NEMZETI KÖZSZOLGÁLATI EGYETEM

Katonai Műszaki Doktori Iskola

Dr. Debrecenine Deák Veronika

Közszolgálati kibervédelmi képességek képzésének lehetőségei

Doktori (PhD) értekezéstervezet

Témavezető:

Krasznay Csaba, PhD

……..

Budapest, 2022

TARTALOMJEGYZÉK

BEVEZETÉS

A kiberbiztonság egy gyorsan változó, fejlődő, illetve bővülő terület, amely napról napra újabb kihívásokat, veszélyeket tartogat számunkra, köszönhetően annak, hogy rohamosan változó világunkban a technológiai fejlődés soha nem látott méreteket ölt. A különféle infokommunikációs technológiák mai modern társadalmunk nélkülözhetetlen alkotóelemét képezik. Ennek következményeként a közszolgálatban is megfigyelhető ezen eszközök, technológiák alkalmazásának térhódítása.

Azonban ezek mindennapos használata és az egyre növekvő függőség számos kockázatot rejthet magában. A megfelelő szintű és minőségű kiberbiztonság megteremtése komplex feladatként jelentkezik, továbbá kritikus jelentőségűnek tekinthető az állami és a magánszféra működőképességének megteremtésében és folyamatos biztosításában egyaránt. A kibertámadások számának folyamatos növekedése és a támadások újabb eszközeinek, alternatíváinak megjelenése új típusú kihívásokat eredményeznek, valamint további védelmi mechanizmusok kialakítását és folyamatos fejlesztését teszi szükségessé. A kihívásokra és fenyegetésekre történő azonnali reagálás hatalmas terhet ró a szervezetekre. A közszolgálat és a különféle kritikus és kritikus információs infrastruktúrák a társadalom mindennapi működésének nélkülözhetetlen feltételeként értelmezhetők, ezért szükséges az ezek alapját képező információs rendszerek megbízható és biztonságos működésének folyamatos biztosítása.

Az elmúlt évek tapasztalatai alapján elmondható, hogy a közszolgálat kiemelt célpontja a kibertámadásoknak, a közszolgálati szervezetek ellen elkövetett kibertámadások mára mindennapossá váltak. A támadások elsősorban belső és bizalmas információk megszerzésére, illetve a különféle szolgálatatások működésének korlátozására irányulnak. Ezért a szervezet egészét – a rendszer legkisebb elemétől kezdve, az információs rendszereken át, egészen az ott dolgozókig – fel kell készíteni egy esetleg támadás megelőzésére, illetve a már bekövetkezett eseményekre való reagálásra. A közszolgálatban is létfontosságú a kibervédelem folyamatos fejlesztése, a kibervédelmi képesség és a kiberbiztonság erősítése, amely megvalósításának alapvető elemei a kiberbiztonsági képzések, oktatások és gyakorlatok kidolgozása és lebonyolítása. A támadások jelentős része a felhasználók felkészületlenségét és

biztonságtudatosságának hiányát célozza, éppen ezért az elsődleges cél a közszolgálatban dolgozók tudatosságának, kibervédelmi képességeinek kialakítása és folyamatos fejlesztése, amely eléréséhez elengedhetetlen egy olyan képzési forma megalkotása, amely segítségével e célok megvalósíthatók.

TUDOMÁNYOS PROBLÉMA MEGFOGALMAZÁSA

A tudományos probléma alapjául szolgál, hogy **globális szinten kiberbiztonsági munkaerőhiány jelentkezik**. A Nemzetközi Információs Rendszer Biztonsági Tanúsító Konzorciuma (The International Information System Security Certification Consortium Inc. – ISC) 2021-es felmérése szerint a kiberbiztonsági munkaerőhiány csökkent ugyan (3,12 millióról 2,71 millió kiberbiztonsági szakemberre), azonban még így is komoly hiányosságokat eredményez. Az ISC szerint a globális kiberbiztonsági munkaerőnek 65%-kal kell növekednie ahhoz, hogy képesek legyen hatékonyan megvédeni a szervezetek kritikus rendszereit, eszközeit. A kutatás rámutat arra, hogy a munkaerőhiány leküzdésének egyik legfontosabb eszköze a munkatársak szakmai képzése. [1] A munkaerőhiány kezelését és a közszolgálatban dolgozók kiberbiztonsággal kapcsolatos tudatosságát, képességeinek fejlesztését célozza egy olyan képzés kialakítása a közszolgálat számára, amely lehetővé teszi a szervezeti és személyi kiberbiztonság kialakítását és fejlesztését. Ennek megvalósítása elengedhetetlen, ugyanis **a megfelelő képzettségű szakemberek hiánya a közszolgálat, így az állam működésében jelentős korlátot, akadályokat eredményezhet.**

A kiberbiztonsági ismeretekkel felruházott munkaerő hiánya és ennek következtében a rendelkezésre álló emberi erőforrásra nehezedett többletfeladatok, illetve a nyomás számos negatív következményt eredményezhet. Ilyen valós káros hatások lehetnek többek között – a teljesség igénye nélkül - a kibertámadások felismerésének hiánya, figyelmen kívül hagyása, belső szabályozók be nem tartása, figyelmetlenségből és túlterheltségből fakadó rosszul konfigurált információs rendszerek, a lassabb javításokkal, frissítésekkel összefüggő feladatellátás, hiányos kockázatértékelés, az ellenőrzési vagy akár a felügyeleti szerepkör nem szakszerű ellátása. **A nem megfelelő feladatvégrehajtás számos kiberbiztonsági és működésbeli kockázatot eredményez.**

A tudományos probléma további elemeként értelmezhető, hogy a jelenlegi hazai helyzet alapján számos olyan a kibertámadási és -védelmi képesség kialakítását szolgáló képzés létezik, amelyek alapfeltétele, bemeneti követelménye valamilyen informatikai alapképzettség megléte, viszont **azok számára, akik nem rendelkeznek sem matematikai, sem pedig informatikai képzettséggel, nem biztosított a jelenleg rendelkezésre álló képzések abszolválása.** Éppen ezért szükséges egy olyan képzési program megalkotása, amely lehetőséget nyújt a közszolgálatban dolgozó, nem informatikai végzettségű személyek kibervédelmi képességének kialakítására. Ezen képesség alatt a személyes kibertámadási és kibervédelmi jártasságok, készségek, képességek összessége érthető, amely képesség elsajátításának célja, hogy azok, akik nem rendelkeznek a szükséges alapismeretekkel, nem mozognak a témában otthonosan, megfelelő felkészítést kapjanak a hatékony és eredményes védelem kialakítása, a különféle kiberfenyegetések megelőzése, illetve a már bekövetkezett események eredményes elhárítása érdekében. Ezen személyek a közszolgálatban dolgoznak, nap mint nap részt vesznek a döntéshozatalban, így elengedhetetlen a kibervédelmi képességük kialakítása, mert ennek köszönhetően nem csak a komplex védelem kialakítása valósulhat meg, de képesek lesznek a kibervédelemmel kapcsolatos stratégiai döntések megalapozott meghozatalára is.

KUTATÁSI CÉLKITŰZÉSEK ÉS HIPOTÉZISEK

Kutatásom célja, hogy egy olyan, a közszolgálati kiberbiztonság fejlesztését célzó képzést definiáljak, amely integrálható a közszolgálati képzési rendszerbe és amely elméleti, illetve gyakorlati ismeretek elsajátításával teszi lehetővé a kibertérből érkező fenyegetések elleni védekezés hatékony és eredményes megvalósítását, így az állami működés akadálytalan, korlátozástól mentes biztosítását.

KUTATÁSI CÉLOK

Figyelemmel az előzőekben ismertetett tudományos problémára és fő célkitűzésre, kutatásom céljai és az azokhoz tartozó részcélok az alábbiakban kerülnek bemutatásra.

Jelen értekezés alapjául szolgáló kutatás célja egy **tudományos alapokon nyugvó felsőoktatási képzések tervezésének lépéseit tartalmazó folyamatmodell definiálása**. Célom azonosítani az olyan egyértelmű feladatokat, lépéseket, amelyek

szükségesek egy képzés definiálásához úgy, hogy a képzés akadémiai szempontból is megalapozott relevanciával bírjon, továbbá bizonyítottnak minősüljön.

A közszolgálati kiberbiztonsági képzés szükségességének vizsgálatához és megalkotásához elengedhetetlen **a megfelelő szintű kiberbiztonság megvalósításához szükséges tudás- és képességhalmaz meghatározása, valamint a képzés célcsoportjának azonosítása**. Ennek keretében szükséges megvizsgálni a közszolgálaton belül a konkrét célcsoportot, valamint azt, hogy melyek azok az általános kiberbiztonsági feladatok, amelyeket a közszolgálati dolgozóknak szükséges végrehajtaniuk akár a mindennapi munkájuk során, akár egy esetleges kibertámadás esetén. Ezt követően határozható csak meg a szükséges és elégséges tudás-, illetve ismerethalmaz, amelyet a célcsoportnak szükséges elsajátítania.

A kutatás további célja **annak feltárása, hogy jelenleg hazánkban, illetve nemzetközi szinten rendelkezésre áll-e a közszolgálat fejlesztését célzó, kibervédelmi képesség kialakítására és fejlesztésére irányuló gyakorlati képzési program. Ennek keretében célom a kibervédelmi képesség nemzetközi és hazai képzéseinek feltérképezése, összehasonlítása, a hazai és nemzetközi „jó gyakorlatok" azonosítása**. Ennek oka, hogy a kapcsolódó képzések és az esetleges hiányosságok feltárásával igazolható a közszolgálati kiberbiztonsági képzés szükségessége. Emellett az összehasonlító elemzés segítségével számos jó gyakorlat azonosítható, amelyeknek hazai képzésbe történő átültetése jelentősen hozzájárulhat a nemzetközi szinten is elismert képzés definiálásához.

Kutatásom célja a definiált tudás- és ismerethalmaz felhasználásával **a közszolgálati kibervédelmi képesség képzési programjának definiálása**. Ennek keretében szükséges a képzés formális specifikálása, alapvető elemeinek, céljának, valamint bemeneti és kimeneti követelményeinek meghatározása. Mindemellett jelen kutatás további célja feltárni, hogy a védelmi szektor egy speciális területén, az Önkéntes Tartalékos Rendszerben felhasználható-e a közszolgálati kiberbiztonsági képzés. Ennek érdekében szükséges megvizsgálni, hogy milyen további, az önkéntes tartalékos állomány szerepéből és jogállásából fakadó speciális jellemzőkön alapuló elemekkel szükséges bővíteni a korábban meghatározott, elsajátítandó tudás- és ismerethalmazt a képzés felhasználásához.

A képzés definiálását követően szükséges **meghatározni a képzési célok támogatásához szükséges műszaki keretrendszert, valamint annak gyakorlati megvalósulásának lehetőségeit**. E cél során arra a kérdésre keresem a választ, hogyan lehet elsajátítani a kibervédelmi képességeket, illetve hogyan lehet átadni a szükséges tudást, a különféle védelmi stratégiákat, technikákat olyan személyek részére, akik nem rendelkeznek informatikai előképzettséggel. A cél az, hogy olyan szakembereket képezzünk, akik gyakorlati ismeretekkel rendelkeznek. Ennek köszönhetően a kutatás részcélja egy olyan környezet kialakítása, amelyen keresztül a képzés résztvevői ismert kibertámadási technikákkal szembesülhetnek és egy szimulált, valós környezetben kipróbálhatják a képzés során megismert védelmi mechanizmusokat.

HIPOTÉZISEK

Kutatómunkám kezdetén a tudományos probléma megfogalmazását követően a következő hipotéziseket állítottam fel.

- H1. Egy felsőoktatási kiberbiztonsági képzés definiálható tudományos alapokon.
- H2. Azonosítható a közszolgálati kiberbiztonság megvalósításához szükséges célcsoport és az általuk elsajátítandó tudáshalmaz.
- H3. Vélelmezem, hogy korábban még nem született a közszolgálat fejlesztését célzó, kibervédelmi képesség kialakítására és fejlesztésére irányuló gyakorlati képzési program.
- H4. Definiálható egy olyan, a közszolgálati kiberbiztonság fejlesztését célzó képzési program, amelynek teljesítése nem igényel informatikai előképzettséget.
- H5. Definiálható egy olyan kiberbiztonsági tudatosság növelését célzó műszaki keretrendszer, amely lehetőséget biztosít a kibertámadások elleni védelmi mechanizmusok gyakorlatban történő alkalmazására.

KUTATÁSMÓDSZERTAN

A fentebb említett hipotézisek bizonyítására felhasznált kutatási módszereket a következőkben ismertetem.

Kutatásom során kvantitatív és kvalitatív kutatási módszereket is igénybe vettem. A kutatási téma inter- és multidiszciplináris jellegéből fakadóan megköveteli a kapcsolódó tudományterületek teljeskörű vizsgálatát. A kitűzött célok

megvalósításához részt vettem a kiberbiztonsággal, információ- és informatikai biztonsággal, valamint az adatvédelemmel kapcsolatos tudományos rendezvényeken, konferenciákon, gyakorlatokon, majd ezt követően feldolgoztam, elemeztem és értékeltem az ott szerzett tapasztalatokat, ismereteket. Emellett folyamatosan nyomon követtem a kiberbiztonsággal, információ- és informatikai biztonsággal, valamint adatvédelemmel kapcsolatos aktualitásokat, fejleményeket a releváns szakfolyóiratok tanulmányozásával, valamint a hírközlési célú médiumokon keresztül, továbbá elemeztem, feldolgoztam és értékeltem a közelmúlt jelentős kibertámadások elleni védekezési eseményeit, tapasztalatait. Megvizsgáltam és elemeztem a jelenleg már elkészített, felhalmozott releváns oktatási anyagokat, segédanyagokat, elkészült doktori (PhD) disszertációkat, valamint a kiberbiztonsági szabályozás tárgyában kiadott nemzetközi, európai uniós és hazai szabályzókat, jogi szervezetszabályozó eszközöket, szabványokat, ajánlásokat és módszertani útmutatókat. Az összegyűjtött hazai és nemzetközi szakirodalmat analitikus módszerrel, majd a rendszerezést követően szintetizálással dolgoztam fel. A szakirodalom feldolgozása során az indukció és a dedukció módszerét is alkalmaztam.

Tudományos munkám során az általános és a különös kutatási módszereket egyaránt alkalmaztam. Az általános módszerek közül a megfigyelést és az összehasonlító módszert használtam fel a nemzetközi tapasztalatok vizsgálata során a külföldi példák hazai alkalmazásának vizsgálata, az esetleges hiányosságok feltárása és a „jó gyakorlatok” azonosítása érdekében. A megfigyelési módszerek közül a közvetlen és közvetett megfigyelést is alkalmaztam a különböző támadási alternatívák alkalmazási lehetőségeinek és korlátainak vizsgálatakor.

Kutatásom során konzultációt folytattam hazai és nemzetközi gyakorlati tapasztalattal rendelkező szakértőkkel, valamint interjút készítettem a „jó gyakorlatok”, tapasztalatok képzésbe történő implementálásához, a képzés valós igényeknek megfelelő definiálásához. Mindemellett a kutatás alapjául szolgáló képzés résztvevőihez hasonló érintetti kör vonatkozásában fókuszcsoportos beszélgetés során gyűjtöttem véleményeket, tapasztalatokat és érzéseket a gyakorlati oktatás szerepéről.

Kutatásom részeredményeit folyamatosan publikáltam, illetve számos tudományos és szakmai konferencián, rendezvényen, fórumon ismertettem a tájékoztatás, a szakmai, gondolkodás elősegítése és a kapcsolódó reakciók feltárása céljából.

ÉRTEKEZÉS SZERKEZETE ÉS JELÖLÉSRENDSZERE

A kitűzött célok megvalósítása, kutatásom és az elért tudományos eredmények bemutatása érdekében értekezésem az alábbi szerkezet szerint épül fel.

Az 1. fejezetben bemutatom azokat a lépéseket, elemeket, amelyek szükségesek egy tudományos alapokon nyugvó képzés kialakításához. Ennek keretében azonosítom és rendszerezem e sarkalatos pontokat, illetve lépéseket egy nyolcelemű folyamatmodell definiálásával, továbbá bemutatom azon kutatási módszereket, amelyek szükségesek egy képzés megalkotásához.

A 2. fejezetben egy interjún keresztül mutatom be a köz-és magánszférában megvalósuló kiberbiztonság közötti különbségeket, majd ez alapján azonosítom a kibertér aktuális kihívásait, a képzés célcsoportját. illetve meghatározom azokat a képességeket, készségeket és ismereteket, amelyeket a kijelölt célcsoport számára át kell adni.

Ezt követően a 3. fejezetben kerül sor a hazai és nemzetközi kiberbiztonsággal összefüggő felsőoktatási képzések azonosítására és összehasonlítására. A képzési program megalkotása során fel kell tárni a program megvalósíthatóságának lehetőségeit, valamint a hasonló hazai és nemzetközi képzéseket, ezen belül azok tartalmát, elemeit annak érdekében, hogy igazolható legyen a képzés létjogosultsága, továbbá, hogy feltárhassam az esetleges hiányosságokat, azok orvoslása, valamint az alkalmazott „jó gyakorlatokat”, azok hazai képzési rendszerbe történő átültetése érdekében. Jelen fejezetben a releváns képzések összehasonlító elemzésére kerül sor az átadott tudásanyag alapján.

Az 4. fejezetben ismertetem a közszolgálati kiberbiztonsági képzés alapvető fogalmainak, elemeinek definícióját, értelmezését, valamint a bemeneti és kimeneti követelményeit. Emellett rögzítem a képzés struktúráját és az elsajátítandó tudás egyes témaköreit. E fejezetben ismertetem az önkéntes tartalékos állomány jogállását, valamint a kibervédelmi feladatok ellátásában betöltött jelenlegi és jövőbeli szerepét. Ezenkívül a közszolgálati kiberbiztonsági képzés Önkéntes Tartalékos Rendszerben történő alkalmazásának lehetőségére teszek javaslatot, a képzés alap tartalmának kibővítésével. A fejezetben bemutatásra kerül a képzés folyamatos fejlesztésének biztosítása céljából a tudásátadás hatékonyságának mérésére szolgáló

szempontrendszer és mérési módszer, amely segítségével megvalósítható a képzés egyes tárgyainak iteratív fejlesztése.

Az 5. fejezetben kerül sor a kétlépcsős gyakorlati képzés működési környezetének meghatározására. A fejezetben bemutatom az általam definiált keretrendszert, amely képes támogatást nyújtani a képzés során az egyéni infokommunikációs eszközök védelmének megismeréséhez, illetve a szervezeti szintű védelmi mechanizmusok használatához. Ennek keretében azonosítom a gyakorlati képzés alapját képező szimulációs környezetet leíró keretrendszert.

Minden fejezet elején ismertetem a kutatás vonatkozó hipotézisét és alhipotéziseit, a felhasznált kutatásmódszertant, valamint a kapcsolódó szakirodalmi áttekintést. Ezt követően bemutatom a hipotézis igazolására szolgáló részkutatást, amelynek tartalmát a fejezet végén összegzem és részkövetkeztetéseket vonok le, valamint azonosítom a fejezet segítségével elért új tudományos eredményeket.

Jelen értekezésben lábjegyzetben jelölöm a saját megjegyzéseimet, kiegészítéseimet, valamint magyarázataimat. A felhasznált irodalom a törzsszövegben sorszámozott hivatkozással, valamint a disszertáció végén, külön fejezetben található irodalomjegyzékben került megjelölésre. A félkövér formázással ellátott szövegrészek az értelmezést segítő, kiemelten fontos szövegrészeket, míg a dőlt szövegrészek a szó szerinti idézéseket jelölik. Az disszertációban található ábrák és táblázatok saját szerkesztésűek, kivéve amennyiben a forrás egyértelműen fel van tüntetve.

Értekezésemet egyes szám első és harmadik személyben írom, amely tükrözi az általam végzett kutatómunkát, azonban azon fejezet (4.6 fejezet) esetében, ahol az elért eredmény közös kutatómunka eredménye, ott a kontribúció többesszám első személyben jelenik meg, reprezentálva az eredmények megosztását a társszerzővel, illetve a fejezet végén egyértelműen meghatározom, hogy mi tekinthető az általam elvégzett kutatómunkának.

1. KÖZSZOLGÁLATI KIBERBIZTONSÁGI KÉPZÉS TERVEZÉSE TUDOMÁNYOS ALAPOKON

1.1. BEVEZETÉS

A kibertámadások jelentős gazdasági, politikai, nemzetbiztonsági, de a társadalomra is kiterjedő káros következményt idézhetnek elő. Az elmúlt évek eseményei alapján megállapítható, hogy a közszolgálat kiemelt célpontja a kibertámadásoknak, így különösen nagy hangsúlyt kell fektetni a lehetséges támadási és védekezési alternatívák megismerésére és alkalmazhatóságának vizsgálatára a hatékony védelem kialakítása érdekében. A közszolgálat fejlesztéséhez a különféle infrastruktúrák védettségének teszteléséhez szükség van a védelmi képesség képzési lehetőségeinek meghatározására a kockázatok és sebezhetőségek feltárása érdekében. Ezek alapján elengedhetetlen a közszolgálatban dolgozók szakmai képzése, így egy olyan képzés megalkotása, amely lehetővé teszi a lehetséges támadási és védekezési stratégiák alkalmazhatóságának megismertetését és ezáltal a kibertérből érkező fenyegetések megelőzését, elhárítását, valamint a már bekövetkezett eseményekre történő hatékony és eredményes reagálást.

Ahhoz, hogy egy ilyen komplex képzés kidolgozása megvalósulhasson, fontos definiálni, hogy melyek azok a lépések és elemek, amelyek szükségesek egy tudományos alapokon nyugvó képzés kialakításához. Jelen fejezetben (lásd 1-1. ábra) azonosítom és rendszerezem ezen sarkalatos pontokat, lépéseket, továbbá bemutatom azon kutatási módszereket, amelyek szükségesek a képzés tudományos alapokon történő meghatározásához. Az így definiált folyamatmodellt használom fel a közszolgálati kiberbiztonsági képzés megalkotása során.

1-1. ábra A képzéstervezés folyamatának magasszintű leírása

1.1.1. HIPOTÉZISEK

A vizsgált hipotézis szerint **egy kiberbiztonsági felsőoktatási képzés definiálható tudományos alapokon (H1)**. A hipotézis szükségességét igazolja, hogy az előző fejezetben meghatározott, jelen értekezés alapjául szolgáló hipotézisek bizonyításához, valamint a közszolgálati kiberbiztonsági képzés definiálásához elengedhetetlen egy tudományos kutatási módszertanon alapuló képzéstervezési metódus meghatározása. Ennek segítségével egy olyan képzés alkotható meg, amely tudományos alapokon került meghatározásra, a hazai és nemzetközi tudományos közösség számára elismert képzésnek tekinthető, szükségessége bizonyításra került, valamint felhasználja az aktuálisan elérhető képzések „jó gyakorlatait", elért eredményeit és tapasztalatait.

A fentiek alapján jelen fejezet célja egy tudományos alapokon nyugvó kiberbiztonsági felsőoktatási képzések tervezésének lépéseit tartalmazó folyamatmodell definiálása, amelynek érdekében az alábbi alhipotéziseket azonosítottam, amelyek megválaszolását tűztem ki célul jelen fejezetben. Az alhipotézisek a következők:

H-1.1. Definiálható egy folyamatmodell, amely meghatározza a tudományos alapokon nyugvó kiberbiztonsági felsőoktatási képzés tervezésének lépéseit.

H-1.2. Azonosíthatóak azon kutatási módszerek, amelyek szükségesek a képzés tudományos alapokon történő meghatározására.

Az első alhipotézis célja megvizsgálni, hogy azonosíthatóak-e olyan egyértelmű feladatok, amelyek szükségesek egy kiberbiztonsági képzés definiálásához úgy, hogy a képzés akadémiai szempontból is megalapozott relevanciával bírjon. A második alhipotézis során azt kell megvizsgálni, hogy melyek azok a kutatási módszertanok, amelyeket egy kutatás során alkalmazni kell az egyes feladatok teljesítése esetén, hogy e feladatok megvalósítása akadémiai szempontból is bizonyítottnak minősüljön.

1.1.2. FELHASZNÁLT KUTATÁSMÓDSZERTAN

A fentebb említett hipotézisek megválaszolására a következőkben bemutatott módszerek kerültek felhasználásra.

Az alhipotézisek igazolására egy 8 elemű folyamatmodellt definiáltam, amelyek között egyértelmű sorrend állítható fel. Az egyes feladatokhoz azonosítottam a

releváns kutatási módszereket. A folyamatmodell helyességét, miszerint a modell segítségével előállított képzés akadémiai szempontból releváns azzal bizonyítom, hogy a jelen értekezés alapjául szolgáló közszolgálati kiberbiztonsági képzés a folyamatmodell lépéseinek megfelelően definiálom.

1.1.3. FEJEZET SZERKEZETE

Jelen fejezet a következő struktúrát követi. Az 1.2 fejezetben a témakörhöz kapcsolódó szakirodalmak kerülnek áttekintésre, míg az 1.3 fejezetben a tervezés során felhasználható kutatási módszerek fogalmi alapjainak ismertetése található. Az 1.4 fejezetben kerül bemutatásra a képzés tervezéséhez szükséges folyamatmodell, illetve a hozzá kapcsolódó feladatok és az azokat bizonyító kutatási módszerek. Az 1.5 fejezetben az összegzett következtetések, és az 1.6 fejezetben pedig az új tudományos részeredmények kerülnek rögzítésre.

1.2. KAPCSOLÓDÓ SZAKIRODALMI ÁTTEKINTÉS

Számos tudományos mű foglalkozik a tudományos kutatás elméleti, gyakorlati, illetve módszertani kérdéseivel. Hornyacsek Júlia *A tudományos kutatás elmélete és módszertana* című könyvében átfogó képet ad a tudományos kutatás gyakorlati alapjairól, módszereiről, valamint ezek elméleti kérdéseiről. Rögzíti a tudományos kutatás szakaszait, így a kutatási téma kiválasztását, az előzetes kutatást és tájékozódást, a kutatás átfogó tervezését, a kutatási terv elkészítését, a kutatás lefolytatását, a kutatás eredményeinek nyilvánossá tételét, továbbá ezen szakaszok feladatait is. Ezt követően bemutatja az adatgyűjtés módszerét, amely a tudományos kutatás kulcsfontosságú eleme. Kifejti a tudományos adatgyűjtés módszereit és bemutatja azokat. Ide sorolható a mérés, a megfigyelés, az elemzés, az esettanulmány, a kísérlet, a kérdezés, valamint a tesztelés. Ezután ismerteti a kérdőíves vizsgálat fogalmát, célját és fajtáit, valamint rávilágít annak folyamatára és esetleges hibáira. A szerző kitér a dokumentumokkal kapcsolatos főbb szabályokra, amelyek a másodlagos kutatási adatok forrásainak tekinthetők. [2]

Gőcze István *Tudományelmélet és kutatásmódszertan alapjai* című könyvében bemutatja a tudomány- és a kutatásmódszertan meghatározó kérdéseit, a tudományos tevékenység legfontosabb formáit. Ennek keretében rögzíti a tudomány- és kutatásmódszertan ismeretelméleti alapjait, a tudományos kutatás típusait, valamint

módszereit. A tudományos módszerek fajtáit és formáit három csoportba sorolja, amely alapján megkülönböztethetünk általános, különös és egyedi módszereket. Az általános módszerek az összes tudományra és annak bármely objektumára vonatkoznak. Ilyen például az összehasonlító módszer, amely segítségével feltárhatók a jelenségek egyetemes összefüggései. A különös módszerek valamennyi tudományban használatosak, de csak a kutatás tárgyának egyik oldalára, például jelenségre vagy mennyiségre vonatkoznak. Ide sorolhatók az empirikus kutatási módszerek, mint például a megfigyelés és a kísérlet, valamint az elméleti-logikai kutatási módszerek, mint például a hipotézis, az analógia, vagy akár a különféle matematikai módszerek. [3]

Carrie Williams tanulmányában három gyakori kutatási módszert mutat be, a kvalitatív, a kvantitatív és a vegyes módszereket. A könyv ezeket fogalmuk, tartalmuk és az adott csoportba sorolható kutatási módszerek segítségével mutatja be. A kvantitatív módszerek közé sorolja a leíró módszert, a korrelációs, fejlesztési, megfigyelési, tervezési tanulmányokat és a felmérés egyes típusait, amelyek összehasonlító és okozati vizsgálati kutatásokban hatékonyan alkalmazhatók. A kvalitatív módszerek közé sorolja az esettanulmányt, a megalapozott elméletet, a néprajzvizsgálatot és a tartalomelemzést. A szerző bemutatja, hogy mely esetben alkalmazhatók ezen módszerek és milyen előnyökkel rendelkeznek. [4]

Earl Babbie könyvében bemutatja a társadalomtudomány és a kutatás elméleti alapjait, majd részletesen elemzi a megismerési folyamatot, illetve annak felépítését. A szerző azonosítja a megfigyelés módjait, mely alapján megkülönböztethető a kísérlet, a kérdőíves vizsgálat, a terepkutatás, a beavatkozásmentes vizsgálat, valamint a hatásvizsgálat. [5]

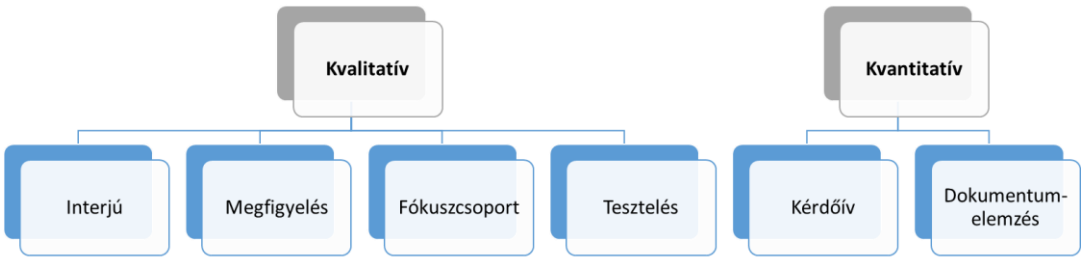
1.3. TERVEZÉS SORÁN FELHASZNÁLHATÓ KUTATÁSI MÓDSZERTANOK

Ahogyan az az 1.2 fejezetben is bemutatásra került a kutatási módszertanokat különbözőféleképpen lehet azonosítani, illetve csoportosítani. Jelen alfejezet célja az értekezés kutatásmódszertani fogalmi rendszerének meghatározása. A fogalmak meghatározása nem kontribúciója a disszertációnak, azonban fontos egyértelműsíteni az egyes fogalmak jelen értekezésben jelentett tartalmát.

A fogalmi rendszer meghatározása Hornyacsek Júlia *A tudományos kutatás elmélete és módszertana* [2] című művét veszi alapul, azonban jelen fejezetben csak az értekezés szempontjából releváns módszertanok kerülnek áttekintésre. Ez alapján az egyes módszereket típusokba sorolhatjuk, amely szerint egy módszer lehet kvalitatív vagy kvantitatív módszer:

- *kvalitatív módszerek*: a tudományterület minőségi mutatóinak vizsgálata.
- *kvantitatív módszerek*: a tudományterület mennyiségi mutatóinak vizsgálata.

