök használata, többtényezős hitelesítés, jelszó házirend szerepe, elemei	3
Összesen:	**20**

10.2.3 A vizsgatevékenység végrehajtására rendelkezésre álló időtartam: 30 perc

10.2.4 A vizsgatevékenység aránya a teljes képesítő vizsgán belül: 20%

10.2.5 A vizsgatevékenység értékelésének szempontjai:

Az írásbeli vizsgát a következők szerint kell értékelni:
Maximálisan elérhető pontszám/százalék: 40 pont / 100%

- 20 db tesztkérdés kibervédelmi ismeretekből (20*2 pont) 100%

Egyéb értékelési szempontok az írásbeli vizsgaértékeléssel kapcsolatban:

- A helyes válasz 2 pontot ér, a helytelen válasz 0 pontot ér.
- A rossz válasz megjelölésért pontlevonás nem jár.

10.2.6 A vizsgatevékenység akkor eredményes, ha a vizsgázó a megszerezhető összes pontszám legalább 51%-át elérte. Törtpontszámos eredmény esetén a kerekítés szabályait szükséges alkalmazni.

10.3 Projektfeladat

10.3.1 A vizsgatevékenység megnevezése: Alkalmazásoldali kibervédelmi projektfeladat

10.3.2 A vizsgatevékenység, vagy részeinek leírása:

A) Alkalmazásoldali kibervédelmi vizsgaremek vizsgarész

A vizsgarész egy előre elkészített gyakorlati feladat – vizsgaremek megvédéséből áll.
A vizsgázónak a vizsgát megelőzően egy asztali, mobil vagy webes alkalmazást kell elkészítenie, tesztekkel lefedve, konténerizálva. Az alkalmazással kapcsolatos elvárások:

- Valós életből vett igényeket elégítsen ki.
- Adattárolási és -kezelési funkciókat is megvalósít, megfelelő adatvédelmet biztosít.
- Legalább 1 biztonságkritikus funkció lefejlesztése, mely nem a bejelentkezéshez kapcsolódik.
- Az interfészei az AAA elveknek megfelelően készülnek, naplózzák a hozzáférést, és ezek biztonsági szempontból tesztelve vannak.
- A forráskódnak a tiszta kód elveinek megfelelően kell készülnie.
- A szoftver célját, komponenseinek technikai leírását, működésének műszaki feltételeit és használatának rövid bemutatását tartalmazó dokumentáció is része a csomagnak.
- Külön dokumentációt készít, mely ismerteti a szoftverrendszer biztonsági korlátait.

A projektfeladat benyújtásának módja

A kész csomagot a vizsga előtt minimum 14 nappal kell a vizsgaközponthoz benyújtani verziókövető rendszeren keresztül (pl. GitHub, GitLab, BitBucket stb.).
A vizsgafeladat során a vizsgázó gyakorlati bemutatóval összekapcsolt szóbeli előadás formájában mutatja be a

- szoftver célját
- műszaki megvalósítását
- működését
- forráskódját
- adatvédelmi funkcióit, tesztjeit
- a naplózás megvalósítását

Nem a vizsgázó szellemi terméke minden olyan – más szerzőtől átvett tartalom – amelynek forrását a vizsgázó nem jelzi egyértelműen.

A vizsgázó által bemutatott anyagot nem az ő szellemi termékének tekintjük, amennyiben az alábbi kritériumok közül legalább 2 teljesül:

- nem ismeri a bemutatásra kerülő anyag szerkezetét, felépítését
- nem tudja elmagyarázni az egyes modulok/komponensek szerepét
- a bemutatott anyagot korábban már publikálták, egészében vagy részben elérhető az interneten és nem az ő szellemi terméke

A projektfeladat bemutatására és megvédésére maximum 15 perc áll a vizsgázó rendelkezésére.

B) Egy kapott szoftver kibervédelmi vizsgálatának elvégzése
A vizsgafeladat során a vizsgázónak egy számítógépes szoftver kibervédelmi vizsgálatát kell elvégeznie. A vizsgálat során a vizsgázónak fel kell ismernie a sérülékenységi pontokat, meg kell neveznie a sérülékenység lehetséges következményeit, és javaslatot kell tennie a sérülékenység elhárítására.

10.3.3 A vizsgatevékenység végrehajtására rendelkezésre álló időtartam: 30 perc

Ezen belül:

A) Alkalmazásoldali kibervédelmi vizsgaremek vizsgarész: 15 perc
B) Egy kapott szoftver kibervédelmi vizsgálatának elvégzése: 15 perc

10.3.4 A vizsgatevékenység aránya a teljes képesítő vizsgán belül: 80%

10.3.5 A vizsgatevékenység értékelésének szempontjai:

A) Alkalmazásoldali kibervédelmi vizsgaremek vizsgarész:

- az alkalmazás konténerizált, a telepítési útmutató segítségével egyszerűen telepíthető és futtatható: 10 pont
- az alkalmazás átfogó értékelése biztonságosság szempontjából: 10 pont
- adatok kezelésének tervezése és megvalósítása, adatvédelem: 20 pont
- az interfészek megvalósítása, tesztelése, naplózás: 20 pont
- a kód minősége: 15 pont
- a dokumentációk minősége és részletezettsége: 15 pont
- az alkalmazás bemutatása során a vizsgázó előadásának szakszerűsége: 10 pont

B) Egy kapott szoftver kibervédelmi vizsgálatának elvégzése:

- sérülékenységi pontok vizsgálata, a tényleges sérülékenységek felismerése, megnevezése: 5 pont
- a sérülékenységek lehetséges következményeinek ismertetése: 10 pont
- javaslat a sérülékenység elhárítására: 10 pont

10.3.6 A vizsgatevékenység akkor eredményes, ha a vizsgázó minden vizsgarésznél a megszerezhető pontszám legalább 51%-át elérte. A vizsgarész eredménytelen, amennyiben a projektfeladat bemutatása közben kiderül, hogy a projektfeladat nem a vizsgázó szellemi terméke, ahhoz jelentős külső segítséget vett igénybe.

10.4 A vizsgatevékenységek lebonyolításához szükséges személyi feltételek:

A vizsga során 15 vizsgázónként legalább 1 rendszergazdának rendelkezésre kell állnia a vizsga során.

10.5 A vizsgatevékenységek lebonyolításához szükséges tárgyi feltételek:

- Számítógép / laptop
- A vizsgaremek védése során internetkapcsolat

10.6 A vizsgatevékenységek alóli felmentések speciális esetei, módja, és feltételei: -

10.7 A képesítő vizsgán használható segédeszközökre és egyéb dokumentumokra vonatkozó részletes szabályok:

- Papír és toll/ceruza használata megengedett.
- A vizsgaremek védése során a vizsgaközpont által ellenőrzött és jóváhagyott, a technikai feltételeknek megfelelő, saját számítógép használata engedélyezett.

10.8 A vizsgatevékenységek megszervezésére, azok vizsgaidőpontjaira, a vizsgaidőszakokra vonatkozó sajátos feltételek: -