Jelen fejezet szempontjából releváns kutatási módszereket az 1-2. ábra szemlélteti, meghatározásuk pedig az alábbiak:



1-2. ábra: Felhasznált kutatási módszerek csoportosítása

- *Interjú*: olyan kvalitatív módszer, amely során az interjúalany előre meghatározott kifejtős kérdésekre válaszol olyan témában, amelynek szakértője. A válaszai azonban nemcsak tárgyilagosak, hanem tartalmazzák az alany személyes véleményét is.
- *Dokumentumelemzés*: olyan kvantitatív módszer, amely során adott témához kapcsolódó dokumentumok részletes elemzése során juthatunk adatokhoz.
- *Tesztelés*: olyan kvalitatív módszer, amely során egy kontrollcsoport ellenőrzött körülmények között végez el meghatározott feladatokat, amelynek sikeressége alátámasztja a hipotézist.
- *Fókuszcsoport*: olyan kvalitatív módszer, amely során egy csoporttal folytatott beszélgetés alatt gyűjtünk véleményeket, érzéseket egy adott problématerülettel kapcsolatban.

- *Megfigyelés*: olyan kvalitatív módszer, amely során az információgyűjtéshez tapasztalati észrevételeket használunk.
- *Kérdőív*: olyan kvantitatív módszer, amely során a kitöltő eldöntendő, vagy feleletválasztós kérdésekre válaszol, ezáltal az eredmény mindig tárgyilagos marad, és statisztikai következtetések vonhatók le belőlük.

1.4. KIBERBIZTONSÁGI FELSŐOKTATÁSI KÉPZÉSEK TERVEZÉSÉNEK LÉPÉSEI

Egy kiberbiztonsági felsőoktatási képzés tervezése során feltételezhetjük, hogy a tervezés szükségessége már alátámasztott, vagyis akár a versenyszférából, akár a közszférából megjelent az igény egy képzésre, amely a főbb jellemzőket azonosítja (például magas szintű témakörök, irányvonalak).

A tervezési folyamatnak az 1-3. ábra olvasható szakaszait különíthetjük el élesen. Jelen alfejezet bemutatja ezen szakaszok tartalmát és ezzel párhuzamosan az alkalmazható kutatási módszereket.

1-3. ábra: Kiberbiztonsági felsőoktatási képzések tervezésének lépései

1.4.1. RELEVÁNS SZEREPLŐK MEGHALLGATÁSA

A folyamat első lépése a releváns szereplők meghallgatása, a képzés szükségességének, relevanciájának, valamint a pontos magán-, illetve közszférából érkező igény feltárása. E lépés elengedhetetlen a képzés megfelelő tervezéséhez, hiszen itt kerül sor a gyakorlati tapasztalattal rendelkező szakértők bevonására, meghallgatására. Ennek célja, hogy átfogó képet kaphassunk arról, hogy az adott szakterületen tapasztalattal rendelkező személyek indokoltnak gondolják-e a tervezett képzést és amennyiben igen, mit tartanak fontosnak, milyen főbb komponensek, tartalmi elemek szükségesek a képzés megvalósításához. A szakértői vélemények bevonása elengedhetetlen a jó gyakorlatok, tapasztalatok képzésbe történő implementálásához, a képzés valós igényeknek megfelelő definiálásához, valamint a képzés tervezésének későbbi szakaszában a képzés folyamatos fejlesztéséhez is. Az ilyen gyakorlati szakemberek segítségével könnyen feltárhatók a létrehozni kívánt képzés esetleges erősségei és gyengeségei, hiszen szakértelmüknek és jártasságuknak köszönhetően valódi tapasztalattal rendelkeznek, ismerik a releváns képzéseket, a tudományterület főbb irányvonalait és az aktuális kihívásokat.

Kapcsolódó kutatási módszerek: dokumentumelemzés, interjú

A releváns szereplők meghallgatásához elengedhetetlen kutatási módszer az interjú, illetve az interjúalanyok által publikált dokumentumok elemzése, továbbá e dokumentumokban hivatkozott publikációk elemzése. Az interjú kulcsfontosságú eszköz ahhoz, hogy a képzéshez kapcsolódóan szaktekintélyek véleményét hallgassuk meg, és ne csak egyetlen nézőpontot alkalmazzunk a képzés létrehozása során. Az itt kapcsolódó dokumentumok olyan információkat tartalmazhatnak, amely a képzés kialakításának fő irányvonalát befolyásolhatják, valamint kontextusát azonosíthatják.

1.4.2. CÉLCSOPORT MEGHATÁROZÁSA

Ahhoz, hogy a képzés minden elemére kiterjedő definiálása megvalósulhasson elengedhetetlen a célcsoport meghatározása. A célcsoport meghatározása során fontos azonosítani a korcsoportot, az előképzettséget és a szakmai tapasztalatot, hiszen így a célcsoportnak megfelelő tartalmú képzés hozható létre. Ennek segítségével az is meghatározható, hogy a képzés általános vagy az adott szakterületre jellemző ismeretekkel, problémákkal és kihívásokkal foglalkozik.

Kapcsolódó kutatási módszerek: dokumentumelemzés, interjú

A dokumentumelemzés jó kiindulópont a célcsoportok meghatározására, ahol a releváns jogszabályok áttekintését és az interjú módszerét is célszerű használni. Ez utóbbi esetben a témakörspecifikus tudással rendelkező interjúalanyok különböző nézőpontok alapján szűkíthetik vagy tágíthatják azon személyek halmazát, akik számára szükséges lehet a képzés.

1.4.3. AZ ÁTADNI KÍVÁNT KÉPESSÉGEK ÉS KÉSZSÉGEK MEGHATÁROZÁSA

A képzés felépítésének és tartalmának meghatározásához szükséges az átadni kívánt képességeket és készségeket definiálni. Ennek első lépése, hogy azonosítsuk azokat az általános feladatokat, amelyeket a célcsoport a mindennapi munkájuk során végrehajt. Ezt követően kerülhet sor a feladatok ellátásához szükséges tudáshalmaz, valamint az ennek elsajátítását követően megszerzett képességek és készségek definiálására. Természetesen a feladatok és az ismerethalmaz meghatározását nagyban befolyásolja, hogy az adott képzés célja általános vagy szakterületspecifikus ismeretek átadása.

Kapcsolódó kutatási módszerek: megfigyelés, dokumentumelemzés

A megfigyelés eszköze elengedhetetlen a képzések definiálása során, így a saját tapasztalatainkra hagyatkozva azonosíthatjuk a szükséges elemeket. A másik fontos kutatási módszer a dokumentumelemzés, amely során azt vizsgáljuk meg, hogy a szakirodalomban milyen igények jelentek meg a témakörben releváns képességekre és készségekre.

1.4.4. HAZAI KÉPZÉSEK VIZSGÁLATA

Egy képzés tervezésekor minden esetben meg kell vizsgálni az aktuális, nemzeti képzéseket, azok tartalmát és felépítését a képzésduplikáció elkerülése érdekében, hiszen amennyiben már létezik az általunk létrehozni kívánt képzéssel tartalmában azonos képzés, nem indokolt annak definiálása, megtervezése. Ehhez azokat a képzéseket kell megvizsgálni, amelyeknek célcsoportja azonos vagy annál tágabb és azt, hogy az átadott tudáshalmaz lefedi-e az előző lépésben meghatározott képességeket és készségeket. Ezen kívül a vizsgálat segítségével meghatározhatók az esetleges hiányosságok, jó gyakorlatok, valamint a vizsgált képzések felhasználásának lehetőségei.

Kapcsolódó kutatási módszerek: dokumentumelemzés

A hazai képzések vizsgálatához természetesen dokumentumelemzésre van szükség, hiszen át kell tekinteni az összes hazai képzést, amely a témához kapcsolódik. Erre jó kiindulópontot jelenthet a Felvi.hu [w7] weboldal, amely az összes felsőoktatási képzést tartalmazza. Ezek mellett a hazai akadémiai publikációkat is szükséges megvizsgálni, hiszen ebből kiderülhet, hogy van-e már tervben hasonló képzés kialakítása.

1.4.5. NEMZETKÖZI KÉPZÉSEK VIZSGÁLATA

A képzés kialakításához mindenképp szükséges feltérképezni és megvizsgálni a nemzetközi oktatásban megjelenő kiberbiztonsággal, információbiztonsággal kapcsolatos képzéseket. Ezen belül a képzések rendszerét, struktúráját, felépítését és tartalmát annak érdekében, hogy a nemzetközi tapasztalatok vizsgálata során feltárt „jó gyakorlatok” esetleges átültetése megvalósulhasson a nemzeti oktatásban. A nemzetközi képzések vizsgálata azért is indokolt, hiszen ennek segítségével megállapítható, hogy egy hazai képzés nemzetközi szinten is releváns képzésnek minősül-e, illetve, hogy a képzés során átadott tudás nemzetközi színtéren is értéket képvisel-e.

Kapcsolódó kutatási módszerek: dokumentumelemzés

A nemzetközi képzések vizsgálatához, hasonlóan, mint a hazai képzések vizsgálata esetén, dokumentumelemzésre van szükség, hiszen át kell tekinteni a releváns nemzetközi képzéseket, amelyek az adott témához kapcsolódnak. Erre jó kiindulópont lehet a TopUniversities.com [w2] weboldal, amely különféle csoportosítások szerint ad hozzáférést a nemzetközi képzésekhez. Ezek mellett az akadémiai publikációkat is érdemes megvizsgálni, hiszen ebből kiderülhet, milyen kihívásokkal küzdöttek meg mások hasonló képzések megalkotása során.

1.4.6. A KÉPZÉS FORMÁLIS SPECIFIKÁLÁSA

A képzés tervezésének következő lépése a formális specifikáció, amely segítségével meghatározhatók a bemeneti és kimeneti követelmények, vagyis hogy melyek azok a feltételek és korábbi tanulmányok, képzési kritériumok, amelyek elengedhetetlenek a képzésen való részvételhez, illetve melyek azok az ismeretek, amelyeket a képzés után a hallgató a magáénak tudhat majd.

Kapcsolódó kutatási módszerek: dokumentumelemzés

A képzés formális specifikációjához a releváns jogszabályokat szükséges áttekinteni, amelyek meghatározzák, hogy mit szükséges a definíció során kötelezően megállapítani. Ezen kívül célszerű a hasonló képzések definícióját, célkitűzéseit is megvizsgálni.

1.4.7. A KÉPZÉSI STRUKTÚRA ÉS TÉMAKÖRÖK MEGHATÁROZÁSA

A képzés struktúrájának és tartalmának meghatározása elengedhetetlen a képzés működése és a korábban meghatározott tudáshalmaz eredményes átadása szempontjából. E lépésben kerül sor a képzés felépítésének és tartalmának definiálására, amely segítségével azonosítható, hogy mely témakörök futhatnak például párhuzamosan, egymással azonos időtartam, félév alatt. A struktúra kialakítása során figyelembe kell venni az egyes témakörök, valamint gyakorlati részt tartalmazó képzés esetén az elméleti és gyakorlati oktatás sorrendiségét annak érdekében, hogy elkerüljük a témakörök közötti előreutalást, amely által a hallgatók számára olyan tudást adnánk át, amelynek alapjait majd csak későbbi félévekben sajátítanának el. Továbbá meg kell határozni a képzés tantárgyainak, valamint azok tantárgyi adatlapjainak alapjául szolgáló témaköröket.

Kapcsolódó kutatási módszerek: dokumentumelemzés, megfigyelés, fókuszcsoport, interjú

A struktúra és a témakörök meghatározása során lehetőség van több kutatási módszert is használni. A nemzetközi és hazai publikációk elemzése megfelelő támpontot adhat a kiinduláshoz, de fontosak a saját és mások tapasztalatain alapuló megközelítések is.

1.4.8. A KÉPZÉS FOLYAMATOS FEJLESZTÉSÉNEK BIZTOSÍTÁSA

Az utolsó lépés rendkívül fontos a kiberbiztonsági felsőoktatási képzés esetében, hiszen ennek segítségével biztosítható a képzés naprakészsége. Éppen ezért elengedhetetlen a képzés relevanciájának és tartalmának folyamatos monitorozása, illetve felülvizsgálata, valamint a képzés szakterületével, tudományterületével kapcsolatos aktuális és új kutatási eredmények, álláspontok, kihívások nyomon követése. A kialakított képzést fel kell készíteni a módosításokra, fejlesztésekre, amelyhez olyan metrikákat, kiértékelési mechanizmusokat kell definiálni, amellyel a képzés minősége mindenkor ellenőrizhető, és kiértékelhető. Az eredmények alapján

képesnek kell lenni megfogalmazni módosítási javaslatokat, hogy a képzés minőségét és színvonalát javítani lehessen.

Kapcsolódó kutatási módszerek: kérdőív, teszt, dokumentumelemzés

Az elkészült képzés indítására, fejlesztésére és minőségének biztosítására olyan kutatásmódszertani eszközöket lehet használni, mint a tesztelés, amely által még a képzés indulása előtt egy kontrollcsoport segítségével kiértékelhetők a tematikák, oktatási stratégiák, stb. A kérdőív pedig a már meglévő vagy a képzés indítása után indított kurzusokhoz lehet hasznos. Előbbi esetben segítséget nyújt, hogy egy kurzust milyen irányba kell alakítani, hogy alkalmas legyen a definiált képzéshez, míg utóbbi esetben már a képzés alkalmazása közben futó kurzusok fejlesztésére lehet következtetni a kérdőívek eredményeiből. Természetesen érdemes megnézni az akadémiai világot, hogy milyen megközelítések állnak rendelkezésre az adott témakörben a képzések fejlesztésére, amelyeket érdemes lehet még átültetni és átalakítani.

1.5. KÖVETKEZTETÉSEK

Az előző alfejezetek egyfajta előkészítései és egyben bizonyításai voltak a hipotézisek megválaszolásának. Jelen alfejezet célja, hogy a megadott hipotézisekre egyértelmű választ adjunk.

A H-1.1 alhipotézis esetén azzal a feltételezéssel éltem, hogy definiálható egy folyamatmodell, amely meghatározza a tudományos alapokon nyugvó kiberbiztonsági felsőoktatási képzés tervezésének lépéseit. Ennek érdekében egy nyolc elemből álló folyamatmodellt definiáltam, amely részletezi, miképpen lehet egy képzést tudományos alapokon meghatározni.

A H-1.2 alhipotézis alapján vélelmeztem, hogy azonosíthatóak azon kutatási módszerek, amelyek szükségesek a képzés tudományos alapokon történő meghatározására. Ennek bizonyítására meghatároztam a folyamatokhoz kapcsolódó releváns kutatási módszereket. A két alhipotézis eredményeit szemlélteti az 1-4. ábra. Ahogy az ábráról is leolvasható a dokumentumelemzés mindegyik fázisban elengedhetetlen eszköz. Az is látható, hogy a képzés tervezésének korai szakaszában jelentős szereppel bír az interjú eszköze, ahol a szakma releváns személyei irányíthatják a képzés fókuszát. A tervezés végén jelenik meg a lehetőség további

módszerek alkalmazására, így a kérdőívek alkalmazására, tesztelésre, megfigyelésre és a fókuszcsoportos interjú használatára.

A bemutatott folyamat és kutatási módszerek csak azon elemeket definiálják, amelyek egy képzés definiálásához kellenek. Minél specifikusabb a célterület az egyes folyamatrészeket érdemes tovább bontani és további kutatási módszertanokat is lehet használni, hogy elégséges alapot képezzen a képzés helyességének bizonyítására.

1-4. ábra: A tervezési lépések során alkalmazható kutatási eredmények

1.6. ÚJ TUDOMÁNYOS EREDMÉNYEK

Jelen fejezetben bemutatott kutatás alapján **bizonyítottam, hogy egy kiberbiztonsági felsőoktatási képzés definiálható tudományos alapokon (E1)**.

E tudományos eredmény igazolásához kutatásom során az alábbi részeredményeket értem el:

Tudományos részeredmény 1. Definiáltam egy folyamatmodellt, amely meghatározza a tudományos alapokon nyugvó kiberbiztonsági felsőoktatási képzések tervezésének lépéseit.

Tudományos részeredmény 2. Azonosítottam azon kutatási módszereket, amelyek szükségesek a képzés tudományos alapokon történő meghatározására.

Jelen fejezet a [k2] publikációra épül, amely részletesen támasztja alá mind az első, mind a második tudományos részeredményt. E folyóiratcikkben egy 8 lépcsős folyamatmodellt definiáltam. A folyamatmodell helyességét, alkalmazhatóságát és akadémiai relevanciáját azzal bizonyítottam, hogy az egyes lépések megoldását lehetséges tudományos kutatási módszerek bemutatásával és azok egy esettanulmányon történő alkalmazásával támasztottam alá. A publikációban bemutatott esettanulmány jelen képzés meghatározását tartalmazza.

2. CÉLCSOPORT, TUDÁS- ÉS KÉPESSÉGHALMAZ MEGHATÁROZÁSA

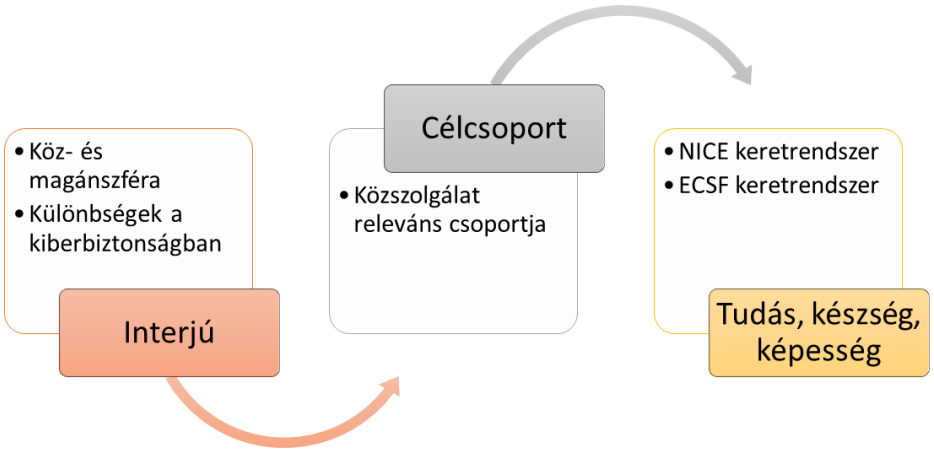
2.1. BEVEZETÉS

Mint minden terület esetén, úgy a közszolgálat vonatkozásában is igaz az, hogy a megfelelő szintű kiberbiztonság megteremtése érdekében a szervezet egészét, – a rendszer legkisebb elemétől kezdve, az információs rendszereken át, egészen az ott dolgozókig – fel kell készíteni egy esetleges kibertámadás megelőzésére, illetve a már bekövetkezett eseményekre történő hatékony reagálásra.

Jelen fejezetben egy interjún keresztül mutatom be a köz-és magánszférában megvalósuló kiberbiztonság közötti különbségeket, majd ezt követően azonosítom a képzés célcsoportját, illetve definiálom azokat a képességeket, készségeket és ismereteket, amelyeket a kijelölt célcsoport számára át kell adni. Mivel a képzésnek nemzetközi szinten is elfogadottnak kell lennie, emiatt érdemes egy olyan nemzetközi alapokon nyugvó keretrendszert megvizsgálni, amely segítséget nyújthat a tudáshalmaz definiálásához. Ennek következtében a NICE Cybersecurity Workforce Framework[1] (a továbbiakban: NICE Keretrendszer) [6] és az ENISA European Cybersecurity Skills Framework[2] (a továbbiakban: ECSF Keretrendszer) [7] által meghatározott, a kiberbiztonsághoz kapcsolódó munkaköröket elemeztem, illetve megvizsgáltam az e munkakörök betöltéséhez szükséges képességeket, készségeket, továbbá elsajátítandó ismeretköröket, majd ezeket alapul véve definiáltam a közszolgálati kiberbiztonsági képzés tudás- és képességhalmazát (lásd 2-1. ábra).

[1] A National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework az Egyesült Államok Kereskedelmi Minisztériumának Nemzeti Szabványügyi és Technológiai Intézete által kiadott tanulmány, amely a kiberbiztonsághoz kapcsolódó munkaköröket kategorizálja, valamint többek között kifejti és leírja a kiberbiztonsági munkakörök tartalmát és ezen munkakörök betöltéséhez szükséges képességeket, készségeket, továbbá elsajátítandó ismeretköröket.

[2] Az Európai Kiberbiztonsági Ügynökség (ENISA) 2022. áprilisában kiadott Európai Kiberbiztonsági Képességek Keretrendszere, amely tizenkét kiberbiztonsággal kapcsolatos munkakör vonatkozásában gyűjti össze az egyes munkakörök sajátosságait, az elvégzendő feladatokat, valamint az elsajátítandó kompetenciákat.



2-1. ábra A fejezetben vizsgált fő elemek

2.1.1. HIPOTÉZIS

Jelen fejezetben vizsgált hipotézis szerint **azonosítható a közszolgálati kiberbiztonság megvalósításához szükséges célcsoport és az általuk elsajátítandó tudáshalmaz (H2)**. Ennek igazolására az alábbi alhipotéziseket azonosítottam, amelyek vizsgálatára a következőkben kerül sor:

H-2.1. Létezik különbség a magánszektor és a közszolgálat között kiberbiztonság szempontjából.

H-2.2. Azonosítható egy célcsoport a közszolgálatban dolgozók köréből, akik számára szükséges lehet a közszolgálati kiberbiztonsági képzés

H-2.3. A közszolgálatban dolgozó személyek számára meghatározható a szervezeti kiberbiztonság megvalósításához szükséges tudás-, képesség-, és ismerethalmaz.

2.1.2. FELHASZNÁLT KUTATÁSMÓDSZERTAN

A H-2.1 alhipotézis esetén egy interjú keretében vizsgáltam a köz- és magánszféra közötti különbséget kiberbiztonsági szempontból. A H-2.2 alhipotézis igazolása során azonosítottam a közszolgálati kiberbiztonsági képzés célcsoportját az interjúból levont következtetések, valamint dokumentumelemzés útján a releváns szakirodalom feldolgozásával. Ennek keretében a közszolgálat fogalmának és komponenseinek vizsgálatával, dokumentumelemzés segítségével definiáltam a közszolgálati kiberbiztonsági képzés célcsoportjának egyes elemeit és kivételi körét. Ezt követően a H-2.3 alhipotézis bizonyítására meghatároztam a képzés során elsajátítandó

ismerethalmazt, amely tartalmazza a NICE, valamint az ECSF Keretrendszer által előírt tudás-, feladat-, készség-, képességhalmazt, valamint egyéb ismeretköröket egyaránt. Az egyéb tudáshalmazt a kapcsolódó szakirodalom, valamint saját oktatói tapasztalataim alapján azonosítottam.

2.1.3. FEJEZET SZERKEZETE

Jelen fejezet a következő struktúrát követi. A 2.2 alfejezetben a témakörhöz kapcsolódó hazai és nemzetközi szakirodalmak kerülnek áttekintésre, majd ezt követően a 2.3 alfejezetben bemutatom az általam készített interjút. A 2.4 alfejezetben azonosítom a jelen értekezés alapjául szolgáló közszolgálati kiberbiztonsági képzés célcsoportját, valamint a 2.5 alfejezetben definiálom a képzés során elsajátítandó tudás-, készség-, képesség- és ismerethalmazt. A 2.6 alfejezet tartalmazza a fejezet egészében bemutatott kutatásból levont következtetéseket, valamint az elért új tudományos eredményeket a 2.7 fejezetben tartalmazza.

2.2. KAPCSOLÓDÓ SZAKIRODALMI ÁTTEKINTÉS

2.2.1. INTERJÚKÉSZÍTÉS ALAPVETŐ SZABÁLYAI

Hornyacsek Júlia a *Tudományos kutatás elmélete és módszertana* című könyvében definiálta az interjúkészítés szabályait, szakaszait és a kérdések típusait. A szerző szerint az interjú az a kutatási módszer, amelynek segítségével az adott témával kapcsolatos adatokat egy másik személy kérdéseire adott válaszain keresztül ismerhetjük meg. Az így nyert adat szubjektív, amely tartalmazza az interjúalany értékítéletét, véleményét, amelyre nagy hatással van az adott személy tapasztalata, szakismerete. A szerző rögzíti az interjú típusait és szabályait. Ezek alapján a kérdezőnek a témáról és a megkérdezettről felkészültnek kell lennie, valamint fontos a szakzsargon kerülése, érthető, értelmezhető kérdések feltétele, illetve a megfelelő interjúalanyok kiválasztása. További szabály, hogy a megkérdezettnek ismernie kell az interjúkészítés okát, célját, valamint a kérdéskört, amiről az interjú szól. Ezen kívül rendkívül fontos a megfelelő helyszínválasztás és az időtartam meghatározása. Fontos szabály, hogy figyelni kell a megkérdezettek kulturális, szociális helyzetéből adódó érzékenységére, valamint minden esetben biztosítani kell az interjúalany

anonimitásának védelmét. A tanulmányban kifejtésre kerülnek az interjúkészítés végrehajtásának főbb szakaszai, feladatai. [2]

Dapzury Valenzuela és Pallavi Shrivastava az *Interjú alapú kvalitatív kutatás* című művükben kifejtik, hogy az interjú különösen hasznos kutatási módszernek tekinthető, hiszen segítségével az adott kérdéskört, témát a résztvevők tapasztalatain keresztül ismerhetjük meg, tárhatjuk fel, továbbá előnye a személyes jelenlét és a feltett kérdések bővítése a beszélgetés alakulása alapján. A szerzők rámutatnak a kérdező felkészültségének és képzettségének fontosságára, hogy minden lehetséges esetre képes legyen reagálni. Bemutatásra kerülnek az interjú típusai is: az informális, a beszélgetés alapú interjú, az általános interjú, a szabványosított, nyitott végű interjú, valamint a zárt rögzített válaszú interjú. Ezt követően a szerzők rámutatnak a felkészülés lépéseire, valamint azon kritériumokra, amelyek elengedhetetlenek az eredményes interjú végrehajtásához. Végül a szerzők rögzítik az interjú végrehajtásának szakaszait és az azt követő teendőket is. [8]

Barbara DiCicco-Bloom és Benjamin F. Grabtree *A kvalitatív kutató interjú* című cikkükben röviden áttekintik a leggyakrabban előforduló kvalitatív interjú módszereket: a strukturált interjúkat, a félig strukturált interjúkat, valamint az egyéni mélyinterjúkat. Megvitatják a mélyinterjúk lebonyolításának módszereit, és áttekintik a releváns etikai témájú kérdéseket, különös tekintettel a résztvevők jogaira és védelmére. Ezt követően ismertetik az interjúalany kiválasztásának szempontjait, az interjú lefolytatásának folyamatát, valamint az eredmények elemzésének lehetőségét. Végül a szerzők megvizsgálnak négy etikai kérdést az interjúkkal kapcsolatban, amelyek a következők: váratlan károk kockázatának csökkentése, az interjúalanyok adatainak védelme, az interjúalanyok hatékony tájékoztatása a tanulmány természetéről, valamint a kihasználás kockázatának csökkentése. [9]

Összegezve, az interjú különösen hasznos kutatási módszernek tekinthető, hiszen segítségével az adott kérdéskört, témát a résztvevők tapasztalatain keresztül ismerhetjük meg, tárhatjuk fel, továbbá előnye a személyes jelenlét és a feltett kérdések bővítése a beszélgetés folyamatos alakulása alapján.

2.2.2. KIBERBIZTONSÁG A MAGÁNSZFÉRÁBAN

A magánszféra kiberbiztonsági kérdéseit több tanulmány vizsgálta a döntési stratégiák, képzések és nemzetközi összehasonlítások mentén. Brent R. Rowe és

Michael P. Gallaher az *A magánszektor kiberbiztonsági befektetési stratégiái: Empirikus elemzés* című tanulmányukban egy esettanulmány keretében interjúsorozatot készítettek különféle ágazatokban működő szervezetekkel, annak érdekében, hogy feltárják és megértsék a befektetési és végrehajtási stratégiájukat, különös tekintettel azon tényezőkre, amelyek meghatározzák az általuk fenntartott kiberbiztonsági szintet. Az interjúk során felmerült általános témaként jelent meg, hogy sok szervezet átfogó elemzést készít a kiberbiztonságról, és sokan megkezdték vagy tervezik megkezdeni folyamataik átalakítását ennek megfelelően. Ezt követően fogalmi megközelítést ajánlanak a kiberbiztonsági beruházási döntés alkotóelemeinek, valamint a különféle beruházási és végrehajtási stratégiák közötti kompromisszumok leírására; továbbá empirikus bizonyítékot szolgáltatnak arról, hogy kapcsolat állhat fenn a szervezet külső nyilvános információk felhasználása, illetve a proaktív és reaktív stratégiák relatív keveréke között. [10]

Mikko T. Siponen és szerzőtársai a *Szervezeti információbiztonság-tudatosság elméleti alapjai* című cikkükben kihangsúlyozzák a biztonságtudatosság fontosságát és szerepét, amely szerint a tudatosság képes minimalizálni a felhasználókkal kapcsolatos sérülékenységeket. Ennek megvalósítására szisztematikus programokon keresztül van lehetőség. A szerzők szerint a tudatossággal kapcsolatos problémák megértéséhez és a képzésekhez két kategóriát szükséges kiemelni, a keretrendszert és a tartalmat. A szerzők ismertetik, hogy egy keretrendszert kell kidolgozni szisztematikus és strukturált módon a releváns szabványok, szakanyagok segítségével. Kiemelt figyelmet kell fordítani a felhasználói viselkedés befolyásolásának megközelítéseire, valamint a különféle meggyőzési stratégiákra. [11]

Lawrence A. Gordon és szerzőtársai a *Kiberbiztonsági beruházások növekedése a magáncégekben* című tanulmányukban egy mikroökonómiai elemzés segítségével mutatják be, hogy a kormányzati kezdeményezések és jogszabályok képesek-e növelni a kiberbiztonsági beruházásokat a magánkézben lévő cégek által. [12]

Hiller és Russell *A magánszektor kiberbiztonságának kihívása és szükségszerűsége: Nemzetközi összehasonlítás* című cikkükben áttekintik a különféle kiberfenyegetéseket és összehasonlítják az Egyesült Államok és az európai kiberbiztonság támogatására irányuló megközelítéseket. Ezt követően bemutatják, hogy ezen megközelítések, hogyan képesek befolyásolni a kiberbiztonsági kockázatokat, valamint egy keretrendszert javasolnak a kiberbiztonsági stratégiák és

jogszabályok hatásainak vizualizálásához. A szerzők megállapítják, hogy annak ellenére, hogy az Egyesült Államoknak és az Európai Uniónak közös kiberbiztonsági céljai és stratégiái vannak, az információmegosztás, valamint a köz-és magánszféra együttműködése eltérően valósul meg. Emellett a szerzők mindkét esetben megvizsgálták, hogy milyen jogi szabályozás áll rendelkezésükre a kiberbiztonság kialakításához és fejlesztéséhez. [13]

2.2.3. KIBERBIZTONSÁG A KÖZSZFÉRÁBAN

A közszféra és elsősorban a közigazgatás kiberbiztonságát számos tanulmány vizsgálta, mint globalizációs problémát, ahol az internet megjelenése olyan kihívásokat támasztott a közszolgálat számára, amelyekkel korábban még nem szembesültek.

Wirtz tanulmányában a közszféra alkalmazottainak a kiberbiztonsággal kapcsolatos hozzáállását, valamint azon intézkedéseket vizsgálja empirikus alapokon, amelyeket a bizalmas kormányzati adatok biztonságos kezelése céljából hajtanak végre az adatvédelmi és egyéb jogszabályok betartása érdekében. [14]

Luigi Coppolino és szerzőtársai a *Hogyan védjük meg a közigazgatást a kiberbiztonsági veszélyekkel szemben: a COMPACT Projekt* című tanulmányban rögzítik, hogy az Internet megjelenése új lehetőségeket nyitott a közigazgatás számára a hatékonyságuk javítása érdekében, amely segítségével egyre több szolgáltatást képes nyújtani az állampolgárok számára az e célra specializálódott hálózati alkalmazások révén, ideértve az e-kormányzatot, az e-egészségügyet és még sok más egyéb szolgáltatást. A COMPACT projekt célja a helyi közigazgatási szervek tudatosságának, kiberbiztonsági készségeinek és az internetes fenyegetésekkel szembeni védelmének növelése. [15]

Az Andreasson által szerkesztett *Kiberbiztonság: A közszféra fenyegetései és reakciói* című könyv a globalizáció konvergenciájára és a közszféra funkcióinak online migrációjára összpontosít és meghatározza azokat a kihívásokat, amelyeknek tudatában kell lennünk. Emellett megvizsgálja a világ minden táján felmerülő trendeket és stratégiákat, praktikus útmutatást kínálva ezzel az aktuális kockázatok kezelésére. A könyv elemzi az Egyesült Államok és Európa jelenlegi stratégiai és politikai környezetét, valamint szemlélteti a kihívásokat minden kormányzati szinten. Ismerteti a kibertámadások eseteit és az ezekre történő reagálás egyes lépéseit,

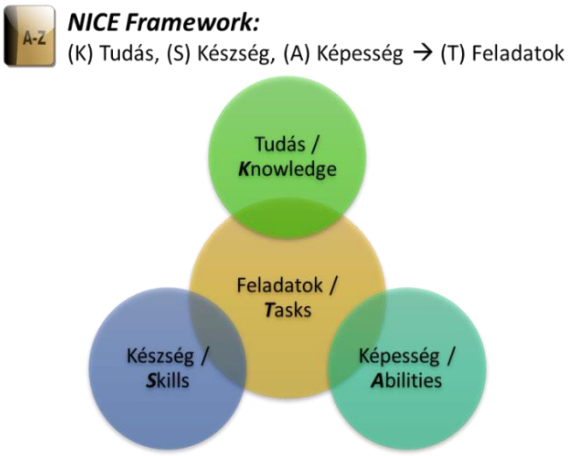
figyelembe véve a kockázatok felmérésének szervezeti keretét és a kialakuló tendenciákat. [16]

2.2.4. NICE KERETRENDSZER

A National Initiative for Cybersecurity Education vagy másnéven a Kiberbiztonsági Oktatás Nemzeti Kezdeményezését (a továbbiakban: NICE) az Egyesült Államok Kereskedelmi Minisztériumának Nemzeti Szabványügyi és Technológiai Intézete vezeti, amely egyfajta partnerségként értelmezhető a kormány, az akadémiai szféra és a magánszektor között. Az együttműködés középpontjában a kiberbiztonsági oktatás, képzés, valamint munkaerő hálózatának folyamatos fejlesztése áll. A NICE ennek keretében tudományos és ipari partnerekkel egyeztetve koordinálja a már meglévő, sikeres kiberbiztonsági programokat, valamint elősegíti az innovációt és a kiberbiztonsági szakemberek jövőképének kialakítását. A NICE olyan országos és nemzetközi kezdeményezéseket támogat, amelyek segítségével növelhető a kiberbiztonsággal kapcsolatos munkák elvégzéséhez szükséges ismeretekkel, készségekkel és képességekkel rendelkező szakértők száma.

A NICE Keretrendszer alapvető referenciaként szolgál olyan munkaerő támogatásához, amely képes kielégíteni a szervezet kiberbiztonsági igényeit egy közös, következetes „lexikon” segítségével, amely leírja a lehetséges kiberbiztonsági munkát kategóriánként, szakterületenként, illetve munkakörönként. [6]

Mindemellett a NICE meghatározza az elsajátítandó kiberbiztonsági tudást, készségeket, képességeket és feladatokat az egyes munkakörökhöz, ahogyan azt a 2-2. ábra is szemlélteti. E keretrendszer kiváló alapként szolgálhat az általunk átadni kívánt tudás, készségek, képességek meghatározására, a kiberbiztonsági tantervek, tantárgyi adatlapok kidolgozására.



2-2. ábra NICE keretrendszer KSA elemeinek kapcsolata

A NICE Keretrendszerről és a kiberbiztonsági oktatás fontosságáról számos nemzetközi tanulmány tartalmaz megállapításokat, következtetéseket.

Izzat Alsmadi tanulmánya rámutat a jelenlegi kiberbiztonsági munkaerőhiány jelenségére, valamint arra, hogy folyamatos növekedés figyelhető meg a kiberbiztonsági szakemberek és készségek iránti igények tekintetében. Továbbá rávilágít az elméleti és gyakorlati képességek közötti egyensúly hiányára, illetve az akadémia és a versenyszféra közötti szakadékra, amelyeket a NICE Keretrendszer segítségével meg lehetne oldani. [17]

Miriam E. Armstrong és szerzőtársai szintén kihangsúlyozzák a növekvő kiberbiztonsági munkaerőhiány jelenlétét, ezáltal pedig a kiberbiztonsági munkaerő iránti kereslet és versengés megjelenését. A cikk rögzíti az egyetemek szerepét, amely szerint hozzájárulnak a növekvő kiberbiztonsági igények kielégítéséhez azáltal, hogy megfelelő kiberbiztonsági képesítést biztosítanak a következő generáció számára, továbbá döntő fontosságú, hogy az ilyen képzések tanterveit úgy alakítsák ki, hogy az adott munkakör típusához is illeszkedjenek, továbbá gyakorlati ismereteket is tartalmazzanak. [18]

Adriane C. Estes és szerzőtársai tanulmányukban feltárják, hogy a NICE kiberbiztonsági munkaerőrendszere hogyan igazítja és hangolja össze a kiberbiztonsági munkákat a potenciális jelöltekkel. A szerzők bemutatják, milyen előnyei vannak egy szervezet számára a NICE Keretrendszer alkalmazásának, illetve hogyan segít azonosítani a kiberbiztonsági képességeket és megoldást találni ezen képességek hiányára, valamint folyamatos fejlesztésére, nemcsak szervezeti, hanem globális szinten egyaránt. [19]

Ernest L. McDuffie és Victor P. Piotrowski rávilágítanak arra, hogy a kiberbiztonsági oktatás és a munkaerő fejlesztése jelentősen hozzájárul a közös kiberbiztonsági nyelv kialakításához, amely nagyban javítja a problémamegoldást is. [20]

2.2.5. Az ECSF Keretrendszer

Az Európai Kiberbiztonsági Készségek Keretrendszerének (ECSF) célja, hogy az európai uniós tagállamokban az egyének, a munkaadók és a képzést biztosító szervezetek, intézmények számára közös álláspontot alakítsanak ki a kiberbiztonsági készségek hiányának orvoslásához szükséges szerepekről, kompetenciákról, készségekről és ismeretekről. Ezenkívül az ECSF segíti a kiberbiztonsággal kapcsolatos készségek elismerését, és támogatja a kiberbiztonsággal kapcsolatos készség- és karrierfejlesztési képzési programok tervezését. Végső soron az ECSF támogatja a foglalkoztathatóságot a kiberbiztonsággal kapcsolatos pozíciókban. Az ECSF Keretrendszer tizenkét kiberbiztonsággal összefüggő munkakört mutat be, ahogyan azt a 2-3. ábra mutatja. Ezen belül rögzíti az egyes pozíciók rövid összefoglalóját, a munkakör küldetését, alapfeladatait, készségeket, képességeket és ismereteket, valamint a szükséges e-kompetenciákat[3] és azok elvárható szintjét. [7]

2-3. ábra ECSF kiberbiztonsággal összefüggő területei (forrás: [7])

[3] Az Európai e-Kompetencia Keretrendszer (e-CF) által definiált e-kompetenciák közül kiválasztott kompetenciák. Az e-CF az IKT-ismeretek közös referenciapontja, amely 40 digitális kompetenciát határoz meg az állami és magánszektor számára.

2.3. INTERJÚ RELEVÁNS SZEREPLŐKKEL

Jelen alfejezetben bemutatott interjú során egy a közszférában és egy a magánszférában vezető tisztséget betöltő személlyel történő beszélgetésre került sor. A közszféra kiberbiztonságának vizsgálatához a Magyar Államkincstárat választottam, amelynek informatikai biztonsági vezetőjét, Dr. Muha Lajost kértem fel az interjú elkészítéséhez. A másik oldalról a magánszféra képviseletére egy vezető szoftverfejlesztő céget, a Login Autonom Kft-t választottam, amelynek egyik ügyvezetőjével Dr. Otti Csabával készítettem interjút. Az interjú teljes egészében megtekinthető az F1. számú függelékben.

2.3.1. CÉLOK ÉS LIMITÁCIÓK

Az interjú célja az alábbi fő kérdésekre választ adni:

- **C1.** Van-e egyértelműen meghatározható különbség a magánszektor és a közszolgálat között kiberbiztonság szempontjából?
- **C2.** Meghatározható-e a személyek képzése és a technológiai fejlesztések között egyértelmű financiális, illetve fontossági sorrend a magánszektor és a közszolgálat esetén?
- **C3.** Létezik-e speciálisan a magánszektor, illetve a közszolgálatra jellemző kibervédelmi stratégia, amely esetleg adaptálható lenne a másik szektorban?
- **C4.** Informatikai infrastrukturális szempontból meghatározható-e egyértelmű különbség a magánszektor és a közszolgálat között?

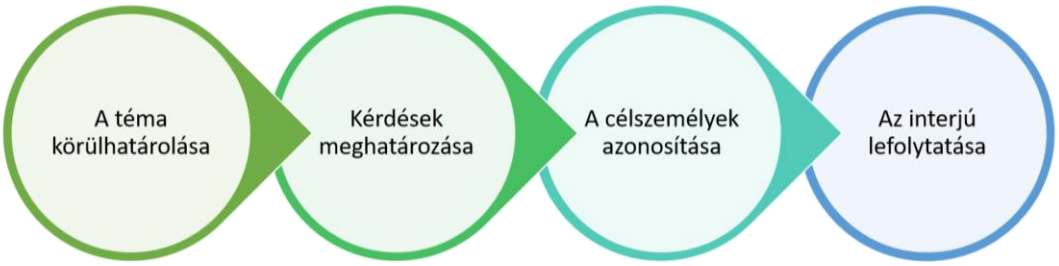
Ahhoz, hogy az itt definiált kérdésekre választ kaphassunk, azonosítani kell azokat a limitációkat is, amelyek egy ilyen jellegű interjú során felmerülhetnek, hogy a részkutatás valós eredményeket tükrözhessen.

- **K1.** A célszemélyek, csak magasszintű válaszokat adhatnak a belső szabályzatuknak megfelelően, így részletes, konkrét esetek nem kerülhetnek bemutatásra.
- **K2.** A célszemélyek nem rendelkeznek az interjú során pontos gazdasági kimutatásokkal.
- **K3.** Bár a célszemélyek a legjobb tudásuk és jó szándékuk szerint válaszolnak a kérdésekre, azonban a nem tényekre hivatkozó kérdések esetén csak a saját véleményüket mutatják be.

2.3.2. ELŐKÉSZÍTÉS FOLYAMATA

Az interjú folyamata a 2-4. ábra által bemutatott szakaszokból épül fel, amelyeket jelen kutatás részletesen kifejt a következő alpontokban.

1. A téma körülhatárolása
2. Kérdések meghatározása
3. A célszemélyek azonosítása
4. Az interjú lefolytatása



2-4. ábra: Az interjú folyamata

2.3.2.1. A téma körülhatárolása

A téma elsődlegesen a magánszektor és a közszolgálat kibervédelmi mechanizmusainak összehasonlítására épül annak érdekében, hogy meghatározhassam, van-e különbség egy piaci alapon működő cég és egy közszolgálati szervezet védelmi stratégiájában. Továbbá fontos megvizsgálni, hogy a vezetők mi alapján döntenek a védelmi stratégia kidolgozása fejlesztése során, így nagy hangsúly kerül az informatikai eszközök vásárlására és a munkaerő továbbképzésére. A téma meghatározását követően sor került a témával kapcsolatos korábbi kutatások eredményeinek feltérképezésére, valamint az interjúkészítés szabályainak elemzésére.

2.3.2.2. Kérdések meghatározása

A kérdések meghatározása során a korábban bemutatott célok megválaszolására szolgáló kérdéseket azonosítottam. A célok alapján csoportosítva, a 2-1. táblázat tartalmazza az általam definiált kérdéseket:

Cél	Kérdés
C1	Szembesültek-e már kiberbiztonsági incidenssel? Megelőzni sikerült-e vagy reagálni a már bekövetkezett eseményekre? Sérült-e az adatok CIA[4]-ja?
C4	Milyen főbb informatikai infrastrukturális komponensei vannak a szervezetnek?
C3	Milyen kibertámadási felületek vannak a szervezetnél?
C3	Milyen védekezési stratégiát alkalmaznak?
C2	Milyen kiberbiztonsággal kapcsolatos képzéseket tartanak az alkalmazottak számára?
C2	Melyiket látja hatékonyabbnak a technológiai védelmet vagy a személyek képességeinek fejlesztését? Miért?
C2	Financiális szempontból melyiket tartják gazdaságosabbnak, a technológiai védelmet vagy a személyek képességeinek fejlesztését?
C2	Milyen kibervédelmi képességek szükségesek a munkavállalók mindennapi feladatainak ellátáshoz?
C1, C4	Lát-e különbséget a közszolgálat és a magánszféra kiberbiztonsági kockázatait illetően?

2-1. táblázat: Az interjú kérdései a kutatási célok szerint

2.3.2.3. *Célszemélyek azonosítása*

A cél olyan személyek bevonása az interjúba, akik eredményesen képviselik a magánszektor és a közszolgálat érdekeit, illetve rendelkeznek azon tudással, amely a kibervédelem és a kiberbiztonság kialakításához, illetve folyamatos fejlesztéséhez elengedhetetlen. A célszemélyek kiválasztásának alapvető feltétele volt, hogy egy a közszolgálatban és a magánszektorban vezető tisztséget betöltő személy kiválasztása valósuljon meg. Fontos szempont volt, hogy az interjúalanyok nap, mint nap részt vegyenek a kiberbiztonsággal kapcsolatos stratégiai és financiális döntések kidolgozásában és meghozatalában.

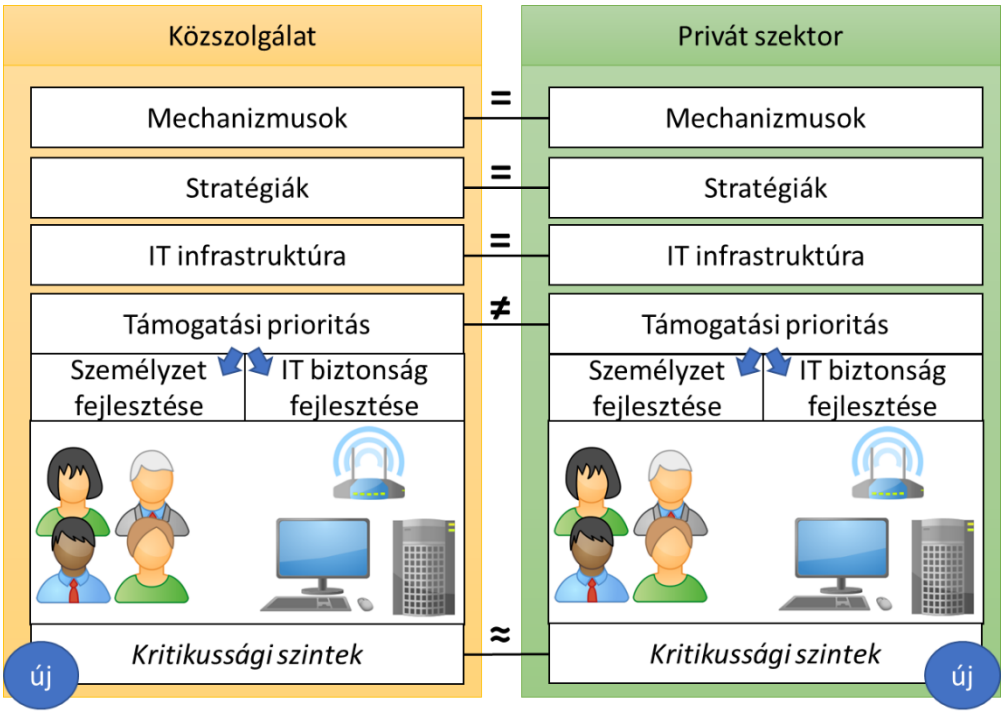
[4] CIA: az információs rendszerek megfelelő szintű védelme érdekében a következő követelményeket kell teljesíteni: bizalmasság (confidentiality), sértetlenség (integrity) és rendelkezésre állás (availability). A követelmények angol megfelelőinek kezdőbetűjéből álló módszertan neve: CIA.

2.3.2.4. Az interjú lefolytatása

A kompetens interjúalanyok kiválasztását követően került sor az interjúra történő felkérésre, illetve a megfelelő helyszín kiválasztására. Ezt követte az interjú végrehajtása, a kérdések feltevése. Az adatrögzítés két lépésben történt, az interjúalanyok engedélyével hang- és videófelvételt készítettem az elhangzottakról, majd pedig írott szöveggé alakítottam azokat. Az interjúalanyok válaszait elektronikus formában küldtem meg részükre ellenőrzés céljából, majd a jóváhagyást követően a válaszokat összegeztem és elhelyeztem az interjút bemutató publikációban [j2] és jelen értekezésben.

2.3.3. AZ INTERJÚ KÖVETKEZTETÉSEI

Az interjú kérdéseire adott válaszok és az azonosított limitációk alapján a 2-5. ábra által prezentált következtetések határozhatók meg a kutatás elején definiált kérdésekre:



2-5. ábra Az interjú alapján elkészített összehasonlítás eredményei

K1. Nem határozható meg egyértelmű különbség a magánszektor és a közszolgálat között kiberbiztonság szempontjából.

Mindkét interjúalany kijelentette, hogy bár lehetnek különbségek a fent említett két szektor között, azonban rendkívül nagy az átfedés. Külön kiemelendő, hogy az interjúalanyok inkább a kritikusság szintjei szerint látnak

eltéréseket a kiberbiztonság szempontjából, azonban a feladatok és védelmi stratégiák megegyeznek. Természetesen a védelmi intézkedések a jogszabályi kötelezettségek függvényében mindkét oldal vonatkozásában tartalmazhatnak eltéréseket. Emellett a legfőbb különbség a támogatások priorizálása kapcsán jelentkezett, tekintettel arra, hogy a szektorok eltérően vélekednek a technológiai védelem és a személyek képességeinek fejlesztését célzó képzések megvalósításának költségeiről és szerepéről.

K2. A magánszektorban és a közszolgálatban eltérő a vélemény a személyek képzése és a technológiai fejlesztések között financiális szempontból.

Míg a közszolgálatban egyértelműen nagyobb eredményt lehet elérni az alkalmazottak továbbképzésével, a magánszektorban a képzések ideje alatti termelés redukálása nagyobb gazdasági hiányt okozhat, ezért inkább kockázatelemzések alapján határozzák meg, hogy melyik aspektusra mekkora keret fordítható.

K3. Nem határozható meg fontossági sorrend a személyek képzése és a technológia fejlesztések között a magánszektor és a közszolgálat esetén.

Az interjúalanyok egyetértettek abban, hogy a technológiai fejlesztések hatástalanok lehetnek, ha az alkalmazottak nem rendelkeznek megfelelő képzettséggel, és a legjobban felkészített alkalmazottak sem képesek mindennemű kibertámadás elhárítására.

K4. A magánszektor és a közszolgálat is hasonló kibervédelmi stratégiákat használ.

Az interjúalanyok válaszai alapján látható, hogy mindkét szektorban megtalálhatóak a kibervédelmi szabályzatok, folyamatos sérülékenységi vizsgálatok, és azonos state-of-the-art megközelítéseket alkalmaznak a kibervédelmi szempontból kockázatos felületek megerősítésére.

K5. Informatikai infrastrukturális szempontból hasonló a magánszektor és a közszolgálat.

Mivel az interjúalanyok hasonló kritikusságú szervezetek vezetői, így az informatikai infrastruktúrájuk is hasonlóak.

2.4. CÉLCSOPORT AZONOSÍTÁSA

A közszolgálati kiberbiztonság megteremtéséhez elengedhetetlen a kibervédelmi képességek elsajátítása és folyamatos fejlesztése. Azonban vannak olyan területei a közszolgálatnak, amelyek sokkal részletesebben és eltérő aspektusból is vizsgálják a kiberbiztonságot (pl. honvédség, nemzetbiztonsági szolgálatok stb.), ezért célszerű meghatározni, hogy a közszolgálat mely területeivel szeretnék foglalkozni jelen kutatás fő kontextusában.

Ahhoz, hogy a célcsoport definiálható legyen, mindenképp szükséges meghatározni a közszolgálat fogalmát. A nemzetközi és hazai szakirodalom alapján megállapítható, hogy nagyon nehéz egy egységes definíciót alkotni a közszolgálatra, hiszen országonként eltérő, hogy mely szervek és alkalmazotti körök társíthatók e fogalomhoz. Antal Zsolt a közszolgálat definícióját többféle megközelítésből (jogi, funkcionális, szervezeti) vezeti le, amelyek alapján a közszolgálat olyan nem piaci mechanizmusok által vezérelt tevékenységek összessége, amelyet az állam által többségében tulajdonolt szervezetek valósítanak meg a közjó fenntartása vagy növelése érdekében. [21]

Hazafi Zoltán doktori értekezésében két definíciót rögzít, az egyik az úgynevezett funkcionális fogalom, amelynek értelmében mindenki, aki közfeladatot lát el közszolgálati alkalmazottnak minősül, függetlenül az őt alkalmazó szervezet jogállásától, személyes státuszától, kiválasztásától, illetve díjazásától. A másik, úgynevezett szűkebb meghatározás szerint közszolgálati alkalmazott az, akit a jogállására vonatkozó szabályok ilyen minőséggel ruháznak fel. [22] Ezen definíciókból következik, hogy a közszolgálati alkalmazotti csoport rendkívül széles spektrumú, mind az ide tartozó munkaköröknek, mind az alkalmazottak képességeinek, készségeinek köszönhetően. Éppen ezért fontos jelen kutatás szempontjából releváns közszolgálati alkalmazotti kör szűkítése olyan területekre, amelyek részt vesznek a döntéshozatalban és alapvető képzésük során nem részesülnek részletes, átfogó kiberbiztonsági oktatásban. Ide tartoznak például az alábbi közszolgálati munkakörök a teljesség igénye nélkül:

a) a közigazgatásban foglalkoztatott tisztviselők,
b) az állami főhatalom szerveinek hivatalaiban dolgozó személyek,
c) az egyes speciális jogállású központi szervekben dolgozó személyek,

d) a rendvédelmi feladatokat ellátó szervek igazgatási feladatot végző tagjai,
e) bírák, ügyészek, illetve a munkájukat segítő alkalmazottak,
f) katasztrófavédelem területén dolgozó igazgatási feladatot ellátó személyek,
g) a Magyar Honvédség igazgatási feladatot végző tagjai.

Összességében megállapítható, hogy a közszolgálati alkalmazottak ilyen típusú szűkítése elengedhetetlen a közszolgálati kiberbiztonság megvalósításához, hiszen ahhoz, hogy meghatározzuk milyen ismerethalmaz elsajátítása a cél, tudnunk kell, hogy milyen területen zajlik a mindennapos munkavégzés, illetve milyen típusú döntéshozatalban vesznek részt az alkalmazottak.

A továbbiakban a közszolgálati munkakörök fogalma alá kizárólag a jelen értekezés alapjául szolgáló kiberbiztonsági képzés szempontjából releváns munkakörök kerülnek besorolásra, amelynek komponenseit a fenti felsorolás elemei alkotják. A képzés közszolgálati célcsoportja köréből kivételt képeznek a fentebb már említett speciális kategóriák, így különösen az alábbiak:

a) Magyar Honvédség személyi állományába tartozó tényleges szolgálatot teljesítő katonák [2011. évi CXIII. törvény 40. § (1)],
b) nemzetbiztonsági szolgálatok (Katonai Nemzetbiztonsági Szolgálat, Nemzetbiztonsági szakszolgálat, Alkotmányvédelmi Hivatal),
c) bűnüldözési szervek bűnügyi felderítési, nyomozati feladatait ellátó szerveinél dolgozó személyek.

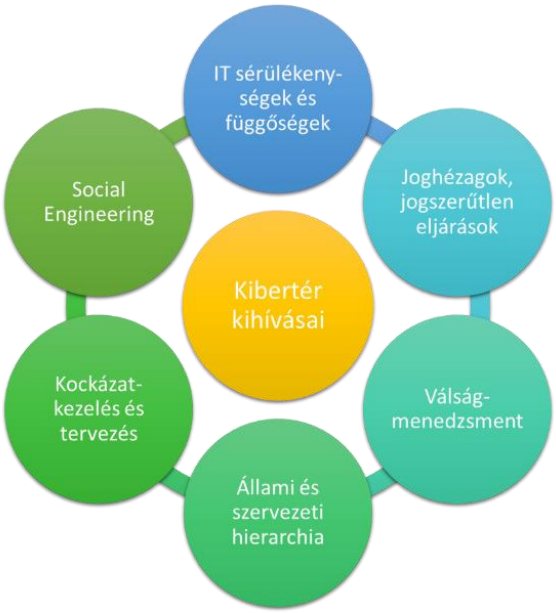
Összegezve, a jelen képzés célcsoportjába alapvetően a közszolgálatban igazgatási feladatokat ellátó személyek tartoznak, tekintettel arra, hogy az egyéb, speciális területeken dolgozó személyek munkaköre eltérő egyedi szakmai ismeretek elsajátítását igényli.

2.5. Feladatok, készségek, képességek és ismeretek azonosítása

Fontos meghatározni, hogy a kiválasztott célcsoportnak milyen feladatai lehetnek a kibertérhez kapcsolódóan, továbbá azonosítani kell, hogy milyen készségek, képességek és ismeretek szükségesek ahhoz, hogy ezeket a feladatokat a lehető legmegbízhatóbban teljesíteni tudják munkájuk során.

2.5.1. A KIBERTÉR KIHÍVÁSAINAK AZONOSÍTÁSA

A képzés célcsoportjának meghatározása után szükséges azonosítani a kibertér kihívásait, hiszen e kihívásokhoz igazodva lehet definiálni az általános kiberbiztonsági feladatokat és az elsajátítandó ismerethalmazt. A kibertér magas szintű kihívásait foglalja össze a 2-6. ábra, amely a következő hat fő terület azonosítja: az IT sérülékenységek és függőségek, joghézagok és jogszerűtlen eljárások, válságmenedzsment, állami és szervezeti hierarchia, kockázatkezelés és tervezés, illetve a pszichológiai manipuláció (social engineering).



2-6. ábra A kibertér kihívásai

IT sérülékenységek és függőségek

Az IT sérülékenységek és függőségek elsődlegesen abból fakadnak, hogy napjainkban szinte minden folyamatban megjelenik valamilyen IT eszköz, amely sok esetben az adott folyamat szükséges elemeként, feltételeként értelmezhető. Ebből következik, hogy egyfajta függőség alakul ki a különféle informatikai eszközök, termékek iránt. A szolgáltatásfüggőséggel összefüggésben azonban nem csak a személyek informatikai eszközök iránti függőségét szükséges kiemelni, hanem az egymással kapcsolatban álló eszközök, rendszer és folyamatok függőségét is.

A különböző informatikai eszközök dinamikusan fejlődnek a különböző igényeknek köszönhetően. Fontos kiemelni, hogy ezen eszközök, illetve termékek sose lehetnek tökéletesen biztonságosak, tekintettel arra, hogy nem lehet olyan szinten tesztelni ezeket az eszközöket, hogy azt lehessen mondani, hogy azok teljes mértékben

biztonságosnak tekinthetőek. Ennek megfelelően az IT komponensek mindig tartalmaznak valamilyen típusú sérülékenységet, amelyeket csak a kihasználásuk után tud majd a komponens fejlesztője javítani. Ezek alapján a 2-2. táblázat tartalmazza azokat a problématerületeket az IT sérülékenységek és függőségek témakörében, amelyeket kezelnie kell a szervezetnek.

IT sérülékenységek és függőségek
folyamatosan erősödő információtechnológiai szolgáltatásfüggőség
informatikai rendszer sérülékenységeit célzó kibertámadások
kriptográfiai összefüggések kihasználását célzó kibertámadások
folyamatosan változó és fejlődő kibertéri technológiák

2-2. táblázat Az IT sérülékenységekkel és függőségekkel kapcsolatos kihívások

Joghézagok, jogszerűtlen eljárások

Számos támadástípus épít arra, hogy a jelenlegi kiberbiztonsági szabályozás számos hiányosságot, joghézagot tartalmaz (pl. felhőhasználat adatvédelmi kérdései), amely segítségével a támadások nem csak hatékonyan kivitelezhetők, de jelentősen megnehezítik a szervezet incidenskezelési folyamatát, tekintettel arra, hogy a nem szabályozott területek a szervezeti kiberbiztonsági gyakorlatot tekintve komoly sebezhetőséget rejthetnek. Mindemellett szükséges megemlíteni az eltérő országokban megjelenő jogi szabályozást, hiszen amennyiben határokon átnyúló kibertámadás következik be, úgy figyelembe kell venni az eltérő szabályozás tartalmát is és e szabályok tárgyi, területi és személyi hatályát egyaránt. Ennélfogva elengedhetetlen a kibervédelem megvalósítása során kiemelt figyelmet fordítani e területtel, amelyen belül a 2-3. táblázat által tartalmazott kihívásokat azonosítottam.

Joghézagok, jogszerűtlen eljárások
joghézagok kihasználását célzó kibertámadások
jogszerűtlen eljárások alkalmazása a kibertámadások elhárítása során
adatvédelmi, információbiztonsági incidensek bekövetkezése kibertámadások során

2-3. táblázat Joghézagokkal és jogszerűtlen eljárásokkal kapcsolatos kihívások

Állami- és szervezeti hierarchia

Sok esetben a szervezet alkalmazottai sincsenek tudatában, hogy egy kibertámadás áldozatává váltak. Azonban, még ha az alkalmazottak észlelik is a támadást, nincs megfelelően kidolgozott szabályozás arra vonatkozóan, hogy kiket kell értesíteni ilyen esetben, milyen információkat kell közölni, illetve milyen további feladatokat

szükséges végrehajtani a hatékony incidenskezelés megvalósítása érdekében. További nehézséget jelent, ha egy kibertámadás határokon is átível, hiszen a szervezet különböző kirendeltségei még nehezebben képesek észlelni ilyen esetekben a támadásokat. Mindemellett egy több országot is érintő biztonsági esemény kezelése során figyelembe kell venni az alkalmazandó jogszabályokat, valamint az eljáró hatóságokat is. Ezek alapján az állami- és szervezeti hierarchiához kapcsolódóan további kihívásokat azonosítottam, amelyek a 2-4. táblázatban találhatóak.

Állami- és szervezeti hierarchia
egyéni és szervezeti kibervédelmi képesség hiánya
egyéni és szervezeti kibervédelmi feladatok nem megfelelő meghatározása és végrehajtása
szervezeten belüli szabályozási hiányosságok kihasználása a kibertámadások végrehajtása során
határokon átívelő kibertámadások
szervezeten kívüli szakértő személyek, szervezetek, hatóságok bevonásának hiánya

2-4. táblázat Állami- és szervezeti hierarchiához kapcsolódó kihívások

Válságmenedzsment

A kiberbiztonsági válsághelyzetben a nem megfelelő diplomáciai, politikai és szervezeten belüli információmegosztás, kommunikáció jelentősen csökkentheti a szervezet incidenskezelési eljárásának hatékonyságát, valamint a szervezet reputációját. Mindemellett jelentősen erősíthető a szervezet alkalmazottai és a szolgáltatást igénybe vevők körében a bizonytalanságot, félelmet. Ennek megfelelően különös figyelmet szükséges fordítani a válságmenedzsmentre a kibertámadások bekövetkezése és kezelése esetén. Ehhez kapcsolódóan a 2-5. táblázat tartalmazza azon problématerületeket, amelyek mint további kihívások kapcsolódnak a válságmenedzsmenthez.

Válságmenedzsment
kiberbiztonsági válsághelyzetben nem megfelelő diplomáciai, politikai és szervezeten belüli információmegosztás, kommunikáció
kibertámadási technika nem megfelelő azonosítása
komplex, összehangolt kibertámadások végrehajtása

2-5. táblázat Válságmenedzsmenthez kapcsolódó kockázatok

Kockázatkezelés és tervezés

A kockázatkezelés és tervezés a kiberbiztonság során is elengedhetetlen minden szervezet életében, tekintettel arra, hogy az eredményes kockázatelemzési- és kezelési tevékenység jelentősen hozzájárul a kibertámadások bekövetkezése esetén azok hatásainak mérsékléséhez, valamint a hasonló típusú események bekövetkezésének megelőzéséhez. Természetesen nehéz felkészülni az olyan típusú eseményekre, amelyekről korábban még csak nem is tudtunk, hogy létezik (pl.: nulladik napi sebezhetőségek), azonban ezekre az esetekre is fel kell készülnünk. A szervezetek egyre több IT eszközt, komponenst használnak, amely egyre több sérülékenység megjelenésének kockázatát rejti, illetve a károk mértéke is egyre nagyobbá válik, amely rendkívül nagy kihívásként értelmezhető a tervezés során. Ennek megfelelően a 2-6. táblázat által bemutatott kihívásokkal kell megküzdeni a kockázatkezelés és tervezés esetén.

Kockázatkezelés és tervezés
a szervezet kiberbiztonsági kockázatainak, sérülékenységeinek hiányos, nem megfelelő feltárása
folyamatosan változó és fejlődő kibertéri technológiák

2-6. táblázat Kockázatkezeléssel és tervezéssel kapcsolatos kihívások

Pszichológiai manipuláció (Social Engineering)

A pszichológiai manipuláció vagy másnéven social engineering a támadók rendkívül veszélyes eszköze, amely során legfőképp a felhasználók manipulálására és befolyásolására építve, a felhasználók hiszékenységét és tudatosságának hiányát kihasználva érik el céljaikat, így például szerzik meg a felhasználók, illetve a szervezetek bizalmas adatait, információit. Éppen ezért rendkívül nehéz e támadási formára felkészülni, hiszen ha a támadók kiismerik a felhasználót, akkor képesek információt szerezni tőle akár a kibertérben is. A social engineering esetén a 2-7. táblázat szerinti kihívásokat azonosítottam:

Social Engineering
a felhasználó kihasználására, biztonságtudatosságának hiányára épülő kibertámadások
a támadó által alkalmazott viselkedési stratégiák a kibertámadások végrehajtása során

2-7. táblázat Pszichológiai manipulációhoz kapcsolódó kihívások

2.5.2. KIBERBIZTONSÁGI FELADATOK

A képzés célcsoportjának és az aktuális kiberbiztonsági kihívások meghatározása után szükséges definiálni azokat az általános kiberbiztonsági feladatokat, amelyeket a közszolgálatban dolgozóknak szükséges végrehajtani akár a mindennapi munkájuk során, akár egy esetleges kibertámadás esetén. A NICE és az ECSF Keretrendszerek segítségével azonosított feladatokat a 2-8. táblázat tartalmazza. [6]

	NICE és ECSF Keretrendszer által definiált feladatok
T1.	kockázatelemzés elkészítése, tanácsadás a felsővezetésnek a kockázatértékelési folyamatról, kockázati szintekről, az információbiztonsági programokról, irányelvekről, folyamatokról és eljárási szabályokról
T2.	üzletmenetfolytonossági tervek elkészítése, kapcsolódó tesztek elvégzése
T3.	kiberbiztonsági érdekek képviselése a szervezeten belül
T4.	adatvédelmi, kiberbiztonsági stratégiai tervek kidolgozása és végrehajtása
T5.	az adatvédelmi és kiberbiztonsági alapelvek a szervezet küldetésében, jövőképében és céljaiban történő megjelenítése
T6.	releváns jogszabályok, szabványok, eljárások, technológiai változások figyelemmel kísérése, értelmezése, alkalmazása
T7.	hazai és külföldi „jó gyakorlatok” alkalmazása
T8.	belső audit végrehajtása, auditjelentések elkészítése
T9.	közvetítés a műszaki és nem műszaki szakemberek között
T10.	közreműködés az információs infrastruktúra kialakításában, fejlesztésében
T11.	incidenskezelési folyamat kialakítása, incidensek kezelése
T12.	a szervezet folyamatainak figyelemmel kísérése a biztonsági és az adatvédelmi szabályok betartásának ellenőrzése céljából
T13.	kapcsolat kialakítása az adatvédelmi és kiberbiztonsággal kapcsolatos hatóságokkal és közösségekkel
T14.	a szervezet kiberbiztonsággal, adatvédelemmel foglalkozó munkatársainak felügyelete, irányítása

2-8. táblázat A kiválasztott célcsoport általános kibervédelmi feladatai

A feladatok meghatározását követően azonban mindenképp szükséges kiemelni, hogy a kiberbiztonsági feladatok és a szervezeten belüli egyéb, a kiberbiztonság területéhez szorosan kapcsolódó munkakörök – így különösen az adatvédelmi tisztviselő, információbiztonsági vezető, szakértő - feladatai több esetben is átfedést tartalmaznak. Ennek oka, hogy e területek egymásra épülnek, szoros kapcsolatban állnak egymással,

továbbá a feladatok végrehajtásával összefüggő ismeretek is fedik egymást, amelyből következik, hogy a feladatok ellátása sok esetben közösen történik.

Azonban a NICE és az ECSF Keretrendszerben rögzített feladatkörök tapasztalataim szerint nem fedik le a kiberbiztonsággal összefüggő feladatok egészét, ezért a fenti felsorolást a 2-9. táblázatban található feladatokkal javaslom kiegészíteni:

	Egyéb feladatok
T15.	kiberbiztonsági fenyegetések, támadások felismerése és szegregálása, a kibertámadásokkal szembeni ellenálló képesség kialakítása
T16.	a szervezet technikai és humán sebezhetőségeinek feltárása, kockázatok azonosítása
T17.	kiberbiztonsággal, adatvédelemmel kapcsolatos képzések, oktatások megtartása, tudatosságnövelő programok lebonyolítása

2-9. táblázat A kiválasztott célcsoport további kibervédelmi feladatai

2.5.3. A NICE ÉS ECSF KERETRENDSZER ÁLTAL DEFINIÁLT ISMERETHALMAZ

A T1-T14 kiberbiztonsággal összefüggő feladatok ellátásához szükséges ismerethalmaz definiálása során a NICE Keretrendszer kiberbiztonsági pozíciói közül az adatvédelmi tisztviselő munkakör került kiválasztásra. Ennek oka, hogy ez a pozíció az, amely a leginkább illeszkedik a célcsoport előképzettségéhez, valamint az általuk megszerezhető képességekhez. Ezt követően megvizsgáltam a keretrendszer által előírt tudás-, képesség- és készséghalmazát és kiválasztottam azokat, amelyek véleményem szerint feltétlenül szükségesek a nevezett feladatok teljesítésének. Ezeket az ECSF Keretrendszerben található munkakörök (pl. információbiztonsági vezető, adatvédelmi tisztviselő) betöltéséhez szükséges képességekkel egészítettem ki. Ennek megfelelően a 2-10. táblázat tartalmazza ezen feladatokat, tudást, képességeket és készségeket:

Tudás (K)
K1. számítógéphálózatokhoz kapcsolódó alapfogalmak ismerete
K2. kockázatkezelési folyamatok ismerete
K3. kiberbiztonsági, adatvédelmi jogszabályok, irányelvek, alapelvek ismerete
K4. kibertérből érkező fenyegetések ismerete
K5. vezeték nélküli technológiák ismerete
Képesség (A)
A1. egyértelmű, világos, átlátható stratégia, iránymutatások, szabályok, eljárások, folyamatok és képzési anyagok, dokumentációk kidolgozásának képessége
A2. szabványos működési eljárások, folyamatok kidolgozásának és folyamatos fejlesztésének, valamint azok jogszabályoknak való megfeleltetésének képessége
A3. a releváns adatvédelmi, kiberbiztonsági jogszabályok, szabványok, keretrendszerek, irányelvek, technológiák elemzése és változásának nyomon követésének képessége
A4. operatív célok eléréséhez szükséges megfelelő intézkedések, eljárások kiválasztásának képessége,
A5. adatvédelmi és információbiztonsági célok összehangolásának képessége
A6. annak meghatározásának képessége, hogy egy biztonsági esemény, incidens megsérti-e a magánélet tiszteletben tartásának elvét, vagy a jogi előírásokat
A7. képzési programok, tervek kidolgozásának képessége
A8. adatvédelmi szabályzatok, stratégiák, dokumentumok kidolgozásának képessége
A9. adatvédelmi, kiberbiztonsági csapatok vezetésének képessége
Készség (S)
S1. adatvédelmi szabályok, irányelvek készítésének készsége
S2. a beszállítókkal és partnerekkel való tárgyalókészség, valamint ezek adatvédelmi gyakorlataival kapcsolatos értékelésének készsége
S3. különböző szintű kommunikációs készség a szervezet különböző területeinek megfelelően

2-10. táblázat T1-T14 feladatokhoz szükséges KSA elemek

2.5.4. Egyéb a NICE és ECSF Keretrendszer által nem definiált ismerethalmaz

A további feladatok végrehajtásához azonban további tudást, képességeket és készségeket is kell azonosítani. Ennek megfelelően a 2-11. táblázat foglalja össze azon további ismerethalmazt, amelyek szükségesként azonosítottam.

	Tudás (K)
K1*	a nemzetközi és állami kibervédelmi rendszer ismerete
K2*	a szervezeten belüli kiberbiztonsági és adatvédelmi felelős pozíciók ismerete
K3*	a kibertámadások bekövetkezése esetén alkalmazható technikák, eljárások ismerete
K4*	az emberi tényező és a kiberbiztonság kapcsolódási pontjainak ismerete
K5*	a kibertámadások mögött rejlő motivációk és pszichológiai tényezők ismerete
	Képesség (A)
A1*	a belső munkavállalók jelentette kiberbiztonsági kockázatok felismerésének képessége
A2*	a humán fenyegetettségből eredő kockázatok csökkentésének képessége a szervezeten belül
A3*	a szervezetben betöltött pozíciójának megfelelő támogatás nyújtásának képessége egy kibertámadás kezelése során
A4*	kiberbiztonsággal, adatvédelemmel kapcsolatos képzések, oktatások megtartásának, lebonyolításának képessége
A5*	incidenskezelési eljárás hatékony lefolytatásának képessége
	Készség (S)
S1*	emberi tényezők kockázatán alapuló támadások felismerésének készsége
S2*	adatbiztonsági és kiberbiztonsági magatartás tanúsításának készsége

2-11. táblázat További feladatokhoz szükséges KSA elemek

2.6. KÖVETKEZTETÉSEK

Az előző alfejezetek egyfajta előkészítései és egyben bizonyításai voltak a hipotézisek megválaszolásának. Jelen fejezet célja, hogy az 2.1.1 fejezetben megadott hipotézisekre egyértelmű választ adhassak.

A H-2.1 hipotézis megfogalmazása során azzal a feltételezéssel éltem, hogy létezik különbség a magánszektor és a közszolgálat között kiberbiztonság szempontjából. Ennek igazolására strukturált interjú segítségével egy a közszférában és egy a magánszférában vezető tisztséget betöltő személlyel történő beszélgetés keretében vizsgáltam, hogy egyértelműen meghatározható-e különbség a magánszektor és a közszolgálat között kibervédelem szempontjából. Ez magában foglalja a személyek kiberbiztonsági képzését, a technológiai fejlesztések megvalósítását, a kiberbiztonsággal kapcsolatos financiális és stratégiai döntések meghozatalának szerepét és az egyes szervezetek kibervédelmi eszközeit, intézkedéseit. A hipotézis

cáfolatra került, mivel nem határozható meg egyértelmű különbség, tekintettel a két terület közötti átfedésre. Az interjúalanyok válaszait és az azokból levont következtetéseket a közszolgálati kiberbiztonsági képzés tartalmának kidolgozása során fogom felhasználni.

A H-2.2 hipotézis során vélelmeztem, hogy azonosítható egy célcsoport a közszolgálatban dolgozók köréből, akik számára szükséges lehet a közszolgálati kiberbiztonsági képzés. E hipotézis bizonyítására a közszolgálat fogalmának és komponenseinek vizsgálatával definiáltam a közszolgálati kiberbiztonsági képzés célcsoportjának elemeit és kivételi körét.

A H-2.3 hipotézis során abból a feltételezésből indultam ki, hogy a közszolgálatban dolgozó személyek számára meghatározható a szervezeti kiberbiztonság megvalósításához szükséges tudás-, képesség-, és ismerethalmaz. Ennek keretében azt vizsgáltam, hogy a közszolgálatban dolgozó személyek számára szükséges-e a NICE és ECSF Keretrendszer által és más egyéb nem e keretrendszerek által meghatározott ismeretkörök elsajátítása. Ennek érdekében először a korábban azonosított célcsoporthoz tartozó feladatokat definiáltam. Emellett meghatároztam azokat a tudás-, képesség- és készségelemeket, amelyeket szükséges átadni a közszolgálatban dolgozó személyeknek, hogy a NICE és ECSF keretrendszerek segítségével azonosított kiberbiztonsági feladataikat maradéktalanul elláthassák. A lefedetlen pontokat új, általam meghatározott a nemzetközi szakirodalmon és saját szakmai tapasztalataimon alapuló ismeretkörökkel bővítettem.

2.7. ÚJ TUDOMÁNYOS EREDMÉNYEK

Jelen fejezetben bemutatott kutatás alapján **azonosítottam a közszolgálati kiberbiztonság megvalósításához szükséges célcsoport és az általuk elsajátítandó tudáshalmaz (E2).**

E tudományos eredmény igazolásához kutatásom során az alábbi részeredményeket értem el:

Tudományos részeredmény 1. Nem határozható meg egyértelmű különbség a magánszektor és a közszolgálat között kiberbiztonság szempontjából

Tudományos részeredmény 2. Definiáltam a képzés tényleges célcsoportját.

Tudományos részeredmény 3. Azonosítottam az általános kiberbiztonsági feladatokat, valamint meghatároztam azokat a tudás-, képesség- és készségelemeket, amelyeket szükséges átadni a közszolgálati kiberbiztonsági képzés során.

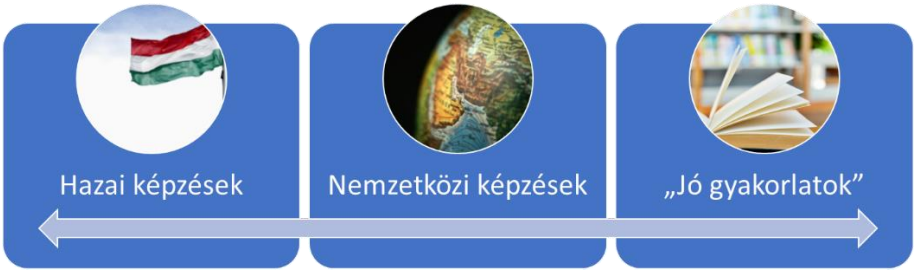
Jelen fejezet a [j2] és [f3] publikációkra épül, amelyek részletesen támasztják alá mind a három tudományos részeredményt. A [j2] folyóiratcikkben egy célzott mélyinterjú keretében vizsgáltam a köz- és magánszférában megvalósuló kibervédelem különbségeit. Az interjú lefolytatásának segítségével számos következtetést vontam le (pl. a kibervédelmi kockázatok mérséklése céljából a felhasználók tudatosítása és a technológiai fejlesztések szerepe), amelyek beépíthetők a közszolgálati kiberbiztonsági képzés tartalmába. Az [f3] publikációban azonosítottam a képzés célcsoportját, valamint az e csoporthoz tartozó feladatokat. Emellett azonosítottam a feladatok végrehajtásához szükséges ismeret-, tudás-, képesség-, és készséghalmazt, amelyek segítségével a szervezet kibervédelemmel összefüggő tevékenysége elvégezhető.

3. HAZAI ÉS NEMZETKÖZI KIBERBIZTONSÁGI KÉPZÉSEK ÖSSZEHASONLÍTÁSA

3.1. BEVEZETÉS

A közszolgálati szervezetek ellen elkövetett kibertámadások mára mindennapossá váltak. A támadások elsősorban belső és bizalmas információk megszerzésére, illetve a különféle szolgálatatások működésének korlátozására irányulnak. Annak érdekében, hogy e támadásokat a közszolgálatban dolgozók hatékonyan és eredményesen képesek legyenek elhárítani elengedhetetlen a kiberbiztonsággal kapcsolatos ismereteket átadó képzés biztosítása. Ennek megvalósítására a képzés típusától függően számos lehetőség áll a közszolgálatban dolgozók rendelkezésére.

Jelen értekezés alapjául szolgáló képzési program megalkotása során fel kell tárni a program megvalósíthatóságának lehetőségeit, illetve a hasonló hazai és nemzetközi képzéseket a képzés szükségességének igazolása és az esetleges hiányosságok feltárása, valamint a hazai és nemzetközi „jó gyakorlatok” átvétele érdekében (lásd 3-1. ábra).



3-1. ábra A fejezet tematikájának főbb elemei

3.1.1. HIPOTÉZISEK

Jelen fejezetben vizsgált hipotézis szerint **korábban még nem született a közszolgálat fejlesztését célzó, kibervédelmi képesség kialakítására és fejlesztésére irányuló gyakorlati képzési program hazánkban (H3)**. Ennek igazolására az alábbi alhipotéziseket azonosítottam, melyek megválaszolását tűztem ki célul jelen fejezetben bemutatom kutatásommal. Az alhipotézisek a következők:

H-3.1. A hazai felsőoktatási rendszerben jelenleg nem létezik olyan képzés, amely lefedi a közszolgálati kibervédelmi képesség kialakításához szükséges alapismereteket.

H-3.2. Definiálható egy kiválasztási módszer és összehasonlítási stratégia, amely alapján azonosíthatók a közszolgálathoz kapcsolódó nemzetközi kiberbiztonsági képzések és vizsgálható a hazai közszolgálati kiberbiztonsági képzés relevanciája nemzetközi szinten.

H-3.3. A hazai közszolgálati kiberbiztonsági képzés releváns felsőoktatási képzés lehet nemzetközi szinten is.

H-3.4. Fellelhetők olyan nemzetközi „jó gyakorlatok", amelyeket érdemes átültetni a hazai képzésbe.

3.1.2. FELHASZNÁLT KUTATÁSMÓDSZERTAN

A H-3.1 alhipotézis esetén dokumentumelemzés segítségével azt vizsgáltam, hogy jelenleg a magyarországi felsőoktatási rendszerben milyen kiberbiztonsággal, kibervédelemmel, információbiztonsággal kapcsolatos képzések léteznek és ezt követően feltérképeztem azok tartalmát, valamint azt, hogy az lefedi-e az előző fejezetben meghatározott képzéshez szükséges alapismereteket.

A H-3.2 alhipotézis esetén arra a kérdésre kerestem a választ, hogyan, milyen technikák segítségével célszerű azonosítani a nemzetközi képzéseket. Ennek megválaszolására definiáltam egy kiválasztási módszert, majd azt vizsgáltam, hogy milyen szempontok, elvárások, követelmények alapján érdemes összehasonlítani a feltárt nemzetközi képzéseket. E cél megvalósítására meghatároztam egy összehasonlítási stratégiát, illetve annak tartalmát, elemeit. Ezen belül dokumentumelemzés segítségével megvizsgáltam, hogy jelenleg a nemzetközi színtéren milyen kiberbiztonsággal, kibervédelemmel, illetve információbiztonsággal kapcsolatos képzések léteznek, ezt követően pedig azonosítottam azokat, és feltérképeztem ezek tartalmát, alapvető elemeit, követelményeit, valamint azt, hogy mennyiben fedi le a NICE és ECSF Keretrendszerben rögzített, általam kiválasztott kiberbiztonsági munkakörhöz kapcsolódó, a korábban meghatározott további ismerethalmazt, továbbá milyen további ismeretköröket tartalmaz.

A H-3.3 alhipotézis esetén a H-3.2 alhipotézisben meghatározott kiválasztási módszer alapján azonosított képzéseket a definiált összehasonlítási stratégia segítségével

hasonlítottam össze. Amennyiben a korábban definiált hazai közszolgálati kiberbiztonsági képzés során átadandó tudáshalmaz legfeljebb az adott országra jellemző tudásanyagban tér el a nemzetközi képzések során átadandó tudáshalmaztól, a képzés nemzetközileg is relevánsnak tekinthető.

A H-3.4 alhipotézis esetén meghatároztam a H-3.2 alhipotézis során feltárt nemzetközi képzések azon elemeit és gyakorlatait, amelyek átültethetők a hazai közszolgálati kiberbiztonsági képzésbe.

3.1.3. FEJEZET SZERKEZETE

Jelen fejezet a következő struktúrát követi. A 3.2 alfejezetben a témakörhöz kapcsolódó hazai és nemzetközi szakirodalmak kerülnek bemutatásra, majd ezt követően a 3.3 alfejezetben ismertetem az azonosított hazai kiberbiztonsággal összefüggő képzéseket. A 3.4 alfejezetben kerül sor a vonatkozó nemzetközi képzések összehasonlítására és a nemzetközi „jó gyakorlatok" azonosítására. A 3.5 és a 3.6 alfejezetek tartalmazzák a fejezet egészének következtetéseit, valamint az elért új tudományos eredményeket.

3.2. KAPCSOLÓDÓ SZAKIRODALMI ÁTTEKINTÉS

Ahhoz, hogy a hazai és nemzetközi kiberbiztonsággal összefüggő képzések feltárása megvalósulhasson, elengedhetetlen a kapcsolódó szakirodalom áttekintése.

3.2.1. HAZAI KIBERBIZTONSÁGI OKTATÁSSAL KAPCSOLATOS TANULMÁNYOK

Elsőkörben azon tanulmányokat vizsgáltam, amelyek a hazai kiberbiztonsági képzésfejlesztésre, a kiberbiztonsági és kibervédelmi képességek fejlesztésére összpontosítanak, illetve a kibervédelmi oktatás kérdéseire keresik a választ.

Az irodalomkutatás során mindenképp ki kell emelni Krasznay Csaba által elkészített *A kiberbiztonság stratégiai vetületeinek oktatási kérdései a közszolgálatban* című publikációt. A szerző rámutat számos olyan a kibertérben történő eseményre, amelyek kétségkívül hatással vannak a fizikai világra és rögzíti, hogy ezen eseményekre az ország védelmében részt vevő szervezeteknek reagálniuk kell. Éppen ezért elengedhetetlen olyan közszolgálati szakemberek alkalmazása és képzése, akik érdemben tudnak reagálni a műszaki és nem műszaki természetű kihívásokra egyaránt.

A szerző a tanulmányban áttekinti milyen kibervédelmi képességekre van szükség Magyarországon, illetve hogyan lehet ezeket megteremteni. Kibervédelmi képességek közé sorolható a kiberbiztonság általános megértésének képessége, incidensmenedzselési képesség, valamint a stratégiai, vezetői képességek. A szerző javaslatot tesz e képességek fejlesztésének lehetőségeire a hazai felsőoktatási rendszerben megvalósuló alap, mester- és továbbképzési szintű oktatás keretében. [23]

Nagyné Takács Veronika és Kovács László *Az információbiztonsági vezető szakirányú továbbképzés tapasztalatai* című publikációja rögzíti az információbiztonság jelentőségét és szabályozását, majd bemutatja a Nemzeti Közszolgálati Egyetem Elektronikus Információbiztonsági Vezető (a továbbiakban: EIV) szakirányú továbbképzésének tartalmát és értékelését, amelyet a szerzők a képzésen végzett hallgatók szakdolgozatának elemzésével végeztek el. Ezek alapján számos következtetést levonnak az EIV fejlesztését célozva, így például javaslatot fogalmaznak meg a képzés céljára és tartalmára, az egyénre szabottabb tanári támogatás biztosítására, illetve a heterogén oktatási csoportok létrehozására vonatkozóan. [24]

Som Zoltán Az információbiztonság fejlesztési lehetőségei az EIV képzésen keresztül című cikkében az EIV szakirányú továbbképzésének tapasztalatait és mérési eredményeit mutatja be, amelynek segítségével rávilágít a rendszerben rejlő fejlesztési lehetőségekre is. Ennek keretében személyes megfigyelésekkel és szabadszavas kérdőíveket töltettek ki az EIV képzésben résztvevőkkel, majd megvizsgálta, hogy milyen kockázatok merülhetnek fel a képzéssel kapcsolatban, illetve milyen intézkedéseket, ellenintézkedéseket kell megtenni a kockázatok csökkentése érdekében. Végül javaslatok határozott meg a képzés fejlesztésére, így például szakkollégium létrehozását, illetve egyéni kommunikációs képességek fejlesztését ajánlja. [25]

Simon Béla *Kiberbűnözés elleni képzésfejlesztés* című publikációjában áttekinti, hogy a jelenlegi hazai képzési, oktatási rendszerben mikor és milyen jellegű állami teendők jelentkeznek. A szerző azonosítja a kiberbűnözés elleni fellépés két fő oldalát, a megelőzési oldalát, valamint a már megvalósított bűncselekmények felderítésének, nyomozásának, bizonyításának és az elkövetők büntető igazságszolgáltatás általi felelősségre vonásának megvalósítását. Bemutatja a rendőri/rendészeti felsőoktatás

lehetséges, illetve tervezett fejlesztési irányainak lehetőségeit, a megrendelői igények összevetésével. [26]

3.2.2. NEMZETKÖZI KÉPZÉSEK ÖSSZEHASONLÍTÁSÁVAL KAPCSOLATOS TANULMÁNYOK

K. Cabaj és szerzőtársai tanulmánya összehasonlító elemzést nyújt számos kiberbiztonsági mesterképzésről, azok felvételi követelményeiről, alapadatairól, tartalmáról, valamint a kiberbiztonsági érettség lényegéről. A cikkben összesen 21 mesterképzést vizsgáltak meg, amelyek kiválasztási kritériumai a következők voltak: a mesterképzés elnevezésében szerepel a kiberbiztonság kulcsszó, valamint ezek a képzések a 2017-es QS Egyetemi Világranglista első 700 egyetemén elérhetők. A kiválasztás fontos további szempontja volt a földrajzi elhelyezkedés, amely alapján különböző országok képzéseit is összehasonlították, így tíz képzést az Egyesült Államokból, ötöt az Egyesült Királyságból, valamint egyet-egyet Ausztráliából, Új-Zélandról, Észtországból, Hollandiából, Izraelből és Spanyolországból elemeztek. Az összehasonlítás során megvizsgálták a képzések felvételi követelményeit, időtartamát, illetve struktúráját. Ez utóbbi során elemezték a képzések felépítését, a teljesítendő kreditek és kurzusok számát, azok típusait, tehát például azt, hogy van-e a hallgatóknak lehetőségük szabadon választható kurzusok felvételére, vagy kizárólag kötelező tantárgyakat abszolválhatnak-e, továbbá fellelhetők-e specializációk, szakirányok az egyes képzések esetében. Ezt követően a szerzők bemutatták a kurzusok tartalmát, illetve azon témákat, területeket, amelyeket az egyes képzések érintenek. Végezetül a képzések abszolválásához szükséges feltételeket elemzését végezték el. [27]

Bogdana Bystrova tanulmányában az Ukrajnában és az Egyesült Államokban elérhető kiberbiztonsági felsőoktatási képzések általános összehasonlítását ismerteti, amelynek célja a hasonló oktatási programok szervezésével, megvalósításával, tartalmával és tanulmányi eredményeivel kapcsolatos alapképzések gyakorlati tapasztalatainak felhasználása az ukrán kiberbiztonsági oktatásban. A szerző az Észak Karolina Állami Egyetem kiberbiztonsági alapképzését és az ukrán kiberbiztonsági képzéseket általánosságban hasonlította össze. Az amerikai képzés esetében a kiválasztás fő szempontja az volt, hogy a vizsgált egyetem a US News and World Report rangsorában az előkelő 31. helyet foglalta el a 150-ből. Bystrova ezt követően összehasonlította a

képzéseket a teljesítendő kreditek száma, a tanulási és oktatási módszertan, az értékelési folyamat, valamint a finanszírozási forma alapján. A szerző legfőbb célja az volt, hogy javaslatot tegyen az amerikai tapasztalatok alapján az ukrán kiberbiztonsági oktatás fejlesztésére, a hiányosságok és problémák orvoslására, az amerikai jó gyakorlatok átvételével. [28]

3.3. HAZAI KIBERBIZTONSÁGGAL KAPCSOLATOS KÉPZÉSEK

Jelen pontban azon kiberbiztonsággal kapcsolatos képzések kerülnek bemutatásra, amelyekre Magyarországon 2020 szeptemberében jelentkezni lehetett. Összesen tíz ilyen képzést azonosítottam, amelyek alapadatait a 3.3.2 alfejezetben taglalom. Ezt követően megvizsgáltam, hogy a képzés tantervében szerepelnek-e az előző fejezetben bemutatott NICE és ECSF Keretrendszer által, valamint az általam meghatározott szükséges alapismeretek, amelyeket a 3.3.3 alfejezetben részletezek.

3.3.1. A HAZAI KÉPZÉSEK BEMUTATÁSA

A bolognai folyamat részeként átalakult felsőoktatási képzési rendszer az alábbi fázisokból épül fel: *alapképzésből és mesterképzésből,* illetve az alap- vagy mesterképzés után egyaránt elvégezhető *szakirányú továbbképzésből*. A hazai kiberbiztonsági képzéseket e három csoport alapján mutatom be a következőkben. Ezen kívül számos további képzéstípus (tudatossági programok, továbbképzések, kurzusok stb.) biztosítja a kiberbiztonsági ismeretek átadását a közszolgálatban dolgozó személyek számára, azonban jelen tanulmány és az alábbi alfejezetek célja kizárólag a magyar felsőoktatási rendszerben megtalálható képzések összegyűjtése és bemutatása.

3.3.1.1. Alapképzési szakok

Az alapképzés általában 3-4 éves időtartamot felölelő képzési forma, amelyen tudományterülettől függően BA (Bachelor of Arts), illetve BSc (Bachelor of Science) fokozat szerezhető. E képzés során tulajdonképpen olyan széleskörű alapszintű ismeretek elsajátítása a cél, amely a munkaerőpiacon hasznosítható szakmai ismereteket és megfelelő elméleti alapozást nyújt az adott szakterületen a tanulmányok mesterképzésben történő folytatásához. [2011. évi CCIV. törvény]

Kiberbiztonsághoz kapcsolódó hazai alapképzések:

a) Nemzeti Közszolgálati Egyetem – Bűnügyi alapképzési szak – Kiber nyomozó szakirány (NKE KNY) [w8]
b) Óbudai Egyetem – Biztonságtechnikai mérnök alapképzési szak – Információbiztonsági specializáció (ÓE BM) [w10]

3.3.1.2. *Mesterképzési szakok*

A mesterképzés elvégzését követően MA (Master of Arts), illetve MSc (Master of Sciences) fokozat és szakképzettség szerezhető. Mesterképzésre az jelentkezhet, aki legalább egy alapképzési diplomával vagy a korábbi képzési rendszer szerinti főiskolai/egyetemi diplomával rendelkezik, de a felvétel pontos követelményeit és feltételeit a felsőoktatási intézmények maguk határozzák meg. A mesterképzés általában 2-4 féléves időtartamot ölel fel. Összességében megállapítható, hogy a mesterképzés során szakterület specifikus és mélyebb elméleti és gyakorlati ismeretek átadása a cél, mely elvégzését követően lehetőség van kilépni a munkaerőpiacra, illetve jelentkezni lehet a képzési rendszer harmadik lépcsőfokát jelentő doktori képzésre, amely a tudományos fokozat megszerzésére készít fel. [2011. évi CCIV. törvény]

Kiberbiztonsághoz kapcsolódó hazai mesterképzések:

a) Nemzeti Közszolgálati Egyetem – Kiberbiztonsági mesterképzés (NKE KB) [w9]
b) Nemzeti Közszolgálati Egyetem – Védelmi infokommunikációs rendszertervező – Információbiztonsági szakirány (NKE VIKR) [w17]

3.3.1.3. *Szakirányú továbbképzések*

Fontos megemlíteni a szakirányú továbbképzés szintjét is, amely a már korábban megszerzett alap- és mesterfokozatra, főiskolai vagy egyetemi szintű végzettségre épülő oklevelet adó, 2-4 félév időtartamú képzési forma. Olyan képzéstípus, amely speciális feladatok ellátására ad szakmai felkészítést, valamint lehetővé teszi a korábban szerzett ismeretek meghatározott irányú elmélyítését. Azonban fontos kiemelni, hogy az elvégzését követően megszerzett oklevél nem emeli a korábbi végzettség szintjét. [87/2015 Korm. rendelet]

Kiberbiztonsághoz kapcsolódó hazai szakirányú képzések:

a) Nemzeti Közszolgálati Egyetem – Elektronikus információbiztonsági vezető szakirányú továbbképzés (NKE EIB) [w15]
b) Nemzeti Közszolgálati Egyetem – Európai uniós adatvédelmi szaktanácsadó szakirányú továbbképzési szak (NKE EUA) [w16]
c) Eötvös Loránd Tudományegyetem – Adatbiztonsági és adatvédelmi szakjogász/szakember szakirányú továbbképzés (ELTE ASZ) [w6]
d) Óbudai Egyetem – Kiberbiztonsági szakmérnök/szakember szakirányú továbbképzés (ÓE KSZ) [w19]
e) Óbudai Egyetem – Információbiztonsági szakmérnök/szakember szakirányú továbbképzés (ÓE ISZ) [w18]
f) Gábor Dénes Főiskola – Adatvédelmi és információbiztonsági menedzser szakirányú továbbképzés (GDF AIM) [w11]

3.3.2. HAZAI KÉPZÉSEK ALAPADATAINAK VIZSGÁLATA

Az első összehasonlítás során a képzések alapadatait vizsgáltam meg, amelyet a 3-1. táblázat szemléltet. A táblázatban látható az egyes képzések időtartama (I.) félévekben megadva; a munkarend (M), ami lehet *nappali* (n), *levelező* (l), esetleg *mindkettő* (n/l); a finanszírozási forma (Fin.), amely alapján a képzés lehet *állami ösztöndíjjal támogatott* (öszt), *önköltséges* (önk) vagy *mindkettő* (öszt/önk), végül a bemeneti követelmények.

A vizsgálatból kiderül, hogy a vizsgált alapképzésekhez bár nincs szükség egyéb végzettségre, azonban megjelennek a jelentkezéshez szükséges további feltételek, mint például az alkalmassági vizsgálat, informatikai jártasság. Ezen kívül az egyes képzések további megszorításokat, követelményeket tartalmaznak azzal kapcsolatban, hogy milyen típusú előképzettségre van szükség, ahhoz, hogy a képzésen részt lehessen venni. Három képzés esetében (NKE VIKR, NKE EIB, NKE EUA) bármely képzési terület alapképzéses diplomáját elfogadják, míg a többi képzés esetében külön rögzítették a bemeneti követelmények konkrét képzési területeit, így például informatikai, műszaki, közigazgatási, jogi és számos további terület alapképzésen szerzett oklevele szükséges a felvételhez.

Az előképzettség a képzés abszolválásának körülményeit is jelentősen befolyásolja, így például más típusú bemeneti tudással rendelkeznek a műszaki és más a humán

területről érkező hallgatók, hiszen míg az utóbbi esetében az informatikai oktatás, addig az előbbi esetében a jogi, társadalomtudományi ismeretek elsajátítása okozhat nehézséget.

	KÉPZÉS	I.	M.	FIN.	BEMENETI KÖVETELMÉNY
BSC/ BA	NKE KNY	8	n	öszt	alkalmassági vizsgálatok + informatikai jártassági és készségvizsgálat
	ÓE BM	7	n/l	öszt/önk	érettségi bizonyítvány, meghatározott érettségi vizsgakövetelmények
MSC/ MA	NKE KB	4	n/l	öszt/önk	alapképzés + informatikai, államtudományi és társadalomtudományi ismeretek
	NKE VIKR	4	n/l	öszt/önk	alapképzés
SZAKIRÁNYÚ TOVÁBBKÉPZÉS	NKE EIB	2	l	önk	alapképzés
	ELTE ASZ	3	l	önk	szakjogász: állam- és jogtudomány képzés szakember: meghatározott alapképzések
	ÓE KSZ	4	l	önk	szakmérnök: mérnöki alapképzés szakember képzés: alapképzés
	ÓE ISZ	4	l	önk	szakmérnök: mérnöki alapképzés szakember képzés: alapképzés
	GDF AIM	2	l	önk	informatikai, műszaki, gazdaságtudományi, társadalomtudományi, pedagógusképzés, jogi, közigazgatási, rendészeti vagy katonai alapképzés
	NKE EUA	2	l	önk	alapképzés

3-1. táblázat Vizsgált hazai képzések alapadatai

Összességében megállapítható, hogy a jelenlegi felsőoktatási képzési rendszer minden szintjén elérhető kiberbiztonsággal, információbiztonsággal foglalkozó képzés. Fontos kiemelni, hogy a jelenlegi képzési rendszer fázisaiban átadott ismeretek mennyisége és mélysége eltérő, jelentősen befolyásolja azt a képzési forma struktúrája, követelményei, időtartama, valamint a képzés során elsajátítandó készségek, képességek, ismeretek halmaza.

3.3.3. HAZAI KÉPZÉSEK ISMERETHALMAZÁNAK VIZSGÁLATA

Miután bemutattam a hazai felsőoktatásban elérhető kiberbiztonsággal foglalkozó képzéseket, szeretném megvizsgálni, hogy létezik-e olyan képzés, mely fedi a 2.5.3 és

2.5.4 alfejezetekben azonosított ismeretek körét. Ehhez megvizsgáltam, hogy az egyes képzések oktatási anyaga tartalmaz-e részletes képzési anyagot a K1-K5 és K1*-K5* tudáshalmazzal kapcsolatban.

A vizsgálat során a képzések weboldalán található információkat, tematikákat és elérhető oktatási anyagokat vizsgáltam meg. Az elemzés eredményét a 3-2. táblázat tartalmazza, ahol a sorok az egyes képzéseket, az oszlopok az azonosított tudáshalmazt jelölik. Egy cellába akkor került ✓ jel, ha az adott sorban található képzés oktatja az adott oszlopban található ismeretanyagot. Ha egy cellába – jel került, akkor nem található információ azzal kapcsolatban, hogy az adott ismeretkört is oktatják az adott képzésen.

A vizsgált képzések közül a Nemzeti Közszolgálati Egyetem védelmi infokommunikációs rendszertervező mesterképzés információbiztonsági szakiránya fedi le a legtöbb korábban meghatározott tudáskört.

KÉPZÉSI FORMA	KÉPZÉS RÖVIDÍTÉSE	K1	K2	K3	K4	K5	K1*	K2*	K3*	K4*	K5*
BSC/ BA	NKE KNY	✓	-	✓	✓	✓	✓	-	✓	-	✓
	ÓE BM	✓	✓	✓	✓	-	-	-	✓	✓	✓
MSC/MA	NKE KB	✓	✓	✓	✓	-	-	-	-	✓	-
	NKE VIKR	✓	✓	✓	✓	✓	✓	✓	✓	✓	-
SZAKIRÁNYÚ TOVÁBB-KÉPZÉS	NKE EIB	✓	✓	✓	-	-	-	-	-	-	-
	ELTE ASZ	✓	-	✓	✓	-	-	✓	✓	-	-
	ÓE KSZ	✓	-	✓	✓	✓	-	-	-	-	-
	ÓE ISZ	✓	✓	✓	-	-	-	-	-	✓	-
	GDF AIM	✓	-	✓	-	-	-	-	✓	-	-
	NKE EUA	-	✓	✓	-	-	✓	✓	-	-	-

3-2. táblázat Hazai kiberbiztonsággal kapcsolatos képzéseinek összehasonlítása

Összességében megállapítható, hogy az általam meghatározott új tudáselemek mindegyike megjelenik valamely vizsgált képzés képzési tervében, amely azt mutatja, hogy ezen ismeretkörök a közszolgálati kiberbiztonsági képzés szempontjából

relevánsnak tekinthetők. A táblázat alapján egyébként az is látható, hogy kivétel nélkül, minden vizsgált képzés tantárgyi programjában szerepel a számítógép-hálózatokhoz kapcsolódó alapfogalmak oktatása.

Azonban egyértelműen kijelenthető, hogy a hazai felsőoktatási rendszerben jelenleg nem létezik olyan képzés, amely teljeskörűen lefedi a közszolgálati kibervédelmi képesség kialakításához szükséges alapismereteket, vagyis nincs olyan képzés, amely kellő mértékben és összhangban tartalmazná a szükséges közigazgatási, jogi és informatikai, műszaki ismeretanyagot. A közszolgálati kiberbiztonsági képzés elhatárolódik az állami és önkormányzati szervezetek információbiztonságáról szóló 2013. évi L. törvényben (a továbbiakban: Ibtv.) [2013. évi L. törvény] meghatározott, az elektronikus információs rendszer védelméért felelős személyek feladatellátáshoz szükséges felsőfokú végzettségtől, mivel nem egy konkrét pozícióra ad képesítést, hanem sokkal általánosabb tudást ad át a közszolgálatban dolgozó személyek számára.

3.4. A NEMZETKÖZI KÉPZÉSEK ÖSSZEHASONLÍTÁSA

A közszolgálati kiberbiztonsági képzés hazai megvalósításához mindenképp szükséges feltérképezni és megvizsgálni a nemzetközi oktatásban megjelenő kiberbiztonsággal, információbiztonsággal kapcsolatos képzéseket. Ezen belül e képzések rendszerét, struktúráját, felépítését és tartalmát, annak érdekében, hogy a nemzetközi tapasztalok vizsgálata során feltárt „jó gyakorlatok” esetleges átültetése megvalósulhasson a hazai oktatásban. Ennek keretében jelen pontban ismertetek néhány külföldi, a kibervédelmi képesség fejlesztését, illetve közszolgálati ismeretek átadását célzó képzési programot. Ezt követően az előző fejezetben felvázolt tudáshalmaz alapján összehasonlítom a kiválasztott nemzetközi példákat aszerint, hogy milyen mértékben jelenik meg a képzésben ezen ismeretek átadása.

3.4.1. A KÉPZÉSEK KIVÁLASZTÁSÁNAK MÓDSZERE

Ahhoz, hogy bizonyítsam a közszolgálati kiberbiztonsági képzés fontosságát, szükségességét és relevanciáját hazánkban, a nemzetközi képzések több típusát is megvizsgáltam, amelyet ezt követően összevetettem egy általam kialakított szempontrendszer alapján. A képzések kiválasztásának módszere a következőkben és a 3-2. ábra ismertetett lépésekből állt.

3-2. ábra: A képzések kiválasztásának módszere

A képzések három csoportját különítettem el. Az első csoportba sorolhatók a *kiberbiztonsággal, kibervédelemmel foglalkozó, informatikai előképzettségre épülő mesterképzések*. A második kategóriát a *közigazgatási mesterképzések* alkotják. A harmadik csoport esetén olyan képzéseket kívántam megvizsgálni, amely az általam a korábbiakban felvázolt, a *közszolgálatban dolgozó személyek számára biztosítja a kibervédelmi képesség kialakítását*. Olyan egyetemi szintű kiberbiztonsági mesterképzések, szakirányú továbbképzések után kutattam, amelyek konkrétan a közszolgálatban dolgozó személyeknek szólnak. Olyan képzést, amely teljesen megfelelne ezen elvárásoknak nem találtam, ezért olyan képzéseket kerestem, amelyek a *kiberbiztonság és a közigazgatás elemeit együttesen tartalmazzák*, így e képzések alkotják a harmadik csoportot.

A képzések felkutatására a QS World University Rankings által felállított világszintű egyetemi rangsort használtam. Honlapjukon megtalálható a világ egyetemeinek összesített rangsorolása, valamint a témánkénti és régiók szerinti rangsorok egyaránt. Ezen kívül a regisztrált felhasználók további információkhoz, elemzésekhez és közvetlen egyetemi összehasonlításokhoz is hozzáférhetnek.[5] Ezeknek köszönhetően a QS általános és téma szerinti rangsorait használtam a megfelelő képzések kiválasztásához. Ennek keretében bármely csoportot is vizsgáltam megnéztem az általános és téma szerinti (például informatikatudomány) rangsort és növekvő sorrendben elemeztem az egyetemeket azzal összefüggésben, hogy található-e a képzési repertoárjukban az általam éppen vizsgálni kívánt képzés. Ennek célja az volt,

[5] Bővebb információ a következő weboldalon található: https://www.topuniversities.com/university-rankings (University Rankings)

hogy mindig az adott ország azon képzését válasszam ki, amely megfelel az általam támasztott elvárásoknak és a ranglistának megfelelően a legjobbnak minősül az adott országban. Ennek érdekében kilistáztam azt általános és a téma szerinti rangsort, sorban haladva megvizsgáltam az országok egyetemeit és minden országból egyet választottam ki, amely megfelel a feltételeknek. Minden csoporthoz három egyetemet társítottam a könnyű áttekintés érdekében, majd pedig egy általam felvázolt szempontrendszer szerint vizsgáltam meg a képzéseiket. Minden egyetem esetében a feltételeknek leginkább megfelelő képzést választottam ki bővebb ismertetés céljából. Az adott képzések konkrét vizsgálatánál az egyetemek honlapjai és az azokon megtalálható tantervek, tájékoztató anyagok szolgáltak információval.

3.4.2. Összehasonlítási stratégia

A kiválasztást követően a képzések összehasonlítására, a NICE és ECSF Keretrendszer segítségével meghatározott tudáselemek képzési programban történő megjelenésére, a jó gyakorlatok azonosítására, valamint következtetések levonására az alábbi összehasonlítási stratégiát alkalmaztam.

A képzések kiválasztását követően minden egyes képzést ugyanazon szempontrendszer szerint vizsgáltam meg, annak érdekében, hogy áttekinthetőbbek legyenek, illetve a képzések bemutatását követően össze is lehessen hasonlítani sajátosságaikat és meg lehessen határozni előnyeiket, hátrányaikat. Minden képzés esetében vizsgáltam a képzés rangsorban betöltött helyét, pontos nevét, időtartamát, illetve a költségtérítés formáját. Ezt követően elemeztem a képzés feltételeit, a bemeneti követelményeket. Ez azért rendkívül fontos, mert például az első csoportban szereplő képzésekre kizárólag az informatikai, matematikai tudományok vagy ezekhez szorosan kapcsolódó képzési területen, alapképzésben szerzett oklevél birtokában lehet jelentkezni. Ezen kívül számos a nemzetközi képzésekre jellemző egyéb feltétel került meghatározásra, mint például az igazolt angol nyelvtudás, GRE/GMAT teszt[6], a közigazgatási mesterképzések esetében pedig a munkatapasztalat és az ajánlólevél. Ezen kívül megvizsgáltam a képzés típusát, az oktatott tantárgyakat, valamint azok tartalmát, az elsajátítandó készségeket, képességeket. Ezután összehasonlítottam a képzéseket az alapján (lásd 3-3. ábra), hogy tantárgyi programjuk milyen mértékben

[6] A nemzetközi egyetemeken felvételi kritériumként alkalmazott szabványosított tesztek, amelyek az alkalmasság felmérése szolgálnak.

tartalmazza a korábban a NICE és ECSF Keretrendszer segítségével definiált tudáshalmazt. A vizsgálat során a képzés weboldalán található információkat, tematikát és elérhető oktatási anyagokat elemeztem és egy táblázat segítségével szemléltettem, hogy az egyes képzések melyik tudáselemet tartalmazzák.

3-3. ábra: Összehasonlítási stratégia

3.4.3. A NEMZETKÖZI KÉPZÉSEK FELTÉRKÉPEZÉSE

Három csoportot azonosítottam a nemzetközi képzések feltérképezése során. Az első csoportba az informatikai alapképzettségre épülő kiberbiztonsággal foglalkozó mesterképzések tartoznak. A második csoportba a klasszikus közigazgatási mesterképzések sorolhatók. A harmadik csoport esetén olyan képzéseket kutattam, amelyek az általálam felvázolt közszolgálati kiberbiztonsági képzéssel hasonlóságot mutatnak.

3.4.3.1. Informatikai alapképzettségre épülő kiberbiztonsággal foglalkozó mesterképzések

A képzések felkutatásához a QS World University Rankings informatikatudományok alapján történő rangsorolását vettem figyelembe. A ranglista 17. helyén a *University College of London (UCL)* található, amely a ranglista első, informatikai alapképzettségre épülő kiberbiztonsági képzéssel rendelkező egyeteme. Ezen a képzésen kiberbiztonsági szakértők a tudományosan alátámasztott elméleti ismereteket és a legmodernebb gyakorlati tudás egyensúlyát tanítják az újdonsült szakemberek számára. [w23] A rangsorban a 18. helyet elfoglaló *Washingtoni Egyetem (University of Washington – UW)* a következő olyan egyetem, amely rendelkezik az informatikai előképzettség meglétéhez kötött kiberbiztonsággal

foglalkozó mesterképzéssel. Kétéves kiberbiztonsági mérnök mesterképzésre jelentkezhet az, aki kiberbiztonsági szakemberré szeretne válni, és aki a technológia fejlődésével lépést tartva kívánja kombinálni az informatikai alapismereteket a modern kiberbiztonsági technológiák elméleti ismereteivel és gyakorlati tapasztalataival. [w24] A rangsor 51-100 helyei közé sorolt hollandiai *Eindhoveni Műszaki Egyetem (Eindhoven University of Technology - EUT)* szintén kétéves mesterképzést biztosít az érdeklődők számára. Az információbiztonsági technológiák néven futó mesterképzés partnerintézményen, a Radboud Egyetemen keresztüli együttműködés keretében valósul meg. Ez a program széles körű áttekintést nyújt az információbiztonsági technológiák módszereiről, amely magában foglalja a jog, a kiberbiztonság, az etika és az üzleti tevékenységek egyes szempontjait is.[w5]

3.4.3.2. *Klasszikus közigazgatási mesterképzések*

E képzések kutatására a közpolitika és közigazgatás téma szerinti rangsort alkalmaztam. A ranglista 1. helyén álló amerikai *Harvard Egyetemen tagintézménye a Harvard Kennedy School (HU HKS)* irányítása alá tartozó kétéves, szakmai tapasztalatra épülő közigazgatási mesterképzést indít, amely során a hallgatók egyéni tanulmányi terv segítségével fejleszthetik tudásukat, összpontosíthatnak személyes és szakmai törekvéseikre, valamint ismereteket szerezhetnek a különféle tudományágakról. A Harvard kurzusain a kibervédelem számos területével találkozhatnak a hallgatók, többek között a digitális kormányzattal, kiberbiztonság technológiai, politikai és jogi aspektusával, valamint a kibertér és az információs műveletek kapcsolatának vizsgálatával is. [w12] A ranglista 3. helyén található angliai *London School of Economics and Political Science (LSE),* rövidebben London School of Economics egy 19 hónapos közigazgatási mesterképzést biztosít az érdeklődők számára. A képzés célja a kormányzati és állami szervek, közintézmények és a magánszektor szakemberei számára olyan tudásfejlesztés megvalósítása, amely ötvözi az egyéni és csoportos munkatapasztalon alapuló problémamegoldást a közszférában és a politikában egyaránt. A képzés tantervében kibervédelmi vonatkozások is megfigyelhetők, de kizárólag a kiberbiztonság jogi hátterének vizsgálatával kapcsolatban. [w13] A rangsor első tíz helyén egy kivétellel angol és amerikai egyetemek váltakoznak. A 7. helyen a *Tokiói Egyetem,* amely kizárólag közpolitika témájú angol nyelvű mesterképzéssel rendelkezik. A 11. helyet az *Ausztrál Nemzeti Egyetem (The Australian National University - ANU)* foglalja el. Kétéves

mesterképzés teszi lehetővé a tágan értelmezett közigazgatás megismerését azok számára, akik az állami, kormányzati szervekben szeretnének elhelyezkedni. A képzés kurzusai között kiberbiztonsági vonatkozásúról nem esett szó, de az ANU Kibervédelmi Intézete lehetőséget biztosít a kiberbiztonsággal mélyebben foglalkozni kívánó hallgatók számára. [w2]

3.4.3.3. *Közigazgatási és kiberbiztonsági ismereteket egyaránt tartalmazó képzések*

Végül olyan képzéseket kutattam, amelyek az általálam felvázolt közszolgálati kiberbiztonsági képzéssel hasonlóságot mutatnak, tehát a közszolgálatban dolgozó szakemberek számára nyújtanak kibervédelmi ismereteket. Összességében megállapítható, hogy az ehhez hasonló képzések száma rendkívül alacsony, konkrét közszolgálati dolgozók számára kiberbiztonsági felsőoktatási képzést nem találtam, ezért olyan képzéseket kerestem, amelyek együttesen ötvözik a közigazgatási és kiberbiztonsági ismeretek elsajátítását. Éppen ezért az ebbe a csoportba tartozó képzéstípusok alacsony számának köszönhetően, nem volt lehetőség eltérő országok képzéseit vizsgálni. Az első ilyen képzés az amerikai *Arizonai Állami Egyetem (Arizona State University – ASU)* kiberbiztonsági politika és menedzsment online elvégezhető mesterképzése, amely egyaránt ötvözi a kiberbiztonsági és a közigazgatással, közpolitikával kapcsolatos ismereteket.[w1] A következő ilyen a San Bernardino-ban található *Kaliforniai Állami Egyetem (California State University, San Bernardino – CSUSB)* olyan kétéves közigazgatási mesterképzést nyújt, amelyen kiberbiztonsági szakirány választható, és amelynek célja, hogy a közszolgálatban vezető szerepek betöltésére készítse fel a hallgatókat. [w3] Ezt követi a szintén amerikai *Carnegie Mellon Egyetem (Carnegie Mellon University – CMU),* ahol információbiztonsági politika és menedzsment szakirányú továbbképzéssel biztosítják az információbiztonsági és közigazgatási, közpolitikai ismeretek elsajátítását. Jelen képzés célja, hogy olyan szakembereket képezzen, akik képesek lesznek az állami és magánszféra szervezeteit, valamint más személyeket biztonságosabbá, biztonságtudatosabbá tenni. Míg más programok az információbiztonság technikai, mérnöki megközelítéseit hangsúlyozzák, addig e képzés a technikai készségeket, a közpolitikai, szakpolitikai, stratégiai és menedzsment kurzusok körével ötvözi. [w4]

3.4.4. NEMZETKÖZI KÉPZÉSEK ALAPADATAINAK VIZSGÁLATA

Az összehasonlítás során a képzések alapadatait vizsgáltam meg, melyet a 3-3. táblázat szemléltet. A táblázatban látható, hogy az egyes képzések időtartama (I.) években megadva; a rangsorban betöltött helyezés (R), amely szám mögött található a rangsor típusa, ami lehet *informatikai tudományok* (I), *közigazgatás és közpolitika* (K), esetleg *általános* (Á); a finanszírozási forma (Fin.), amely alapján a képzés lehet *állami ösztöndíjjal támogatott* (öszt), *önköltséges* (önk) vagy *mindkettő* (öszt/önk), végül a bemeneti követelmények.

Fontos kiemelni, hogy természetesen léteznek egyéb a közszolgálatban dolgozó személyek számára elérhető továbbképzések, tréningek, különféle oktatások, azonban jelen kutatás célja ezen vonatkozásban kizárólag a felsőoktatási képzési rendszerbe illeszkedő képzéstípusok elemzése

	KÉPZÉS	I.	R.	FIN.	BEMENETI KÖVETELMÉNY
INFORMATIKAI ALAPKÉPZETTSÉGRE ÉPÜLŐ KIBERBIZTONSÁGI KÉPZÉSEK	UCL	1	17 (I)	önk.	Informatikai. elektronikai mérnöki és matematikai területeken alapképzésben szerzett oklevél, angol nyelvtudás (pl. IELTS, TOEFL)
	UW	2	18 (I)	önk.	Informatikai területen alapképzésben szerzett oklevél, angol nyelvtudás, 3,0 feletti görgetett átlag
	EUT/RU	2	51-100 (I)	önk.	Informatikai, matematikai, információ-biztonság vagy kapcsolódó területeken alapképzésben szerzett oklevél, külföldi hallgatók esetében az alapképzésben szerzett oklevél egyedileg kerül elbírálásra, személyes interjú
KLASSZIKUS KÖZIGAZGATÁSI MESTERKÉPZÉSEK	HU HKS	1	1 (K)	önk	alapképzésben szerzett oklevél + 4 mesterképzési szakon indított kurzus teljesítése/mesterképzésben szerzett oklevél, 3 év szakmai tapasztalat, GRE/GMAT teszt, angol nyelvtudás
	LSE	1,5	3 (K)	önk	alapképzésben szerzett oklevél, 2 ajánlólevél, magas szintű angol nyelvtudás, 5 év munkatapasztalat
	ANU	2	11 (K)	önk.	alapképzésben szerzett oklevél, szakmai tapasztalat, 7 pontos GPA, angol nyelvtudás
KÖZSZOLGÁLAT+ KIBERBIZTONSÁG	ASU	2	215 (Á)	önk	kriminológia, igazságügyi igazgatás, közigazgatás, közszolgálat, szociológia, közbiztonsági/tűzvédelmi menedzsment, környezetvédelem, közegészségügy, alkalmazott tudományok, földrajz vagy más szorosan kapcsolódó területen alapképzésben szerzett oklevél, 2 éves szakmai tapasztalat, 2 ajánlás, 3,00 GPA, angol nyelvtudás
	CSUSB	2	-	önk	alapképzésben szerzett oklevél, szakmai tapasztalat, statisztikai előképzettség (bevezető kurzus)
	CMU HC	2	48 (Á)	önk.	alapképzésben szerzett oklevél, szakmai tapasztalat, angol nyelvtudás (TOEFL, IELTS), GRE teszt

3-3. táblázat: A vizsgált nemzetközi képzések alapadatai

3.4.5. NEMZETKÖZI KÉPZÉSEK ISMERETHALMAZÁNAK VIZSGÁLATA

Miután bemutattam a nemzetközi felsőoktatásban elérhető kiberbiztonsággal foglalkozó képzéseket, szeretném megvizsgálni, hogy létezik-e olyan képzés, mely fedi a 2.5.3 és 2.5.4 alfejezetekben azonosított ismeretek körét. Ehhez megvizsgáltam, hogy az egyes képzések oktatási anyaga tartalmaz-e részletes képzési anyagot a K1-K5 és K1*-K5* tudáshalmazzal kapcsolatban.

A vizsgálat során a képzések weboldalán található információkat, tematikákat és elérhető oktatási anyagokat vizsgáltam meg. A vizsgálat eredményét a 3-4. táblázat tartalmazza, ahol a sorok az egyes képzéseket, az oszlopok az azonosított tudáshalmazt jelölik. Egy cellába akkor került ✓ jel, ha az adott sorban található képzés oktatja az adott oszlopban található ismeretanyagot. Ha egy cellába ━ jel került, akkor nem található információ azzal kapcsolatban, hogy az adott ismeretkört is oktatják az adott képzésen.

KÉPZÉSI FORMA	EGYE-TEM	K 1	K 2	K 3	K 4	K 5	K1*	K2*	K3*	K4*	K5*
INFORMATIKAI ALAPKÉPZETTSÉGRE ÉPÜLŐ KIBER-BIZTONSÁGI KÉPZÉSEK	UCL	✓	✓	-	✓	✓	-	-	✓	✓	-
	UW	✓	-	-	✓	✓	-	-	✓	✓	-
	EUT/RU	✓	✓	✓	✓	✓	-	-	✓	-	✓
KLASSZIKUS KÖZIGAZGATÁSI MESTERKÉPZÉSEK	HU HKS	-	✓	✓	✓	-	-	-	-	-	-
	LSE	-	-	✓	-	-	-	-	-	-	-
	ANU	-	✓	-	-	-	-	-	-	-	-

KÖZSZOLGÁLAT+ KIBERBIZTONSÁG	CSUSB	✓	✓	-	✓	✓	-	-	✓	✓	-
	CMU	✓	✓	✓	✓	✓	-	-	✓	-	✓
	ASU	✓	-	✓	-	-	-	-	✓	-	-

3-4. táblázat: A vizsgált nemzetközi képzések összehasonlítása

A vizsgált képzések közül a University College of London információbiztonsági mesterképzése, az Eindhoven University of Technology információbiztonsági technológiák mesterképzése, a California State University közigazgatási mesterképzés kiberbiztonsági szakiránya, valamint a Carnegie Mellon University Heinz College információbiztonsági politika és menedzsment mesterképzése fedi le a legtöbb korábban meghatározott tudáshalmazt. Több különböző ország képzése is kifejezetten nagy mértékben tartalmazza a vizsgált témaköröket, ami azt jelenti, hogy egy kiberbiztonsági képzés, amely ezen ismereteket tartalmazza nemcsak hazánkban, hanem nemzetközi szinten is relevánsnak tekinthető.

A nemzetközi szinten elérhető klasszikus közigazgatással kapcsolatos mesterképzések többségében nem tartalmaznak kiberbiztonsági ismereteket. Ez azt a nemzetközi gyakorlatot szemlélteti, hogy a kiberbiztonsági ismereteket nem a klasszikus közigazgatási mesterképzésekbe kell integrálni, hanem külön kiberbiztonság-specifikus képzéseket kell létrehozni, amely ötvözi a közszolgálati és kiberbiztonsági ismereteket egyaránt.

Összességében megállapítható, hogy a korábban meghatározott tudáselemek jelentős része (két elem kivételével az összes) megjelenik valamely vizsgált képzés képzési tervében, amely azt mutatja, hogy ezen ismeretkörök a közszolgálati kiberbiztonsági képzés szempontjából is relevánsnak tekinthetők. A táblázat alapján egyébként az is látható, hogy nincs olyan tudáselem, amely minden vizsgált képzés tantárgyi programjában szerepelne. Ez mutatja a képzések felépítésének, meghatározott előképzettségeinek, feltételeinek és típusainak különbségét.

Fontos kiemelni, hogy a jelenlegi képzési rendszer fázisaiban átadott ismeretek mennyisége és mélysége eltérő, jelentősen befolyásolja azt a képzési forma struktúrája, követelményei, időtartama, valamint a képzés során elsajátítandó készségek, képességek, ismeretek halmaza. Ezen kívül befolyásoló tényezőnek

tekinthető a képzés munkarendje is, tehát, hogy a hallgatók nappali, levelező vagy online munkarendben teljesítik az adott képzést.

3.4.6. NEMZETKÖZI JÓ GYAKORLATOK AZONOSÍTÁSA

A közszolgálati kiberbiztonsági képzés hazai megvalósításához elengedhetetlen feltérképezni és megvizsgálni a nemzetközi oktatásban megjelenő kiberbiztonsággal, információbiztonsággal kapcsolatos képzéseket, azok struktúráját, tartalmát és tapasztalatait. Az előző pontban bemutatott képzések összehasonlító elemzése során számos „jó gyakorlatot" azonosítottam, amelyeknek átültetése a hazai képzésbe jelentősen hozzájárulhat a nemzetközi szintű képzés definiálásához. A feltárt jó gyakorlatokat a következőkben ismertetem.

A cél az volt, hogy olyan nemzetközi gyakorlatokat azonosítsak, amelyek bizonyíthatóan hozzájárulnak az adott felsőoktatási intézmény minőségi színvonalának emeléséhez. Éppen ezért olyan eljárásokat, eszközöket, módszereket és egyéb gyakorlatokat kerestem, amelyek pozitívan képesek befolyásolni a hatékony elméleti és gyakorlati tudásátadást. A nemzetközi tapasztalatok implementálásának előnye, hogy ezek már olyan nemzetközi színtéren kipróbált és bevált gyakorlatok, amelyek hatékonyságát az egyetemek eredményei is igazolnak. Fontos azonban megemlíteni, hogy komplex oktatási rendszerek integrálása nem minden esetben valósítható meg egy az egyben, mivel minden országnak, így azok felsőoktatási rendszereinek is más és más sajátosságai, hátterei, követelményei és társadalmi, gazdasági viszonyai vannak. Éppen ezért fontos, hogy a saját körülményeinket, felsőoktatási rendszereink felépítését, működését figyelembe véve szükséges e tapasztalatokat adaptálni. A „jó gyakorlatok" implementálása során kiemelt figyelmet kell fordítani azok technikai, szervezési és anyagi feltételeire is, csak ezek tisztázását követően kezdődhet meg ezek alkalmazása. A nemzetközi gyakorlatok átültetését követően kulcsfontosságú ezek hatékonyságának ellenőrzése és értékelése, valamint a tapasztalatok folyamatos rögzítése.

Az azonosított jó gyakorlatok az alábbiak:

a) hallgatók és tanárok, karok, intézetek közötti szoros kapcsolattartás;
b) hallgatók közötti együttműködés;
c) gyakorlati oktatás, labor;
d) gyakorlati projektmunka;

e) esettanulmányok segítségével történő oktatás;
f) állami vagy magánszférában dolgozó kiberbiztonsággal foglalkozó szakértők meghívott előadóként való részvétele az oktatásban.

A jó gyakorlatok közé tartozik a hallgatók és a tanárok, karok, illetve intézetek, tanszékek között szoros kapcsolattartás elősegítése, folyamatos biztosítása. Ennek célja, hogy a hallgatók félévi munkája során felmerülő problémák, nehézségek leküzdésében, valamint a munka folytatásában megfelelő szakmai segítséget kaphassanak.

A következő tapasztalat szorosan kapcsolódik az előbb említetthez, hiszen lényege, hogy a hallgatók megfelelő támogatást kapjanak tanulmányaikhoz. A hallgatók közötti együttműködés erősítésének célja, hogy fejlessze a hallgatók együttműködő-képességét, valamint a saját ötletek csoportban történő megosztásával hozzájáruljon a gondolkodás és a megértés elmélyítéséhez.

A gyakorlati oktatás, illetve labormunkák előnye, hogy a hallgatók a magán- és állami szférában felmerülő konkrét problémákkal, feladatokkal találkozhatnak, így valódi és releváns szakmai tapasztalatot szerezhetnek. Ezen kívül a kiberbiztonsággal összefüggő ismeretek elsajátítása során elengedhetetlen a különféle infokommunikációs technológiák, támadási és védelmi alternatívák konkrét műszaki környezetben történő szimulálása. Így e gyakorlati feladatok és laborgyakorlatok nélkülözhetetlen részét képezik a kiberbiztonsági oktatásnak.

A gyakorlati projektmunka lényege egy informatikára, kiberbiztonságra specializálódott projekt képzés végén történő végrehajtása, mely során egy valós ügyféllel, szervezettel történő együttműködés keretében egy aktuális problémára, kihívásra keresik a hallgatók a választ.

Az esettanulmányok segítségével történő oktatás számos egyetemre jellemző sajátosság, amelynek lényege, hogy egy konkrét, gyakorlati példa segítségével szemléltesse az átadni kívánt ismeretanyagot, valamint egy adott kihívás, probléma megoldásának lehetőségeit a hallgatók számára. Ezen oktatási módszer előnyei, hogy fejleszti a hallgatók problémamegoldó, analitikus, érvelési és együttműködési képességeit, továbbá hozzájárulnak valós gyakorlati problémák megismeréséhez.

Az aktuális kiberbiztonsági kihívások szemléltetését számos egyetem állami vagy magánszférában dolgozó kiberbiztonsággal foglalkozó szakértők meghívott

előadóként való részvételével biztosítja. E módszer szintén hozzájárul a valós, gyakorlati problémák és azok megoldásainak megismeréséhez, valamint a munkaerőpiacon szerzett tapasztalatok megosztásához.

3.5. KÖVETKEZTETÉSEK

Jelen fejezetben ismertetett kutatás egyfajta előkészítése és egyben bizonyítása volt a 3.1.1 alfejezetben meghatározott alhipotézisek megválaszolásának.

A H-3.1 alhipotézis esetén azzal a feltételezéssel éltem, hogy a hazai felsőoktatási rendszerben jelenleg nem létezik olyan képzés, amely lefedi a közszolgálati kibervédelmi képesség kialakításához szükséges alapismereteket. Ennek érdekében a többek között a hazai felsőoktatási képzésekről tájékoztatást nyújtó felvi.hu portál segítségével feltártam a 2020 szeptemberében induló kiberbiztonsággal kapcsolatos képzéseket. Az egyes képzések képzési, illetve tantárgyi programjai segítségével bemutattam azok alapvető jellemzőit, a képzéseket csoportosítottam a többciklusú bolognai rendszer fázisai alapján, és megvizsgáltam, hogy az egyes képzések tartalmazzák-e az első hipotézisben meghatározott tudáselemeket. Ez alapján megállapítható, hogy a második hipotézis igaznak bizonyul, hiszen egyik képzés sem fedte le maradéktalanul a szükséges alapismereteket.

A H-3.2 alhipotézis alapján vélelmeztem, hogy definiálható egy kiválasztási módszer és összehasonlítási stratégia, amely alapján azonosíthatók a közszolgálathoz kapcsolódó nemzetközi kiberbiztonsági képzések és vizsgálható a hazai közszolgálati kiberbiztonsági képzés relevanciája nemzetközi szinten. E hipotézis bizonyítása a 3.4.2 alfejezetben meghatározott keresési stratégia és összehasonlítási szempontrendszer, amely alapján kiberbiztonsággal kapcsolatos nemzetközi képzések a célnak megfelelően összehasonlítók.

A H-3.3 alhipotézis azon a feltételezésen alapul, hogy a hazai közszolgálati kiberbiztonsági képzés releváns felsőoktatási képzés lehet nemzetközi szinten is. Ennek teljesülését bizonyítja az 3.4 alfejezetben található, a vizsgált nemzetközi képzések ismerethalmazának vizsgálatán alapuló összehasonlítás (3-4. táblázat), amelynek eredményeként megállapítható, hogy egy hazai közszolgálati kiberbiztonsági képzés a nemzetközi szinten is releváns képzésnek minősül, hiszen a korábban meghatározott tudáselemek jelentős része (két elem kivételével az összes)

megjelenik valamely vizsgált képzés képzési tervében. Csak azon ismeretkörök nem jelennek meg (K1* és K2*), amelyek nemzetspecifikusak, országonként eltérőek.

Végül a H-3.4 alhipotézis, amely szerint fellelhetők olyan nemzetközi „jó gyakorlatok", amelyeket érdemes átültetni a hazai képzésbe, szintén igaznak bizonyult, ennek bizonyítása a 3.4.6 alfejezetben található meg, vagyis fellelhetők olyan nemzetközi jó gyakorlatok, amelyeket érdemes átültetni a hazai képzésbe.

3.6. ÚJ TUDOMÁNYOS EREDMÉNYEK

Jelen fejezetben **bizonyítottam, hogy szükséges egy olyan eddig még nem létező képzési program megalkotása a hazai képzési környezetben, amely lehetőséget nyújt a közszolgálatban dolgozó, nem informatikai végzettségű személyek kibervédelmi képességének kialakítására (E3)**. Mindemellett igazoltam, hogy a közszolgálati kiberbiztonsági képzés nemzetközi szinten is releváns képzésnek tekinthető. A vizsgált képzések képzési tervében szinte az összes korábban definiált tudáselem megjelenik, amely azt mutatja, hogy ezen ismeretkörök a közszolgálati kiberbiztonsági képzés esetében is helytállók.

Jelen fejezetben bemutatott kutatás alapján az alábbiakat tekintem új tudományos részeredménynek:

Tudományos részeredmény 1. Definiáltam a nemzetközi képzések feltérképezéséhez szükséges kiválasztási módszert.

Tudományos részeredmény 2. Meghatároztam a képzések összehasonlító elemzésére szolgáló összehasonlító stratégiát,

Tudományos részeredmény 3. Megvizsgáltam a feltárt nemzetközi képzések tartalmát, elemeit és követelményeit, ez alapján pedig azonosítottam e képzések „jó gyakorlatait".

Jelen fejezet az [f2] és [f3] publikációkra épül, amelyek részletesen támasztják alá mind a három tudományos részeredményt. Az [f2] folyóiratcikk keretében a hazai felsőoktatási rendszerben elérhető kiberbiztonsággal kapcsolatos képzéseket, valamint azok tartalmát mutattam be, amely során arra a kérdésre kerestem a

választ, hogy az egyes képzések tartalmazzák-e a korábban definiált tudáselemeket. Az [f3] publikációban azonosított nemzetközi képzések feltérképezéséhez szükséges kiválasztási módszer segítségével azonosítottam és összehasonlítottam a releváns nemzetközi képzéseket, valamint meghatároztam azok tartalma és a kapcsolódó nemzetközi tapasztalatok alapján e képzések „jó gyakorlatait”.

4. KÖZSZOLGÁLATI KIBERBIZTONSÁGI KÉPZÉS

4.1. BEVEZETÉS

A korábbiakban már számos alkalommal került hangsúlyozásra a kiberbiztonság aktualitása, a megfelelő szintű és minőségű védelmi intézkedések megléte, kivitelezése, valamint a felhasználók folyamatos tudatosítása, képzése, köszönhetően a támadások egyre gyakoribb és kifinomultabb megvalósításának. Nincs ez másként a közszolgálatban sem, ahol a közszolgáltatások zavartalan működése és az állampolgárok bizalmának megtartása érdekében még inkább előtérbe kerül a proaktív és reaktív kiberbiztonsági intézkedési rendszer kiépítésének igénye. Ennek alapvető eleme a szervezetben dolgozók kibervédelmi képességeinek kialakítása, folyamatos fejlesztése és erősítése a tartós kibertérből érkező fenyegetések elleni hatékony védelem kialakításához. E képességek szervezeti és személyi szinten történő biztosításához elengedhetetlen a tudatosító képzések szervezett formában történő lebonyolítása, így például képzési programok kidolgozása.

Mindemellett a kiberbiztonsággal, információbiztonsággal foglalkozó szakemberek hiánya indokolttá teszi e terület képzési programjának kidolgozását a közszolgálat fejlesztése érdekében. Az előző fejezetben igazolásra került a közszolgálatban dolgozó, nem informatikai végzettségű személyek kibervédelmi képességének kialakítására irányuló képzési program kidolgozásának szükségessége.

4.1.1. HIPOTÉZISEK

Jelen fejezetben vizsgált hipotézis szerint azzal a feltételezéssel éltem, hogy **definiálható egy olyan, a közszolgálat fejlesztését célzó képzési program, amelynek teljesítése nem igényel informatikai előképzettséget (H4).** Ennek igazolására az alábbi alhipotéziseket azonosítottam, amelyek megválaszolását tűztem ki célul jelen fejezetben bemutatom kutatásommal. Az alhipotézisek a következők:

H-4.1. Definiálható a magyar közszolgálat számára egy felsőoktatási kiberbiztonsági képzés.

H-4.2. Definiálható a képzés alapvető elemét képező struktúra, tantervi háló és értékelési rendszer.

H-4.3. Mérhető egy tantárgy oktatása során megvalósuló tudásátadás hatékonysága, valamint definiálható egy szempontrendszer, amely alapján osztályozható, hogy a tantárgy keretében átadott tudás kellően részletes-e.

4.1.2. FELHASZNÁLT KUTATÁSMÓDSZERTAN

A H-4.1 alhipotézis igazolására a korábban azonosított tudás-, képesség-, készséghalmazra, valamint a vizsgált hazai és külföldi képzésekre építve definiálom a közszolgálati kiberbiztonsági képzést, továbbá annak tartalmát és alapvető elemeit, bemeneti, kimeneti követelményeit.

A H-4.2 alhipotézis esetén definiáltam a közszolgálati kiberbiztonsági képzés struktúráját és felépítését, amelynek keretében meghatároztam a képzés elméleti és gyakorlati részének komponenseit, a főbb tárgyköreit. Emellett definiáltam a képzés tantervi hálóját, valamint az általános értékelési rendszer alapjait.

A H-4.3 alhipotézis igazolására egy valós tantárgy oktatása során megvalósuló tudásátadás hatékonyságát mértem, amely esetén vizsgáltam azt is, hogy az oktatott ismeretanyag elegendő-e a NICE és ECSF Keretrendszerben meghatározott képességek elsajátítására és a Certified Information Systems Security Professional (CISSP) képesítés[7] megszerzésére. Továbbá definiáltam egy szempontrendszert, amely az előzőekben említett hatékonyság alapján osztályozni tudja az egyes témaköröket az alábbiak tekintetében:

a) mélyebb tudás átadása szükséges,

b) a témakör kellően részletes,

c) a témakör egyszerűsítése szükséges.

Ezt követően, amennyiben az az eredmény születik a kutatás során, hogy a vizsgált tantárgy felhasználható, úgy bemutatom, hogy milyen változtatások szükségesek a közszolgálati kiberbiztonsági képzésbe történő integrálásához.

[7] A Certified Information Systems Security Professional (CISSP, más néven minősített információs rendszer biztonsági szakember) képzése az informatikai rendszerek technikai kérdéseinek biztonsági vonatkozásairól szól. Bővebb információ a következő weboldalon található: www.isc2.org/Certifications/CISSP#

4.1.3. FEJEZET SZERKEZETE

A 4.2 alfejezetben definiálom a közszolgálati kiberbiztonsági képzés fogalmát, alapvető elemeit, bemeneti és követi követelményeit, majd ezt követően a 4.3 alfejezetben a képzés struktúráját, felépítését, valamint a képzés során átadni kívánt oktatási anyag főbb témaköreit. Ezután a 4.4 alfejezetben bemutatom a képzési program tantervi hálóját, valamint az általános értékelési rendszer főbb komponenseit. A 4.5 fejezetben javaslatot teszek a közszolgálati kiberbiztonsági képzés lehetséges felhasználására a kibervédelmi képességek fejlesztése céljából az Önkéntes Tartalékos Rendszerben. Végezetül a 4.6 alfejezetben a tudásátadás hatékonyságának mérését mutatom be, amelynek keretében ismertetem a részkutatás eredményeit, kiértékelését, az oktatott témakörök osztályozását, valamint a definiált szempontrendszert és a tantárgy felhasználásának lehetőségét. A 4.7 és a 4.8 alfejezetek tartalmazzák a fejezet egészének következtetéseit, valamint az elért új tudományos eredményeket.

4.2. KAPCSOLÓDÓ SZAKIRODALMI ÁTTEKINTÉS

Ahhoz, hogy a jelen fejezetben célul kitűzött képzés minden elemére kiterjedő definiálása, valamint annak tartalmának meghatározása során a szükséges kutatási módszerek azonosítása megvalósulhasson, nélkülözhetetlen a releváns hazai és nemzetközi szakirodalom mélyebb vizsgálata.

4.2.1. KÉPZÉSTERVEZÉSSEL KAPCSOLATOS TANULMÁNYOK

Az irodalomkutatás során olyan hasonló keretrendszereket, valamint tanulmányokat kerestem, amelyek választ adnak arra a kérdésre, hogy milyen komponensek, lépések szükségesek egy felsőoktatási képzés definiálásához.

Shaaron Pratt és Caroline Adams bemutatták egy radiográfiai felsőoktatási képzés kidolgozásának és érvényesítésének módját. A szerzők szerint egy új kurzus, illetve tanterv kidolgozása előtt és közben tíz kérdésre kell választ adni. Ide sorolhatók a képzés céljaira, tartalmára, annak megszervezésére, az oktatási stratégiák meghatározására, oktatói módszerekre és számos további a képzés konkrét megszervezésére vonatkozó kérdések. A szerzők kifejtik, hogy a kurzus fejlesztésének (vagy egy már meglévő képzés újradefiniálásának) a folyamata egy irányító csoport létrehozásával kezdődik, amely általában a kurzus csapatának tagjaiból áll és szükség

esetén más egyetemek bevonásával történik. Az érvényesítési mechanizmus megköveteli a meglévő tanfolyam felülvizsgálatát. Az eredmények, a hallgatói visszajelzések, a külső vizsgáztatók észrevételei, a szakértői vélemények és az eredmények tükrében figyelembe vett erősségeket és gyengeségeket rögzíteni kell a tanterv tervezése során. Meg kell határozni a képzés kimenetelét, valamint a kívülről érkező igényeket. A képzési programnak tükröznie kell az aktuális iránymutatásokat, ajánlásokat a kapcsolódó szakirodalmat és kutatásokat. A szerzők a tantervelméleti szakemberekre hivatkozva bemutatják, hogy a tantervben hivatalos tananyag, hivatalos tanterv, tényleges tanterv és rejtett tanterv is rendelkezésre áll, majd ismertetik ezek lényegét. Végül a cikk kitér a tanulási és tanítási stratégiákra, amely számos képességet és készséget tartalmaz. [29]

Ping Wang cikkében rávilágít arra, hogy a különféle doktori programok tantervét és kurzusait folyamatosan frissíteni és fejleszteni kell a társadalom gyors változásainak kezelése érdekében, különösen az információs rendszerekkel és technológiákkal összefüggő programok esetében. A szerző kiemeli, hogy egy doktori képzés meghatározása során a szakmai és karriercélokat is figyelembe kell venni. Kiemelt figyelmet kell fordítani az úgynevezett moduláris tevékenységekre, mely azokra a képzés specifikus tevékenységekre utal, amelyek közvetlenül hozzájárulnak a képzés tanulási eredményeihez és támogatják a szakmai és karriercélokat. A szerző rögzíti a kurzus kimenetelére vonatkozó követelményeket is. [30]

4.2.2. KIBERBIZTONSÁGI KÉPZÉSEK TERVEZÉSÉVEL KAPCSOLATOS TANULMÁNYOK

Régner Sabillón és szerzőtársai olyan kiberbiztonsági képzést definiáltak, amelyen vállalatok alkalmazottai vehetnek részt vállalati szinten. A képzés négy elhatárolt csoportra bontja az alkalmazottakat: IT szakértők, vezetők, operatív tagok és végfelhasználók. A csoportoknak különböző témaköröket definiálnak aszerint, hogy mi a számukra legszükségesebb továbbképzési pont. A képzés elvégzése után a képzés sikerességét nem személyenként vizsgálják, hanem a csoportokhoz kapcsolódó metrikákat ellenőrzik le a vállalat mindennapi munkája során. A kiértékelés után a vállalatot érettségi szintjének megfelelő kategóriába sorolják (éretlen, fejlődő, érett, előrehaladott). [31]

Razvan Beuran és szerzőtársai a képzési tevékenységek három fő kategóriáját különítik el a kiberbiztonság témakörében, a támadásorientált képzést, az elemzésorientált képzést, valamint a védelemorientált képzést nevesítik. A szerzők szerint két követelmény megvalósulása szükséges a hatékony kiberbiztonsági képzési rendszer létrehozásához: az egyik a módosítás és az új képzési tartalmak hozzáadásának képessége, a másik a képzési környezet automatikus létrehozásának és kezelésének képessége. [32]

Marc J. Dupuis egy bevezető kiberbiztonsági tanfolyam szükségességét és fejlesztését mutatja be tanulmányában. A cikkben a szerző bemutatja a kurzus tantervét, felépítését, tartalmát, előnyeit, valamint az esetleges kihívásokat. Vizsgálja a kurzus kilenc fő célját és az azok alapján meghatározott témaköröket a félév során történő időbeli elhelyezkedésük alapján. A szerző szerint fontos a megfelelő értékelési rendszer kialakítása. A bemutatott képzés során a csoportos vetélkedőkből, projektekből, szakmai előadásokból, laborfeladatokból álló számonkérés a meghatározó. [33]

Patricia Toth és Penny Klein tanulmányukban bemutatják az amerikai szövetségi intézmények, szervezetek, részlegek informatikai, illetve kiberbiztonsági szerepalapú képzését. A publikáció relevanciáját a szerzők által bemutatott oktatási tervezési modell öt szakaszát adja: az elemzés, a tervezés, a fejlesztés, a megvalósítás és az értékelés. [34]

4.3. A KÉPZÉS FORMÁLIS SPECIFIKÁLÁSA

Az eddigi fejezetekben meghatároztam a közszolgálat számára szükséges tudáshalmazt és megvizsgáltam, hogy létezik-e olyan felsőoktatási rendszerben elérhető képzés, amely a felvázolt szükséges ismeretköröket tartalmazza. Mivel egyértelműen kiderült, hogy nem található ilyen képzés hazánkban, ezért elengedhetetlen egy olyan képzés definiálása, amely lefedi ezen ismereteket.

A következőkben meghatározom a közszolgálati kiberbiztonsági képzés alapvető fogalmainak, elemeinek definícióját, értelmezését, a bemeneti, képzési és kimeneti követelményeit.

4.3.1. A KIBERBIZTONSÁGI KÉPZÉS DEFINIÁLÁSA

Ahhoz, hogy definiálhassuk magát a képzést elengedhetetlen a kibervédelmi képesség pontos meghatározása. A képzés szempontjából fontos, hogy ebben az esetben a személyes kibervédelmi képességről beszélünk. Természetesen a végső cél a közszolgálat szervezeti szintű kibervédelmi képességének kialakítása, s ezáltal a kiberbiztonság fejlesztése, amelynek első lépése a szervezet alkalmazottai körében e képesség elsajátítása. A szervezeti és a személyi kibervédelmi képesség tehát elkülönül egymástól, de egymásra épül. A kibervédelmi képesség magában foglalja az információbiztonság-tudatosságot is, alapvető részeként értelmezhető, amely elengedhetetlen feltétele e képesség kialakításának.

Ezek alapján a *kibervédelmi képesség* azon személyes kibervédelmi képességek összességét jelenti, amely a kibertérből érkező jelenleg ismert vagy ismeretlen fenyegetések és támadások megelőzésére, felismerésére, megakadályozására és következményeinek mérséklésére irányul.

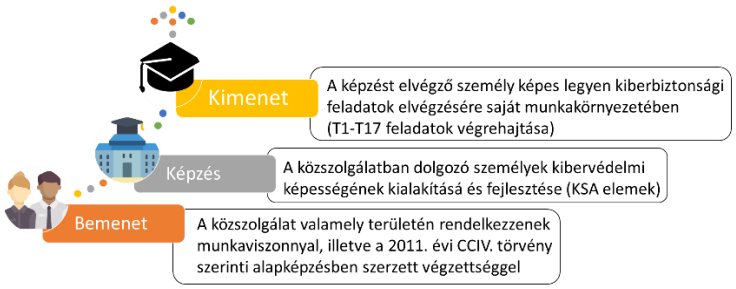
E képesség kialakítását célozza a *közszolgálati kiberbiztonsági képzés*, amely a közszolgálatban dolgozó személyek kibervédelmi képességének kialakítására irányul a közszolgálati kiberbiztonság fejlesztése érdekében.

A képzés jelen esetben egyfajta tudásátadás a közszolgálatban dolgozó személyek, döntéshozók számára, hogy a kibertérből érkező jelenleg ismert vagy ismeretlen fenyegetéseket és támadásokat képesek legyenek megelőzni, felismerni és megakadályozni.

A képzés célja a közszolgálatban dolgozó személyek, döntéshozók ismeretének módszeres kiterjesztése a kibervédelmi képességhez szükséges tudással, amelynek segítségével a kibertérből érkező jelenleg ismert vagy ismeretlen fenyegetések és támadások kockázatát azonosíthatják, esetlegesen a végrehajtás során kisebb mértékben beavatkozhatnak.

4.3.2. A KÉPZÉSI FORMA ALAPVETŐ ELEMEINEK MEGHATÁROZÁSA

A képzés alapvető be- és kimeneti követelményeit, valamint a képzés célját tekinti át a 4-1. ábra. Az alfejezet további részében ezen elemeket részletezem.



4-1. ábra: A közszolgálati kiberbiztonsági képzés definíciója és alapvetői követelményei

A képzés bemeneti követelménye, hogy a képzésben részt vevő személy a közszolgálat valamely területén rendelkezzen munkaviszonnyal és hazai alapképzési, illetve mesterképzési szakkal vagy ezzel egyenértékű külföldi felsőoktatási végzettséggel.

A képzés során a közszolgálatban dolgozó személyek a kibervédelem elméleti és gyakorlati oldalát is egyaránt megismerhetik, hiszen a képzés egy elméleti és egy gyakorlati részből áll. Az elméleti részben a résztvevők elsajátíthatják többek között – a teljesség igénye nélkül – a munkájukhoz szorosan kapcsolódó államtudományi, jogi és közigazgatás-szervezési ismereteket, biztonságpolitikai, diplomáciai ismereteket, kommunikációs ismereteket, informatikai alapismereteket, információ- és informatikai biztonsági ismereteket, valamint adatvédelmi ismereteket. Ahhoz, hogy a képzés résztvevői a megszerzett elméleti tudást éles helyzetbe is át tudják ültetni a képzés gyakorlati része nyújt segítséget, amely során konkrét támadásokkal szembesülhetnek, amelyeket önállóan vagy csapatban kell megoldaniuk. Ennek szerepe, hogy az alkalmazottakat ne érje váratlanul egy valós támadás és meg tudják hozni a megfelelő, sok esetben stratégiai döntéseket. A képzés gyakorlati része a hazai és nemzetközi oktatásban is megjelenő kibergyakorlatokra épül, amely során konkrét támadások szimulálásával a már meglévő tudásra alapozva, összekapcsolható az elméleti és a gyakorlati tudás. Ennek következtében a résztvevők képesek lesznek felismerni a kibertérből érkező fenyegetéseket és esetleges kockázatokat. A képzés gyakorlati része során a mindennapos üzemeltetési feladatokkal és az információs rendszer, valamint az ehhez kapcsolódó folyamatok, eljárások megfelelőségének ellenőrzésével is meg kell birkózniuk a hallgatóknak.

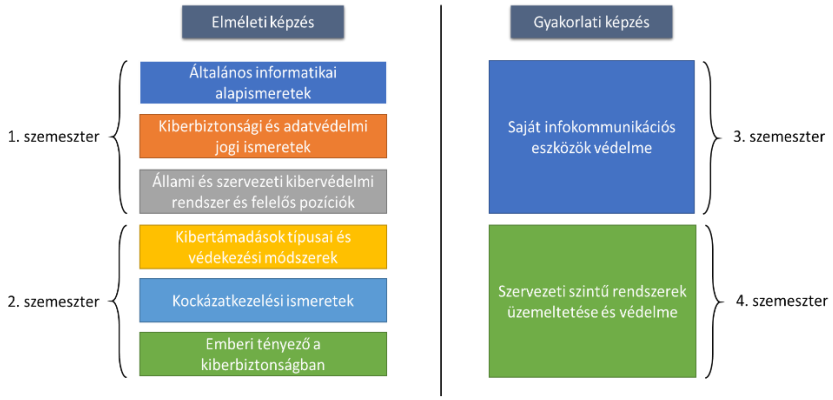
A képzés kimeneti követelménye, hogy a képzést elvégző személy képes legyen a korábban definiált és azonosított feladatok elvégzésére saját munkakörnyezetében. A képzés abszolválását követően a korábban említett területeken szerezhetnek

széleskörű szakmai ismereteket, valamint a mindennapi munkájuk során előforduló aktuális és lehetséges kihívások megoldására szolgáló szakmai kompetenciákat.

Összegezve a közszolgálati kiberbiztonsági képzés egy gyakorlatban is alkalmazható szakmai tudást, valamint problémafelismerő és -megoldó készséget nyújt résztvevőinek, amelynek elsajátításával képesek felismerni, feltérképezni a kibertámadások támadási felületeit és megelőző lépéseket tenni a környezetében jelentkező kibertámadási pontokon. Továbbá a résztvevők képesek lesznek azonosítani egy-egy konkrét támadást, illetve beavatkozni szükség esetén.

4.4. A KÉPZÉSI STRUKTÚRA ÉS TÉMAKÖRÖK MEGHATÁROZÁSA

A képzés során a közszolgálatban dolgozó személyek a kibervédelem elméleti és gyakorlati oldalát egyaránt megismerhetik, hiszen a képzés egy elméleti és egy gyakorlati részből áll. A képzés felépítésének meghatározásához a korábban azonosított ismeretkörök, a hazai és nemzetközi képzések vizsgálatakor feltárt jó gyakorlatok elemzése, valamint az elmúlt évek oktatói tapasztalata nyújtott segítséget. A képzés vázlatos felépítését a 4-2. ábra szemlélteti.



4-2. ábra A képzés magas szintű, vázlatos felépítése

4.4.1. AZ ELMÉLETI RÉSZ TARTALMA

A képzés első félévében az elméleti részben a hallgatók elsajátíthatják többek között a következőkben felsorolt főbb témaköröket: az általános informatikai alapismereteket, a kiberbiztonsággal és adatvédelemmel kapcsolatos jogi ismereteket, alapvető fogalmakat, valamint a hazai és nemzetközi kibervédelmi rendszer felépítését, a szervezeten belüli kiberbiztonsági és adatvédelmi felelős pozíciókat. Ezt követően a második félévben megismerkednek további szükséges ismeretkörökkel, így például a

különféle kibertámadások típusaival, támadási technikákkal, illetve az ezek megelőzésére és elhárítására irányuló módszerekkel. Ezen kívül elsajátítják a kockázatkezelés módszertanát, továbbá feltárják az emberi tényező kiberbiztonságban betöltött szerepét és kapcsolódási pontjaikat, valamint az alapvető pszichológiai és kommunikációs ismereteket. Ezek bemutatására a következő alfejezetben kerül sor.

Ahhoz, hogy a képzés résztvevői a megszerzett elméleti tudást éles helyzetbe is át tudják ültetni a képzés gyakorlati része nyújt segítséget, amely során konkrét támadásokkal szembesülhetnek. Ennek szerepe, hogy a közszolgálati dolgozókat ne érje váratlanul egy valós támadás és meg tudják hozni a szükséges, sok esetben stratégiai döntéseket.

4.4.2. A KÉTLÉPCSŐS GYAKORLATI KÉPZÉS TARTALMA

A képzés gyakorlati részének feltétele az első két félév elméleti ismeretanyagának elsajátítása, hiszen ahhoz, hogy a hallgatók képesek legyenek a gyakorlatban is alkalmazni a különféle kibervédelmi mechanizmusokat, elengedhetetlen a kiberbiztonság elméleti hátterének vizsgálata. A gyakorlati rész további két szakaszra osztható, amelyek a harmadik és negyedik félévben kerülnek megtartásra. Ezen kétlépcsős gyakorlati képzés során a hallgatók először a saját infokommunikációs eszközeik védelmi mechanizmusaival ismerkednek meg, majd szimulált, szervezeti szintű környezetben a támadások elhárítását hajtják végre.

A képzés gyakorlati része során a konkrét támadások szimulálásával a már meglévő tudásra alapozva, összekapcsolható az elméleti és a gyakorlati tudás. Ennek következtében a hallgatók képesek lesznek felismerni a kibertérből érkező fenyegetéseket és esetleges kockázatokat.

A közszolgálati kiberbiztonsági képzés harmadik félévében kerül sor a gyakorlati képzés első lépcsőjére, amely alapvetően a hallgatók saját infokommunikációs eszközeinek biztonsági beállításaira, az ezeket érintő fenyegetésekre és ezek megelőzésére, elhárítására irányuló módszerekkel kapcsolatos gyakorlati feladatok teljesítésére terjed ki. Ezen kívül a mindennapos üzemeltetési feladatokkal és az információs rendszerek, valamint az ehhez kapcsolódó folyamatok, eljárások megfelelőségének ellenőrzésével is meg kell birkózniuk a hallgatóknak. Ennek célja, hogy a hallgatók képesek legyenek a gyakorlatban is végrehajtani a különféle üzemeltetéssel, megelőzéssel és védekezéssel kapcsolatos teendőket. A hallgatók saját

infokommunikációs eszközeinek köre magában foglalja azon eszközöket, amelyeket a közszolgálatban dolgozók nap, mint a nap használnak, így például az okostelefonokat, tableteket, laptopokat, okosórákat. Természetesen a technológia fejlődésének és az egyre újabb eszközök megjelenésének köszönhetően ez a lista folyamatos bővítést igényel. A saját eszközök vizsgálata azért indokolt, mert sok esetben előfordul, hogy a munkavállalók ezeket munkaügyi feladatokra, munkavégzés céljára használják. Így például dokumentumokat töltenek le, szerkesztenek, továbbítanak a saját eszközeik, illetve az ezen lévő alkalmazások segítségével. Előfordulhat, hogy az adott munkahely ezt engedélyezi alkalmazottai számára, például a BYOD (Bring Your Own Device) politika keretein belül, melynek célja, hogy a munkavállalók saját eszközeik segítségével hatékonyan és folyamatosan képesek legyenek a rájuk bízott munkát bármikor és bárhol végrehajtani. Ennek az elvnek számos előnye van, azonban a hátrányairól és veszélyeiről sem szabad megfeledkeznünk. Ezen kívül annak ellenére, hogy a legtöbb szervezetnél nem engedélyezett a saját eszközök munkaügyi célokra történő használata, illetve ennek fordított változata, mégis sok esetben előfordul, hogy az alkalmazottak a tiltás ellenére vagy külön engedély birtokában használják azt. Számos további biztonsági kérdést vet fel annak ténye, hogy az esetleges otthoni munkavégzés során kizárólag a munkahelyi eszközök vagy akár saját infrastruktúra is használható-e. Továbbá fontos megemlíteni, hogy a saját infokommunikációs eszközök védelme nem csak a különféle kiberbiztonsággal kapcsolatos incidensek elkerülése érdekében elengedhetetlen, hanem a személyes adatok és a magánélet védelme szempontjából is kiemelt jelentőséggel bír.

Az első lépcső keretében a hallgatók megismerkedhetnek az általuk használt eszközök, alkalmazások működésével, biztonsági és adatvédelmi beállításaival, az eszközeiket érintő fenyegetésekkel és kibertámadási technikákkal. Megvizsgálják böngészők biztonsági beállításait, így például a bejelentkezések és jelszavak, a sütik, az engedélykérések (hely, kamera, mikrofon stb.), adatgyűjtés, tartalomblokkolás, vagy akár a tanúsítványok testreszabásának szerepét, jelentőségét és az esetleges veszélyeket. A hallgatók elsajátítják a közösségi média specifikus szabályokat, sebezhetőségeket, illetve beállításokat, ennek keretében többek között feltérképezik a jelszókezelés, az azonosítás és a hitelesítés formáit, a személyes adatok védelmével kapcsolatos beállítások típusait, fontosságát és lehetőségeit. A képzés résztvevői megismerkednek a különféle levelezőrendszerekkel, felhőtechnológiákkal, azok

veszélyeivel, illetve a különféle biztonsági és adatvédelmi beállítások fontosságával, részleteivel. Ezen kívül a félév során kiemelt figyelmet kapnak a különféle operációs rendszerek (pl. Windows, iOS, Android, Linux) sebezhetőségei, használatának szabályai, valamint a különféle védelmi intézkedések megvalósításának lehetőségei. A hallgatók megismerkednek a leggyakrabban használt szöveg-, táblázat- és diasor szerkesztő programok alapvető veszélyeivel. A lehetséges eszközök, alkalmazások és egyéb programok körét a 4-3. ábra szemlélteti. Emellett végrehajtanak számos további az infokommunikációs eszközöket érintő alapvető üzemeltetési feladatot, valamint elvégzik a sebezhetőségek feltárását, a különféle fenyegetések elleni megelőzés és védekezés alapvető lépéseit.

4-3. ábra Leggyakrabban használt eszközök és alkalmazások szemléltetése

Fontos, hogy ebben a félévben a hallgatók a megelőzés részeként nemcsak a különféle biztonsági beállítások testreszabását és a sebezhetőségek feltárását valósítják meg, hanem eszköz- és alkalmazásspecifikusan konkrét kibertámadásokkal is találkoznak, továbbá az ezekre történő reagálás egyes lépéseit és módszereit egyaránt végrehajtják és begyakorolják.

A közszolgálati kiberbiztonsági képzés negyedik félévében kerül sor a gyakorlati rész második felének megtartására. Ennek keretében a hallgatók szimulált szervezeti környezetben kibertámadások elhárítását önállóan vagy csapatban hajtják végre. Ennek lényege, hogy a félév során szervezeti szintű környezetet szimulálunk, hiszen csak ilyen gyakorlati tevékenységek segítségével érhető el, hogy a hallgatók megszerezzék azon szükséges készségeket, képességeket, amelyek segítségével a lehető legrövidebb időn belül képesek lesznek majd reagálni készség szinten egy valós incidensre, illetve biztonsági eseményre. Ennek keretében a hallgatók megismerkednek a munkahelyi eszközök és az információs rendszerek felépítésével, ezek sérülékenységeivel, a kapcsolódó üzemeltetési feladatokkal, valamint a megelőzés és a védekezés lehetséges alternatíváival. Ennek részeként feltárják az eszközök működését biztosító alaprendszerek típusait, üzemeltetésének feltételeit,

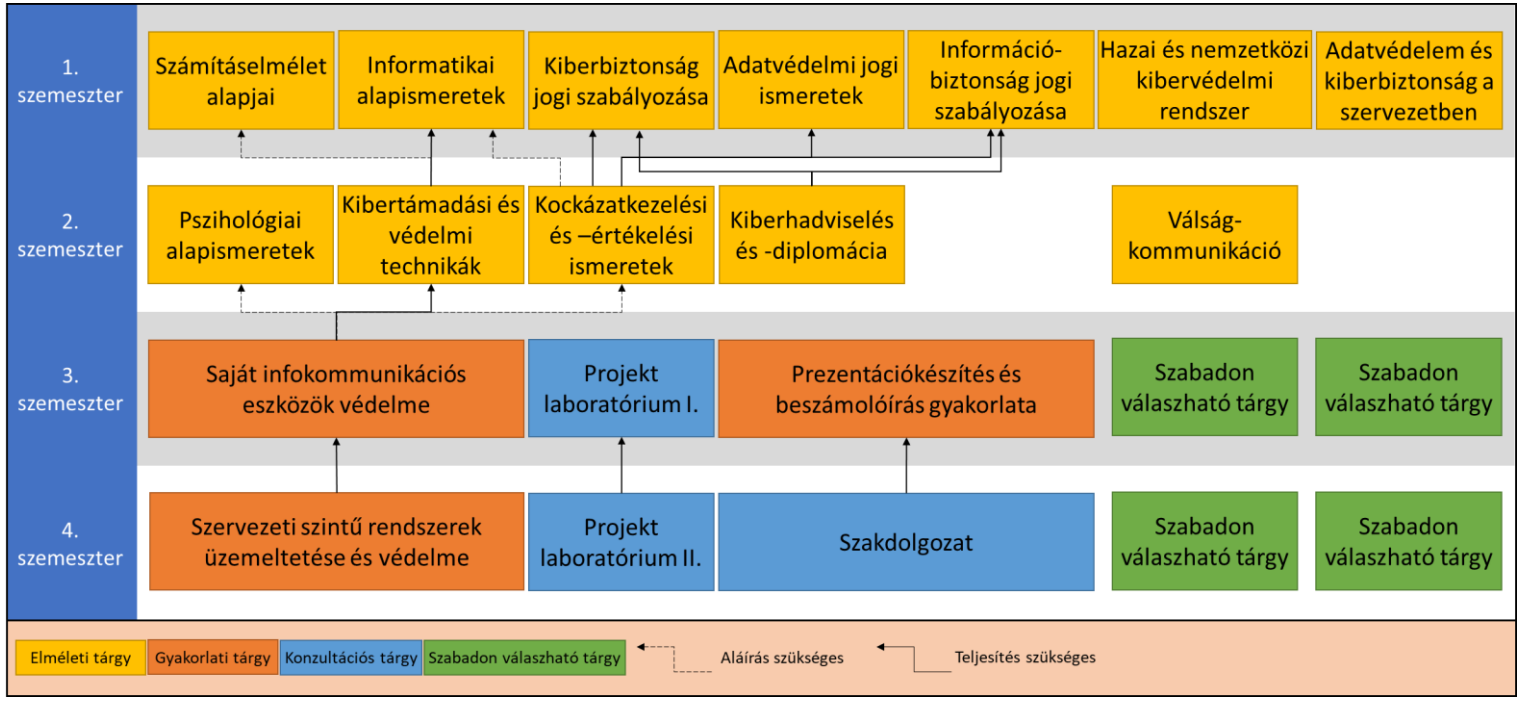
sebezhetőségeit és a különféle védelmi, biztonsági beállításokat. Számos alkalmazás és szoftver telepítése indokolt a munkahelyi eszközökön így ezek telepítésének, működésének és veszélyeinek feltárása, valamint a licenszek eredetének vizsgálata is különösen fontos, amennyiben az alkalmazott maga telepíti azt a munkahelyi eszközére. Gyakorlati példák segítségével kerül szemléltetésre az idegen eszközök munkahelyi eszközökhöz való kapcsolódásának, valamint ezek nyílt hozzáférésű internet hálózathoz történő csatlakoztatásának veszélyei. Ezen kívül említésre kerülnek a levelezőrendszerek használatának alapvető szabályai és sebezhetőségei, a különféle adathalász levelek és kártékony programok csatolmányként történő érkezésének gyakorlati tapasztalatai.

A hallgatók szimulált szervezeti környezetben tapasztalják meg milyen kibertámadások jelentenek veszélyt az információs infrastruktúrára, illetve milyen megelőző és védelmi intézkedésekkel háríthatók el ezen támadások. Ennek keretében többek között megismerik – a teljesség igénye nélkül - a DoS, DDoS, XSS, SQL injection támadásokat, a kártékony programok különféle típusait, adathalászatot, továbbá a social engineering technikáit valós helyzetekben. Ebben a félévben külön kurzus keretében kerülnek bemutatásra és szimulálásra a social engineering módszerek. A social engineering az ember megtévesztésével, kihasználásával és manipulálásával teszi lehetővé belső és bizalmas információk megszerzését vagy akár egy infokommunikációs eszköz kártékony programmal történő megfertőzését. Ezen technikák a kiberhadviselésben jól alkalmazhatók, hiszen a technológiai sérülékenységeket és a felhasználók sebezhetőségeit együttesen használják ki. Ezen kívül a képzés során a hallgatók további kiberbiztonsági kihívásokkal is szembesülnek, így például a felhasználói azonosítóval történő visszaéléssel, valamint illetéktelen rendszer- vagy adathozzáféréssel, bármely, a felhasználó által használt szolgáltatás, rendszer, infokommunikációs eszköz tekintetében (pl. elektronikus levelezés, szakrendszer stb.). Fontos, hogy nem csak a kibertérből érkező fenyegetések kapnak hangsúlyt a képzés során, hanem az eszközök állapotában bekövetkező különféle fizikai változások, mint például a hallgató tulajdonában lévő infokommunikációs eszközök elvesztése, megrongálódása, vagy akár a megbontására utaló jelek kezelése.

A gyakorlati képzés célja, hogy a hallgatók valósághű környezetben begyakorolják a vészhelyzetek során alkalmazandó lépéseket, technikákat és ellenőrizzék a stratégiai tervek alkalmazhatóságát.

4.4.3. TANTERVI HÁLÓ

A képzési program főbb elemeit az előző pontokban részleteztem, jelen pontban a képzés konkrét tantervi hálója, a teljesítendő tantárgyak köre kerül bemutatásra, amelyet a 4-4. ábra szemléltet. A tantárgyak tartalmának kidolgozásának alapjául az összehasonlításban érintett képzések tantárgyi programjai, a NICE és az ECSF Keretrendszer, valamint az általam meghatározott tudáshalmaz szolgált.



4-4. ábra A közszolgáltati kiberbiztonsági képzés tervezett tantervi hálója

4.4.3.1. 1. szemeszter

A képzés elméleti részét képező első szemeszterében az alábbi tantárgyak oktatása valósulna meg:

a) Számításelmélet alapjai
b) Informatikai alapismeretek
c) Információs rendszerek és hálózatok védelme
d) Kiberbiztonság jogi szabályozása
e) Adatvédelmi jogi ismeretek
f) Információbiztonság jogi szabályozása
g) Hazai és nemzetközi kibervédelmi rendszer
h) Adatvédelem és kiberbiztonság a szervezetben

Az egyes tantárgyak tartalma a következő:

Számításelmélet alapjai: tantárgy keretében a hallgatók megismerkedhetnek az informatikai szakterület legfontosabb általános elméleteivel, összefüggéseivel, és az ezekkel összefüggő fogalomrendszerrel, különösen a számítógép architektúrák, operációs rendszerek, számítógépes hálózatok, valamint az adatbázisok elméleti alapjai területein.

Informatikai alapismeretek: tantárgy célja az alapvető szakmai ismeretek átadása a számítógépek felépítése, működése, a számítógép-architektúrák, operációs rendszerek funkciói, belső szerkezete, működési elvei területeken. Ezek megismerésével a képessé válnak konkrét számítógép-rendszerek és operációs rendszerek dokumentációinak gyors megértésére, üzemeltetési, konfigurálási, karbantartási feladatok gyors megtanulására.

Információs rendszerek és hálózatok biztonsága: tantárgy keretében a hallgatók megismerhetik a hálózati infrastruktúra alapjait, hálózati kapcsolatok beállítási és hibaelhárítási lehetőségeit. [8]

Kiberbiztonság jogi szabályozása: tantárgy célja a kiberbiztonsággal kapcsolatos hazai és nemzetközi szabályozás, ajánlások, szabványok, valamint az ezekkel összefüggő fogalomrendszer megismertetése a hallgatókkal. Ennek keretében a hallgatók megismerkedhetnek a kiberbiztonság jogi és szervezeti hátterével, a kibertér

[8] E tárgy tartalmának kidolgozása során az NKE-EIV információs rendszerek és hálózatok biztonsága 1-2. tárgyak tantárgyi adatlapjai szolgáltak alapul.

és kiberbiztonság fogalmi alapjaival, valamint a kibervédelem tervezésének, szervezésének legfőbb komponenseivel.

Adatvédelmi jogi ismeretek: tantárgy bemutatja az adatvédelem helyét a jogrendszerben, a személyes adatok védelmével összefüggő hazai és nemzetközi szabályozást, a kapcsolódó alapfogalmakat, valamint az adatkezelések megvalósításával összefüggő alapvető ismereteket. A tantárgy célja az adatvédelmi jog területével összefüggő elméleti és gyakorlati tudás átadása.

Információbiztonság jogi szabályozása: a tantárgy betekintés nyújt az információbiztonság alapjaiba, így bemutatja a kapcsolódó fogalmi rendszert, alapelveket, a vonatkozó hazai és nemzetközi szabályozást, valamint az információbiztonság megvalósítását célzó eszközöket, intézkedéseket egyéni és szervezeti szinten egyaránt.

Hazai és nemzetközi kibervédelmi rendszer: a tantárgy segítségével a hallgatók megismerhetik a kiberbiztonsággal foglalkozó hazai és nemzetközi szervezetekkel, hatóságokkal, valamint ezek jogszabályban rögzített feladataival. A tantárgy kitér a szervezeti együttműködés kereteire, szerepére és a kapcsolódó szankciók rendszerére.

Adatvédelem és kiberbiztonság a szervezetben: a tantárgy célja megismertetni a hallgatókkal az adatvédelemmel és kiberbiztonsággal összefüggő szervezeti feladatok, valamint a szervezeten belüli adatvédelemmel és kiberbiztonsággal összefüggő pozíciók feladatainak és felelősségeinek tartalmát. A tantárgy keretében megismerhetik a hallgatók az adatvédelmi és kiberbiztonsági szerepkörök együttműködésének lehetőségeit és területeit.

4.4.3.2. 2. szemeszter

A képzés elméleti részét képező második szemeszterében az alábbi tantárgyak oktatása valósulna meg:

a) Pszichológiai alapismeretek
b) Kibertámadási és –védelmi technikák
c) Kockázatkezelési és –értékelési ismeretek
d) Kiberhadviselés és –diplomácia
e) Incidenskezelés alapjai
f) Válságkommunikáció

Az egyes tantárgyak tartalma a következő:

Pszichológiai alapismeretek: tantárgy betekintést nyújt a kibertámadások sikeressége mögött álló motivációkba, azok pszichológiai tényezőibe, valamint a manipuláción és befolyásoláson alapuló támadások működési mechanizmusaiba (social engineering). A hallgatók megismerhetik a támadók és az áldozatok lehetséges viselkedési jellemzőit, stratégiáit és az ezek elleni védekezés viselkedési mechanizmusait.

Kibertámadási és –védelmi technikák: tárgy keretében a hallgatók megismerhetik az aktuális kibertérből érkező fenyegetéseket, azok típusait, megvalósításának lehetőségeit és működési mechanizmusait. A hallgatók betekintést kaphatnak a támadási technikák kivitelezésének informatikai hátterébe, a támadások megelőzése és elhárítása érdekében tett intézkedések alternatíváiba, valamint a szervezet által végrehajtandó adminisztratív, logikai és fizikai védelmi intézkedésekbe.

Kockázatkezelési és –értékelési ismeretek: tantárgy célja megismertetni a hallgatókkal az általános kiber-, és információbiztonság területéhez tartozó kockázatelemzés és –kezelés módszertanát. Ennek keretében a hallgatók átfogó ismeretek kaphatnak a kockázatkezelés fogalomrendszerével, a kockázatelemzés módszereivel, lépéseivel és vonatkozó személyi, szervezeti feladatokkal, szerepkörökkel, valamint a kockázatok típusaival és a kockázatok csökkentésére irányuló technikákkal kapcsolatban. A hallgatók gyakorlati ismereteket szerezhetnek a kockázatkezeléssel összefüggő esettanulmányok kidolgozása által.

Kiberhadviselés és –diplomácia: tárgy célja megismertetni a hallgatókkal az információs támadások elemeit, hatásait és megvalósításának lehetőségeit. A tárgy keretében sor kerül a kiberhadviseléssel összefüggő alapfogalmak, valamint a kiberműveletek és az információs műveletek bemutatására. A tantárgy betekintést nyújt a kibrbiztonsággal összefüggő nemzetközi kapcsolatok szerepéről, feladatairól és aktuális kérdéseiről, valamint a kiberdiplomáciával kapcsolatos fogalom- és szervezeti rendszerről.

Incidenskezelés alapjai: tárgy átfogó szakmai, gyakorlati ismereteket nyújt a hallgatóknak az incidenskezelés alapjaival, így az incidenskezelésben érintett személyek és szervezetek, hatóságok szerepével és feladataival, valamint az incidensek típusaival (pl. adatvédelmi incidens, biztonsági esemény) kapcsolatban. Emellett a hallgatók megismerkedhetnek az incidenskezelés folyamatával,

sajátosságaival, valamint az incidenskezelés és az üzletmenetfolytonosság-tervezés kapcsolódási pontjaival, az üzletmenedzsmentfolytonosság-tervezés elemeivel.

Válságkommunikáció: tárgy célja megismertetni hallgatókkal a szervezetben előforduló válsághelyzetek kezelésének alapjait, a hatékony és eredményes kríziskommunikáció megvalósításának lehetőségeit. Ennek keretében a hallgatók esettanulmányok segítségével próbálhatják ki magukat valós szituációkban.

4.4.3.3. 3. szemeszter

A képzés gyakorlati részét képező, harmadik szemeszterében az alábbi tantárgyak oktatása valósulna meg:

a) Saját infokommunikációs eszközök védelme
b) Projekt Laboratórium I.
c) Prezentációkészítés és beszámolóírás gyakorlata
d) Szabadon választható tárgy I.
e) Szabadon választható tárgy II.

Az egyes tantárgyak tartalma az alábbiakban kerülnek kifejtésre:

Saját infokommunikációs eszközök védelme: tárgy keretében a hallgatók megismerkedhetnek az általánosan használt információs rendszerek és eszközök működésével, biztonsági és adatvédelmi beállításaival, valamint e rendszereket és eszközöket érintő támadási alternatívákkal. A hallgatók ezen kívül gyakorlati feladatok végrehajtásával megismerkedhetnek a böngészők biztonsági beállításaival, a közösségi média veszélyeivel, jogosultságkezeléssel, operációs rendszerekkel és egyéb a saját eszközeiket érintő adminisztratív, logikai és fizikai védelmi intézkedéssel.

Projekt Laboratórium I.: Jelen gyakorlat során a hallgatók egy szimulált környezetben ismerkedhetnek meg a különféle kibertámadási technikákkal és e környezetben kipróbálhatják a képzés során megismert védelmi mechanizmusokat. A támadások és védelmi intézkedések szimulációjával a hallgatók első kézből sajátíthatják el a kibertámadások felismeréséhez és elhárításához szükséges gyakorlati ismereteket.

Prezentációkészítés és beszámolóírás gyakorlata: tárgy célja, hogy a hallgatók elsajátíthassák a magas szintű tudományos munka alapvető szabályait, a hivatalos

írásbeli kommunikáció típusait, így a kiberbiztonsági, információbiztonsági és adatvédelmi dokumentumok alapvető kritériumait. Ezt követően a hallgatók esettanulmányokon és gyakorlatokon keresztül megismerkedhetnek a hivatalos kommunikáció formáival, továbbá a prezentációkészítés és -tartás alapszabályait.

E félévben a hallgatnak két szabadon választható tantárgyat szükséges abszolválniuk, amelyek a – teljesség igénye nélkül – a következők lehetnek:

a) Informatikai rendszerek és alkalmazások I-II.
b) Információs rendszerek üzemeltetése
c) Biztonsági tesztelés
d) Logelemzés
e) Felhőszolgáltatások biztonsági kérdései
f) Információbiztonsági szabványok
g) Vezetéselmélet
h) Kriptográfia
i) Elektronikai hadviselés
j) Számítógép-hálózati hadviselés
k) Információs műveletek technológiai alapjai
l) Információs infrastruktúrák alapjai
m) Biztonság- és védelempolitika
n) Iratkezelési és elektronikus ügyintézési ismeretek
o) Projektmenedzsment
p) Információbiztonsági minőségügyirányítás
q) Adatvédelmi és információbiztonsági audit

4.4.3.4. *4. szemeszter*

A képzés gyakorlati részét képező, negyedik szemeszterében az alábbi tantárgyak oktatása valósulna meg:

a) Szervezeti szintű rendszerek üzemeltetése és védelme
b) Projekt Laboratórium II.
c) Szakdolgozat
d) Szabadon választható tárgy III.

e) Szabadon választható tárgy IV.

Szervezeti szintű rendszerek üzemeltetése és védelme: tantárgy célja, hogy a hallgatók gyakorlati szemszögből ismerkedhessenek meg a munkahelyi eszközök és információs rendszerek felépítésével, ezek sérülékenységeivel, a kapcsolódó üzemeltetési feladatokkal, valamint a megelőzés és a védekezés lehetséges eszközeivel, módszereivel.

Projekt Laboratórium II.: tantárgy tartalma igazodik a Projekt Laboratórium I. keretében elsajátított szimulációs gyakorlatok során átadott ismeretanyaghoz, a tantárgy felvételének és teljesítésének feltétele az első rész abszolválása.

Szakdolgozat: Jelen tantárgy lehetőséget biztosít a hallgatók és oktatók közötti folyamatos szakdolgozati konzultáció megvalósítására.

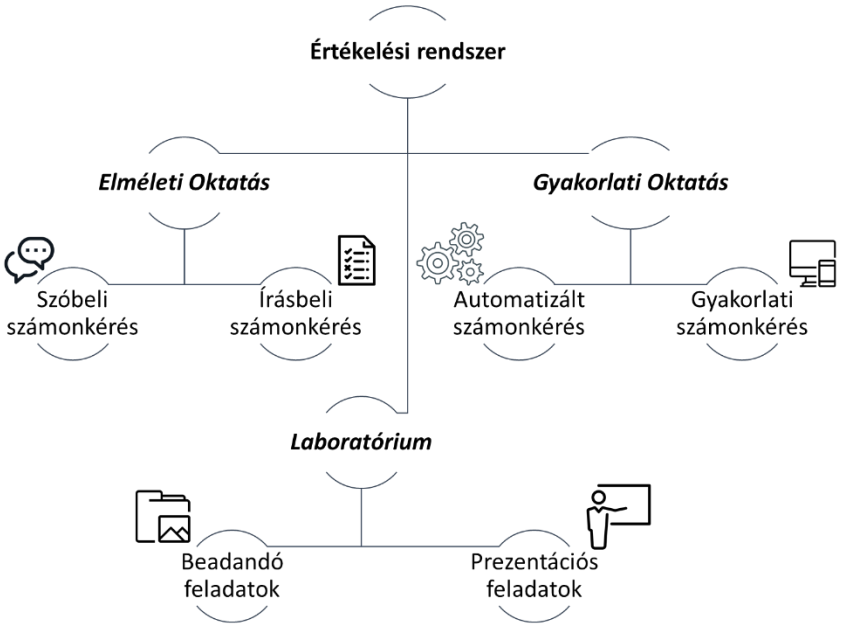
A Szabadon választható tárgy III-IV. lehetőségei megegyeznek az harmadik félévben felvehető tárgyak listájával.

4.4.4. ÉRTÉKELÉSI RENDSZER

A tantervi háló segítségével bemutattam, hogy mely tárgyak szerepelnek a tervezett képzés programjában. Az egyes tárgyak csoportosíthatók típusaik szerint is. Ezek alapján megkülönböztetünk elméleti, gyakorlati és laboratóriumi oktatásokat. Mindhárom tárgytípushoz különböző értékelési rendszer ajánlok, melyeket a 4-5. ábra szemléltet.

Elméleti oktatás: az elméleti oktatás során a klasszikus számonkérési módszereket érdemes alkalmazni, mint a szóbeli, illetve írásbeli számonkérés.

Szóbeli számonkérés: szóbeli számonkérés esetén az adott tárgy keretében az oktató feladata már az első előadás során elérhetővé tenni a hallgató számára a tétellistát. A szóbeli vizsgáztatás során a vizsgáztatónak elsődleges feladata felmérni, hogy a hallgató képes-e összefüggéseiben átlátni az adott kurzus során legadott tananyagot.



4-5. ábra Értékelési rendszer a különböző tárgy típusokhoz

Írásbeli számonkérés: írásbeli számonkérés során esszéjellegű és számolós feladatokra kell készülniük a hallgatóknak, amelyeken keresztül megmutathatják logikus gondolkodásukat a tárgy keretein belül. A vizsga értékelése során a vizsgáztató elsődleges feladata felmérni, hogy a hallgató rendelkezik-e a tárgy során elsajátított ismeretanyag alapvető összefüggéseinek és azokat képes-e logikusan alkalmazni egy-egy feladat során.

Gyakorlati oktatás: a gyakorlati oktatás során a számonkérések a hallgató önálló munkáin alapulnak, így célszerű beadandó, illetve prezentációs feladatokon keresztül felmérni a hallgatók tudását, önálló aktivitását.

Beadandó feladatok: a beadandó feladatok esetén a hallgatók feladata önállóan megismerni és feldolgozni olyan területeket (egyeztetve a tárgy oktatóival), amelyek nem részei a képzés során leadott tananyagnak, de szervesen köthetőek a tárgyhoz. A vizsgáztató feladata azt ellenőrizni, hogy a hallgató képes-e önállóan feltérképezni ismeretlen témaköröket, illetve felelőssége azt megvizsgálni, hogy a hallgató képes-e lényegre törő, összefoglaló jelentést készíteni.

Prezentációs feladatok: a prezentációs feladatok esetén (hasonlóan a beadandó feladatokhoz) a hallgatók feladata önállóan megismerni és feldolgozni olyan területeket (egyeztetve a tárgy oktatóival), amelyek nem részei a képzés során leadott tananyagnak, de szorosan kapcsolódnak a leadott ismeretanyaghoz. A vizsgáztató feladata azt ellenőrizni, hogy a hallgató képes-e önállóan feltérképezni ismeretlen

témaköröket, illetve azt megvizsgálni, hogy a hallgató képes-e megfelelő absztrakciós szinten előadni több ember előtt.

Laboratórium: a laboratóriumok során számítógépes termekben nyílik lehetőség a vizsgázgatásra, így olyan számonkérési módszerek kerülhetnek használatra, amelyeket számítógépes környezetben lehet alkalmazni.

Automatizált számonkérés: az automatizált számonkérésnek elsősorban az 5. fejezetben részletesen bemutatásra kerülő értékelési rendszer tekinthető. A vizsgáztatás során szimulált kibertámadást kell a hallgatónak elhárítania, ahol egy kiértékelő rendszer feladata azt vizsgálni, hogy a hallgató sikeresen megoldotta-e a feladatot. A vizsgáztató feladata a szimuláció elindítása és a kiértékelés áttekintése. A számonkérés célja, hogy a valóshoz rendkívül hasonló szimulációs környezetben is képesek legyenek a hallgatók alkalmazni a képzés során megszerzett tudást.

E-learning platformok használata: az e-learning platformok használata (pl. Moodle) lehetőséget nyújtanak a számonkérések számítógépes laborokban történő hatékony végrehajtására. Ellentétben az írásbeli számonkéréssel, jelen esetben több és rövidebb feladatot kell a hallgatóknak megoldaniuk, így itt elsősorban a lexikális tudást érdemes mérni, illetve az egyes feladatok rövidsége miatt azt is, hogy hallgató mennyire és hogyan kezeli készségszinten a megszerzett tudást.

4.5. KIBERVÉDELMI KÉPESSÉGEK FEJLESZTÉSE AZ ÖNKÉNTES TARTALÉKOS ÁLLOMÁNYBAN

Magyarországon folyamatosan zajlik az önkéntes tartalékos állományba történő toborzás, amelynek oka, hogy napjaink kihívásaira történő eredményes reagálás és országunk biztonsága érdekében nélkülözhetetlen az önkéntes tartalékosok képzése, akik képesek hatékonyan támogatni a haderő munkáját és egy esetleges veszélyhelyzet bekövetkezése esetén készen állnak a beavatkozásra. A jelenleg futó Honvédelmi és Haderőfejlesztési Program alapvető eleme az Önkéntes Tartalékos Rendszer.

Az Önkéntes Tartalékos Rendszer központi szereppel bír, tekintettel arra, hogy a Honvédség különleges jogrendi időszakban a hivatásos állomány mellett a kiképzett tartalékos és az aktív önkéntes tartalékos erőkkel egészül ki. A hazai Önkéntes Tartalékos Rendszer működésének jogszabályi alapját Magyarország Alaptörvénye adja (a továbbiakban: Alaptörvény). Az Alaptörvény XXXI. cikke alapvető

kötelességek között rögzíti, hogy minden magyar állampolgár köteles a haza védelmére, valamint a békeidőszaki felkészülés alapjainak megteremtésével alaptörvényi szinten rendezi az önkéntes tartalékos rendszerben való szerepvállalás lehetőségét, azzal, hogy kimondja Magyarország önkéntes honvédelmi tartalékos rendszert tart fenn. [Alaptörvény, XXXI. cikk]

4.5.1. ÖNKÉNTES TARTALÉKOS RENDSZER

Magyarország Önkéntes tartalékos állományáról a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény (a továbbiakban: Hvt.) rendelkezik. [2011. évi CXIII. törvény] A törvény alapján a Magyar Honvédség személyi állományának folyamatos kiegészítése békében részben az önkéntes tartalékos katonai szolgálatra toborzottak felvétele útján történik. [2011. évi CXIII. törvény 40. § (2)]

A Hvt. rögzíti, hogy a Honvédség tartalékos rendszere önkéntesség és jogszabályi kötelezettség alapján szervezett tartalék elemekből áll. [2011. évi CXIII. törvény 26. § (1)] A törvény szerint a tartalékos állományba tartozik az önkéntes tartalékos, a kiképzett tartalékos, valamint a potenciális hadköteles (a továbbiakban együtt: önkéntes tartalékos állomány).[2011. évi CXIII. törvény] A kiképzett tartalékos kategóriába azon hadkötelezettség alá tartozó személyek tartoznak, akik a Honvédség állományából kikerültek és önkéntesség alapján katonai szolgálatot teljesítettek. Potenciális hadkötelesnek tekinthető minden olyan, a hadkötelezettség alá tartozó személy, aki nem tartozik a kiképzett tartalékos kategóriába. [2011. évi CXIII. törvény] Fontos kiemelni, hogy a kiképzett tartalékosként, valamint a potenciális hadkötelesként nyilvántartott személy csak rendkívüli állapot, vagy megelőző védelmi helyzet idején a hadkötelezettség bevezetését követően teljesíthet tényleges katonai szolgálatot. [2011. évi CXIII. törvény] A Hvt. rögzíti az önkéntes tartalékos szerepét, amely szerint önként vállalja, hogy törvényben meghatározott feltételrendszer szerint rendelkezésre áll, és behívását követően tényleges szolgálata teljesítésével közreműködik a Honvédség feladatai ellátásában. [2011. évi CXIII. törvény 40. § (5)]

Mindemellett szükséges megemlíteni, hogy a következő évben, 2023. július 1-jén hatályba lépő, a honvédelemről és a Magyar Honvédségről szóló [2021. évi CXL. törvény 71. §] kiterjeszti a tartalékos állomány szereplőit, amely alapján a tartalékos állományba az önkéntes tartalékos, a hadkötelezettség időszakára katonai szolgálatot

önkéntesen vállalt honvédelmi alkalmazott, a kiképzett hadköteles, valamint a kiképzetlen hadköteles tartozik. A [2021. évi CXL. törvény 71. § (3)] bekezdés az önkéntes tartalékos szerepét is bővíti, amely alapján a honvédelmi szervezet egészének feladatai ellátásban részt vesz. A jogszabályi változás azt eredményezi, hogy a jövőben az önkéntes tartalékosok sokkal bővebb személyi- és feladatkörben tudnak majd szolgálatot teljesíteni.

4.5.2. KIBERVÉDELMI FELADATOK ELLÁTÁSA

A XXI. századi hadviselés egyik legnagyobb kihívása, hogy a korábban kiforrott haditechnikák egy részét a kibertérben is alkalmazhassuk. Ennek fontosságát mi sem mutatja jobban annál a ténynél, hogy 2016 júliusában az Észak-Atlanti Szerződés Szervezete (a továbbiakban: NATO) varsói csúcstalálkozóján hivatalosan is deklarálták, hogy a kibertér önálló hadszíntérnek, műveleti dimenziónak tekinthető, a korábbi fizikai dimenziók mellett (szárazföldi, légi, tengeri, kozmikus). [w26]

Ez azt jelenti, hogy a különféle kibertámadások komoly kihívásként értelmezhetők, továbbá számtalan – a hagyományos támadásokhoz hasonlóan – káros következményt idézhetnek elő napjaink társadalmaira nézve. Éppen ezért már a NATO kollektív védelmi feladatai között is megjelenik a kibervédelem. [35]

A fentebb említettek alapján megállapítható, hogy a kibertér a hadviselés minden területén létfontosságú szerepet tölt be, amelynek köszönhetően elengedhetetlen a haderő kibervédelmi feladatainak vizsgálata.

A Hvt. rendelkezései alapján a Honvédség fegyverhasználat jog nélkül ellátott feladatok közé sorolja a Magyarország biztonságát, honvédelmi érdekeit sértő, veszélyeztető, katonai jellegű kibertér műveletek, kibertérre ható cselekmények vagy kibertámadások elleni fellépést, illetve az ezekkel összefüggő szövetségi, illetve nemzetközi együttműködési keretben megvalósuló feladatok ellátását. [2011. évi CXIII. törvény 36. § (2)] Ezenfelül a Hvt. rendelkezik a kibertér műveletekre vonatkozó különös szabályokról is, így kibertér műveletekkel összefüggő feladatokról. Ennek keretében a [2011. évi CXIII. törvény 62/A. § (1)] bekezdése rögzíti „*a honvédelmi szervezetek kibertérből érkező fenyegetésekkel és támadásokkal szembeni védelmét, az arra történő felkészülést és - a külön jogszabályban meghatározott elektronikus információbiztonsági feladatokra figyelemmel - a kapcsolódó biztonsági feladatokat, valamint az e feladatokkal összefüggésben a folyamatban lévő, kibertérből*

érkező támadás megszakításához szükséges intézkedések végrehajtását, vagy annak kezdeményezését, továbbá külön döntés szerint a Magyarország biztonságát, honvédelmi érdekeit, vagy szövetségesi kötelezettségeit sértő vagy fenyegető rendszerekkel szembeni katonai kibertér műveleti fellépést." Mindez azt is jelenti, hogy a kibertéri műveleti erők mellett az önkéntes tartalékos állományt is fel kell készíteni a kibertérből érkező fenyegetésekkel szembeni védelem megvalósításának lehetőségeire, tekintettel arra, hogy az önkéntes tartalékosok a Honvédség hadkiegészítési szerepét látják el, így kiemelt figyelmet kell fordítani a kibervédelmi képességeinek kialakítására és folyamatos fejlesztésére.

A kibervédelmi képességek elsajátítására békeidőben is szükség van tekintettel arra, hogy az állami működés ma már elképzelhetetlen a különféle információs rendszerek működése nélkül. A kibertéri fenyegetések elhárításához naprakész szakmai ismeretek elsajátítására van szükség, amely megvalósulásának alapvető feltétele a magas színvonalú oktatás és képzés. E képzést a Magyar Honvédség Kiber Képzési Központja biztosítja a katonák számára.

A Kiber Képzési Központ létrehozása mellett fontos megemlíteni a honvédelmi miniszter utasítását, amely a Magyar Honvédség Kiber- és Információs Műveleti Központ kialakításával összefüggő egyes feladatokról rendelkezett. [32/2021. HM utasítás] Az új szabályozás értelmében a Magyar Honvédség parancsnokának alárendeltségébe tartozó kiber- és információs műveleti feladatokat ellátó honvédségi szervezetek szervezeti felépítése és feladatrendszere átalakításra kerül. Ennek keretében a Honvédség katonai kibertéri műveleti képességeinek fejlesztése érdekében az MH Civil-katonai Együttműködési és Lélektani Műveleti Központ 2021. december 31-ei hatállyal megszüntetésre került és annak jogutód szervezeteként további szervezeti elemek beolvadásával a Honvédség hadrendjének részeként 2022. január 1-jei hatállyal MH Kiber- és Információs Műveleti Központ (a továbbiakban: MH KIMK) megnevezéssel új szerv került létrehozásra. [32/2021. HM utasítás 1. §] Az MH KIMK megalakítása és rendeltetése a honvédelmi szervezet 2022. évi kiemelt feladatai között szerepel, amelynek keretében kiemelt figyelmet kell fordítani a meglévő kiberműveleti képességek integrálására és új képességek kialakítására egyaránt. [3/2022. HM utasítás]

A fentiek alapján megállapítható, hogy az információs technológiák, a hozzá kapcsolódó fenyegetések térhódításával és folyamatos fejlődésével, valamint a

kibertér műveleti térré válásával különös hangsúlyt kell fektetni a kibervédelmi képességek kialakítására és folyamatos fejlesztésére az új kihívásoknak megfelelően. Ez azonban nem csak a tényleges szolgálatot teljesítő katonák esetében releváns, hanem az önkéntes tartalékos állomány tagjai számára is, hiszen haderőkiegészítő szerepüknek köszönhetően különleges jogrend esetén a hivatásos állomány erőforrásigényét biztosítják. Ezek alapján az önkéntes tartalékos állomány jövőben ellátandó feladatai vonatkozásában analógia figyelhető meg a hivatásos állománnyal szemben, így a kibervédelmi képességek kialakításával összefüggésben is célszerű, ha nem is ugyanolyan de hasonló elveket képviselni, így azokat fejleszteni. Ezen analógia mentén szükséges megvizsgálni a Honvédség kibervédelmi és kiberműveleti képességeinek fejlesztését célzó intézkedéseket.

Ezt igazolja a 2013-ban kiadott, de továbbra is hatályos a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról szóló utasítás is [60/2013. HM utasítás], amely rögzíti a Honvédség kibervédelmi feladatait. Ennek keretében kiemelt figyelmet fordít a kibervédelmi képesség kialakítására, annak összetettségére, továbbá arra a tényre, hogy az egymásra épülő képességkialakítási feladatok a technológiai fejlődés, valamint a szervezeti feladatok változása miatt az elért eredmények és a környezeti változások elemzésén kell, hogy alapuljanak. Mindemellett az MH Kibervédelmi Képesség kialakítását az alábbi három fő lépés végrehajtásához rendeli.

1. Kezdeti Kibervédelmi Képesség;
2. Alap Kibervédelmi Képesség és
3. Teljes Kibervédelmi Képesség kialakítása.

Fontos megemlíteni, hogy a kiberbiztonság soha nem tekinthető teljesnek, így a „teljes kibervédelmi képesség” meghatározás adott honvédelmi követelmények, információs infrastruktúra és szolgáltatások ismeretében kialakított, azok megfelelő szintű védelméhez igazított képességet foglal magában. A Koncepció rögzíti, hogy a Kezdeti Kibervédelmi Képesség kialakításához szükséges végrehajtandó feladatok részeként értelmezhető az Önkéntes Tartalékos Rendszer igénybevétele és az ebből adódó lehetőségek kihasználása. [60/2013. HM utasítás (7)] Ebből is következik, hogy a kibervédelmi képességek fejlesztése az önkéntes tartalékos állomány esetében is elengedhetetlen. [60/2013. HM utasítás]

4.5.3. MAGYARORSZÁG NEMZETI KATONAI STRATÉGIÁJA

Magyarország Nemzeti Katonai Stratégiájáról szóló 1393/2021. (VI. 24.) Korm. határozatban (a továbbiakban: Katonai Stratégia) is megjelenik az önkéntes tartalékos rendszer szerepe. [1393/2021 Korm. hat.] A Katonai Stratégia kimondja, hogy a kor biztonsági kihívásainak és kockázatainak megfelelni tudó, a reguláris erők feladatait békében és különleges jogrendben is támogatni képes tartalékos erő kiépülése érdekében a Honvédség fokozatosan növeli az önkéntes tartalékos rendszer személyi állományát és képességeit, továbbá felkészíti az alaprendeltetéséből adódó feladatai ellátására. A Katonai Stratégia szerint reális célként értelmezhető, hogy 2030-ra az önkéntes tartalékos rendszer a feladatainak végrehajtásakor egységes, koherens rendszert alkosson a hivatásos és szerződéses állománnyal. A Katonai Stratégia kitér arra is, hogy a többszintű információs hálózatba szervezett műveletvezetési rendszer fejlett kiberbiztonsági képességekkel biztosítja a Honvédség műveleteinek vezetését, akár korlátozó körülmények fennállása esetén is. Mindemellett fontos kiemelni, hogy a Magyar Honvédség képességei moduláris rendszerben épülnek fel, a kialakításra kerülő és folyamatosan fejlesztett katonai kibertér műveleti képességek pedig biztosítani fogják a kibertérből érkező katonai jelentőségű fenyegetések és veszélyek azonosítását, hatékony kezelését, illetve az azokkal kapcsolatos válaszlépések és ellenintézkedések végrehajtását. Ezek a képességek támogatják a szárazföldi erők, a légierő és a különleges műveleti erők kinetikus képességeit, valamint aktívan hozzájárulnak Magyarország kiberbiztonságához. [1393/2021 Korm. hat.]

Összegezve, az önkéntes tartalékos állomány kibervédelmi képességeinek kialakítása és folyamatos fejlesztése elengedhetetlen, tekintettel arra, hogy a kibertérből érkező fenyegetések állandó kihívásként értelmezhetőek, amelyekre történő reagálás nem csak a hivatásos szolgálatot teljesítő katonák, hanem a haderőkiegészítést jelentő önkéntesek feladataként is megjelenik. Ennek köszönhetően a szükséges és elégséges ismerethalmaz definiálására van szükség, amely ismertetésére a következőkben kerül sor.

4.5.4. ÖNKÉNTES TARTALÉKOS ÁLLOMÁNY ÁLTAL ELSAJÁTÍTANDÓ KIBERVÉDELMI KÉPESSÉGEK

A fentiekben bemutatásra került a jogszabályi alapokon nyugvó önkéntes tartalékos állomány kibervédelmi képességeinek fejlesztésére irányuló igény szükségessége.

Ezzel összefüggésben jelen pontban a tartalékosok számára elsajátítandó ismerethalmaz meghatározására kerül sor.

Az önkéntes tartalékos állomány kiberbiztonsági felkészítése érdekében szükséges meghatározni azokat a képességeket és ismerethalmazt, amelynek elsajátításával a tartalékosok képesek lesznek a korszerű technikai eszközök és technológiák hatékony alkalmazására, a honvédelmi szervezetek kibertérből érkező fenyegetésekkel és támadásokkal szembeni védelmének megvalósítására és az arra történő felkészülésre egyaránt, tekintettel arra, hogy az önkéntes tartalékos állomány haderőkiegészítési szerepet tölt be, így egy esetleges háborús helyzet, nemzetközi konfliktus vagy terrorista cselekmény bekövetkezése esetén a tartalékosok bevonhatók a katonai műveletek végrehajtásába.

A tartalékos állomány kibervédelmi képességeinek kialakításához megfelelő alapként szolgálhat a közszolgálati kiberbiztonsági képzés, hiszen tartalmazza mindazon kiberbiztonság megvalósításával kapcsolatos ismereteket, amelyek a kibertámadások hatékony és eredményes megelőzéséhez és elhárításához szükségesek. Fontos azonban, ahhoz, hogy a szükséges tudás- és ismerethalmaz minden részletre kiterjedő definiálása megvalósulhasson, elengedhetetlen a vonatkozó honvédelmi szervezetrendszerrel összefüggő speciális követelmények azonosítása, tekintettel arra, hogy a honvédelmi feladatok ellátása során felmerülő kiberbiztonságot érintő fenyegetések és az alkalmazandó infokommunikációs eszközök köre sok esetben eltér. Ennek következtében a közszolgálati kiberbiztonsági képzésben meghatározott tudás- és képességhalmazt honvédelemspecifikus ismeretekkel szükséges kibővíteni. Ezek alapján a korábbiakban definiált ismerethalmaz a 4-1. táblázat elemeivel bővíthető ki:

Tudás (K)	
KT1	hazai honvédelmi rendszer ismerete
KT2	védelmi infokommunikációs feladatok végrehajtásához szükséges ismeretek
KT3	információs műveletekben alkalmazható technológiák, eljárások és eszközök ismerete
KT4	védelmi célú infokommunikációs rendszerek elleni fenyegetések ismerete

Képesség (A)	
AT1	a katonai és védelmi célú infokommunikációs rendszerek működtetése és használata
AT2	az információs műveletek humán összetevőinek alkalmazása
AT3	honvédelmi feladatot ellátó szervezetek információs rendszereinek biztonságos üzemeltetése
Készség (S)	
ST1	a katonai és védelmi célú infokommunikációs rendszerek működtetésének készsége
ST2	a katonai és védelmi célú infokommunikációs rendszereket célzó fenyegetések hatékony és eredményes megelőzésének, kezelésének készsége

4-1. táblázat A tartalékos állomány számára szükséges tudás, képesség, készség

4.5.5. AZ ÖNKÉNTES TARTALÉKOS ÁLLOMÁNY KIBERBIZTONSÁGI FELKÉSZÍTÉSE

Az önkéntes tartalékos állomány kibervédelmi felkészítésének szükségességét már 2012-ben Krasznay Csaba doktori értekezésében is vizsgálta. Krasznay Csaba meghatározta az önkéntes tartalékos kibervédelmi egység létrehozásának okait, amely alapján megkülönböztethetünk anyagi, humán, tulajdonjogokkal kapcsolatos, hatásköri és tudástranszferrel kapcsolatos indokokat, amelyek mind alátámasztják az önkéntes tartalékos kibervédelmi haderő létjogosultságát. Mindemellett a szerző javaslatot tett a civil szféra Magyar Honvédség által a kibervédelembe történő bevonásának lehetőségeire és szereplőire. [36]

Ugyanakkor nem hagyhatjuk figyelmen kívül a jelen időszakban megvalósuló ukrán-orosz háború történéseiből levonható következtetéseket sem. Így például azt a tényt sem, hogy hibrid hadviselés zajlik és a kibertér már valóságos hadszíntérként jelenik meg, köszönhetően a kiberfegyverek folyamatos alkalmazásának. Fontos kiemelni, hogy Ukrajna korábban nem rendelkezett jelentős kiberhaderővel, ennek ellenére stratégiai jelentőséggel bírt az orosz kibertámadások visszaverésének képessége.

Számos tanulmány foglalkozott a korábbi, kelet-ukrajnai és a Krím-félszigeten megvalósuló orosz-ukrán konfliktus kibertérben megvalósuló tevékenységekről, így például Margarita Levin Jaitner *Orosz információs műveletek: Leckék Ukrajnából*

című tanulmányában az információs fölény megszerzésének szerepét, a kiberkémkedés stratégiai hatásait, az Oroszország által végrehajtott információs műveletek sajátosságait fejtette ki. A szerző szerint az orosz információs műveletek jelentősen hozzájárultak a Krím-félsziget sikeres annektálásához és a kelet-ukrajnai válság kialakulásához. [37]

A fentiek alapján megállapítható, hogy a kibertér nyújtotta műveleti lehetőségek új eszközöket, alternatívákat biztosítanak egy háborús konfliktus során a védekező és a támadó oldalon egyaránt. Ebből következik, hogy a hivatásos állomány mellett a kiképzett tartalékos és az aktív önkéntes tartalékos erőket is fel kell készíteni egy esetleges háborús helyzet vagy nemzetközi konfliktus bekövetkezésének esetére az azonnali hatékony és eredményes reagálás érdekében.

Az előzőekben bemutatásra került az önkéntes tartalékos állomány kibervédelmi felkészítésének szükségessége, azonban emellett meg kell határozni ennek módját, illetve megvalósításának lehetőségeit.

Az önkéntes tartalékos állomány képzése megvalósítható a korábban definiált közszolgálati kiberbiztonsági képzés segítségével. Ennek oka, hogy a közszolgálati kiberbiztonsági képzés tartalmazza azokat a kiberbiztonság megvalósításához szükséges alapismereteket, amelyek elsajátítása az önkéntes tartalékos állomány számára is elengedhetetlen, tekintettel arra, hogy a kibertérből érkező fenyegetések a kibervédelmi és –támadási feladatok végrehajtása azonos alapokon nyugszik, továbbá a képzés tartalma a közszolgálati célcsoportnak köszönhetően illeszkedik az önkéntes tartalékos rendszer sajátosságaihoz. Azonban fontos kiemelni, hogy a kibertérből érkező katonai jelentőségű fenyegetések és veszélyek azonosítása, kezelése, valamint az ellenintézkedések végrehajtása speciális ismereteket is igényel, amelynek elsajátításához szükséges a közszolgálati kiberbiztonsági képzést kibővíteni honvédelemspecifikus ismeretekkel. Ez azt jelenti, hogy a kétéves képzést egy további félévvel indokolt kiegészíteni. E félév során a résztvevők elsajátíthatják az előző alfejezetben azonosított tudás-, képesség-, és készséghalmazt, amelynek keretében megismerkedhetnek a különféle katonai és védelmi célú infokommunikációs rendszereket érintő fenyegetésekkel és a kapcsolódó működtetési, védelmi feladatok végrehajtásával összefüggő feladatokkal egyaránt.

A ráadás félévben meghatározott tantárgyak definiálásához a Katonai Műszaki Doktori Iskolában folytatott tanulmányaim, valamint a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Karának Védelmi Infokommunikációs rendszertervező mesterképzési szak mintatanterve szolgált alapul. [w27] Mindezek alapján az utolsó félévben az alábbi tantárgyak abszolválása szükséges a honvédelmi célú kibervédelmi képességek elsajátításához:

a) Katonai műveletek és a katonai támogatás alapjai
b) Védelmi infokommunikációs rendszerek működtetésének alapjai
c) Elektronikai hadviselés
d) Kognitív befolyásolási eszközei
e) Nemzetközi hadviselés jogi alapjai
f) Szabadon választható tantárgy III.

Katonai műveletek és a katonai támogatás alapjai: tantárgy keretében a hallgatók betekintést nyerhetnek a katonai műveletek alapvető típusaiba, jellegébe, színtereibe, szintjeibe, valamint azok információs környezetébe. Emellett megismerkedhetnek az egyes katonai műveletek támogatásának szerepével és a végrehajtás egyes elemeivel. A tárgy célja továbbá bemutatni az információs műveletek típusait és kibertéri megvalósulásának lehetőségeit.

Védelmi infokommunikációs rendszerek működtetésének alapjai: tárgy során a hallgatók elsajátíthatják a katonai műveletek információs környezetével összefüggő ismereteket, megismerkedhetnek a korszerű katonai infokommunikációs rendszerekkel, valamint azok működtetésének és üzemeltetésének alapjaival. Ennek keretében bemutatásra kerülnek a korszerű infokommunikációs rendszerek és védelmi infokommunikációs hálózatok felépítése, főbb jellemzőik és hadviselésben betöltött szerepük is.

Elektronikai hadviselés: tantárgy betekintés nyújt az elektronikai hadviselés és a felderítés alapjaiba, így különösen az elektronikai támogatás, az elektronikai védelem és az elektronikai ellentevékenység hadviselésben betöltött szerepébe és e tevékenységek tartalmába. Emellett bemutatásra kerülnek az elektronikai felderítés megvalósításának lehetőségei, valamint a kibertérben megvalósuló elektronikai hadviselés elméleti és gyakorlati alapjai.

Kognitív befolyásolás eszközei: tantárgy során a hallgatók betekintést nyerhetnek a kognitív dimenzióban megvalósuló információs tevékenységek ismérveibe, eszközeibe, a kognitív kibertéri műveletek alapjaiba, valamint az információs műveletek kognitív képességeibe.

Nemzetközi hadviselés jogi alapjai: tárgy keretében a hallgatók megismerkedhetnek a hadviselés nemzetközi jogi környezetével, a hazai és nemzetközi katonai szervezetekkel, valamint a NATO és az Európai Unió hadviselésben betöltött szerepével, továbbá az egyes szervezetek felelősségeivel, feladataival.

Összegezve a fent nevesített tantárgyak lehetőséget biztosítanak az önkéntes tartalékos állomány kibervédelmi képességeinek fejlesztésére és ezen keresztül a kibertámadások hatékony megelőzésére, észlelésére, valamint elhárítására.

4.6. A KÉPZÉS FOLYAMATOS FEJLESZTÉSÉNEK BIZTOSÍTÁSA

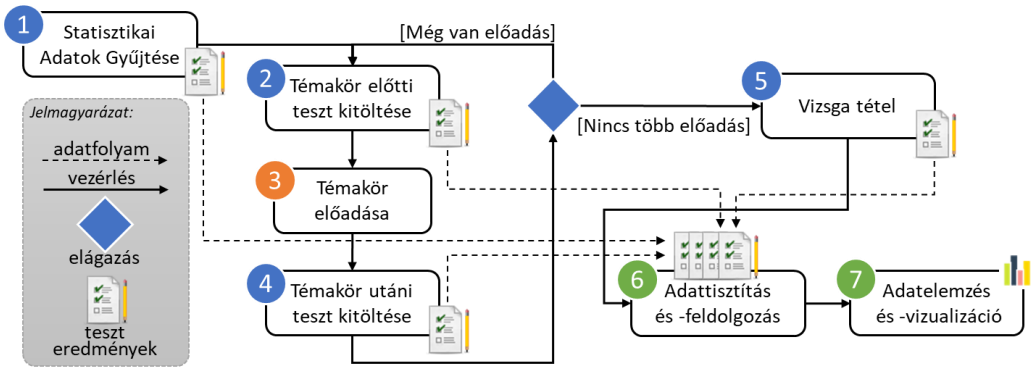
Bár az általam definiált képzés jelenleg kizárólag a tervezés fázisában van, még nem indult el, fontos feladat a képzés folyamatos fejlesztésének biztosítása a tudásátadás hatékonyságának mérése céljából és ezáltal a képzés egyes tárgyainak iteratív fejlesztése. A kialakított mérési környezet definiálását és végrehajtásának lépéseit egy, már folyamatban lévő, rokon területen megvalósított képzés keretében oktatott tantárgy hatékonyságának elemzésével mutatom be, amelynek tematikája esetlegesen felhasználható a közszolgálati kiberbiztonsági képzéshez, mint az általános informatikai alapismeretek tárgy.

4.6.1. MÉRÉSI KÖRNYEZET

4.6.1.1. Mérési folyamat meghatározása

A 4-6. ábra mutatja be azt a folyamatot, amelyet a tudásátadás hatékonyságának mérésére dolgoztunk ki. Első lépésként a hallgatók általános felmérését kell elvégezni, amelynek megfelelően statisztikai adatokat gyűjthetünk. Ezt követően minden témakör oktatása előtt és után olyan tesztet kell kitöltetni a hallgatókkal, amely az adott témakör előadása során elhangzottakra kérdez rá. Ezen tesztek eredményét fogjuk felhasználni a hatékonyság vizsgálata során. Ha az adott tárgy a félév végeztével vizsgával zárul, akkor a vizsgaeredményeket is fel lehet használni a tudásátadás hatékonyságának hosszútávú mérésére. Az összegyűjtött adatokon (teszteredmények,

illetve vizsgaeredmények) adattisztítást kell végezni annak érdekében, hogy csak a méréshez releváns adatokkal kelljen dolgozni. Végül a megtisztított adatok értelmezéséhez, illetve következtetések levonásához az adatokat célszerű vizualizált formában megjeleníteni.



4-6. ábra A mérési folyamat lépései

4.6.1.2. Hatékonyság

A mérési folyamatnak megfelelően a hatékonyságot úgy definiáltuk az egyes témakörök esetén, hogy vettük az oktatás előtt és után mért helyes válaszok százalékos arányának különbségét:

$$hatékonyság_{témakör}[\%] = \left\{\frac{helyes\ válaszok_{témakör}^{oktatás\ után}}{összes\ teszt\ kérdés_{témakör}} - \frac{helyes\ válaszok_{témakör}^{oktatás\ előtt}}{összes\ teszt\ kérdés_{témakör}}\right\} \times 100$$

4-1. egyenlet A hatékonyság képlete

4.6.1.3. Témakörök osztályozása

Szükséges megvizsgálni minden témakör esetén, hogy a hallgatók e tudást maradéktalanul elsajátították-e. A témakörök előadásai után kitöltött tesztek eredményei alapján a témakörök osztályozhatók aszerint, hogy a NICE és ECSF Keretrendszerben rögzített ismereteket milyen mértékben sajátították el a hallgatók. Ehhez egy speciális szempontrendszert dolgoztunk ki. Ez azért elengedhetetlen, mert ennek segítségével megállapítható minden egyes témakör tekintetében, hogy a továbbiakban szükséges-e mélyebb tudásátadás az előadásokon, kellően részletes-e az adott témakör, illetve indokolt-e a téma egyszerűsítése.

A témakörök csoportosításához az átadott tudás szintjét használjuk fel. Ezek alapján a következő csoportosítás alkalmazható:

- 90% felett: *Kiváló*
- 80%-90%: *Jó*
- 70% - 80%: *Közepes*
- 60%-70%: *Elégséges*
- 60% alatt: *Nem megfelelő*

4.6.2. ESETTANULMÁNY: ADATBIZTONSÁGI INFORMATIKAI ALAPISMERETEK

Jelen alfejezetben a fentebb említettek alapján a tudásátadás hatékonyság mérésének lehetséges módszerét a következő esettanulmányon keresztül mutatom be.

4.6.2.1. A tárgy jellegzetességei

A tantárgy során az adatvédelem és az adatbiztonság által meghatározott követelmények informatikai leképeződését kell elsajátítania a hallgatóknak. Itt kerül kifejtésre:

- számítógépes, hálózati és internetes biztonság,
- a védelem szintjei – fizikai védelem;
- a védelem szintjei – informatikai védelem;
- a biztonsági protokoll, a tűzfal és a biztonsági támadások;
- rendszergazdai irányelvek.

Ezen kívül a tantárgy segít megismertetni a hallgatókkal a kibertérből érkező fenyegetéseket és az információs társadalom új típusú kihívásait, valamint bemutatja az adatbiztonság összetevőit, a védelem lehetséges eszközeit, módszereit.

Jelen tantárgyat az Eötvös Lóránd Tudományegyetem Állam- és Jogtudományi Kar által szervezett Adatbiztonsági és adatvédelmi szakjogász képzés második félévében tartottuk meg 6 kredit értékben[9], kizárólag előadások formájában, gyakorlati oktatásra nem került sor. A tárgy teljesítése kollokvium keretében, tesztfeladatok megoldásával történt a félév végén. A mérést a 2018/19-es tanév tavaszi szemeszterében végeztük.

[9] A jelenlegi felsőoktatási rendszerben a kredit a tanulmányok elvégzése során alkalmazott mérőeszköz, amely a tantárgy súlyozására és típusának meghatározására szolgál.

4.6.2.2. *A mérés körülményei*

A mérési folyamatnak megfelelően az első előadás során egy általános információbiztonság-tudatosság mérésére szolgáló tesztet töltettünk ki a hallgatókkal. Ennek célja, hogy felmérjük a hallgatók általános biztonságtudatosságának szintjét, valamint a statisztikai kérdéseknek köszönhetően számos további következtetést határozzunk meg az egyes témakörök esetében. Ezt követően minden témakör oktatása előtt és után a hallgatók egy, a témára vonatkozó tesztet töltöttek ki. Témakörönként különböző kérdések, de a témakörök előtt és után azonos kérdéseket válaszoltak meg a hallgatók. A témakörökhöz kapcsolódó kérdések minden esetben szorosan illeszkedtek az előadáson elhangzott tananyaghoz. Tesztenként öt feleletválasztós kérdésre kellett válaszolniuk a hallgatóknak négy lehetséges opcióból a Kahoot alkalmazáson[10] keresztül. Ezek a kérdések a félév végén bekerültek a vizsgakérdések közé is, amely az egyetem Moodle rendszerén keresztül került kitöltésre.

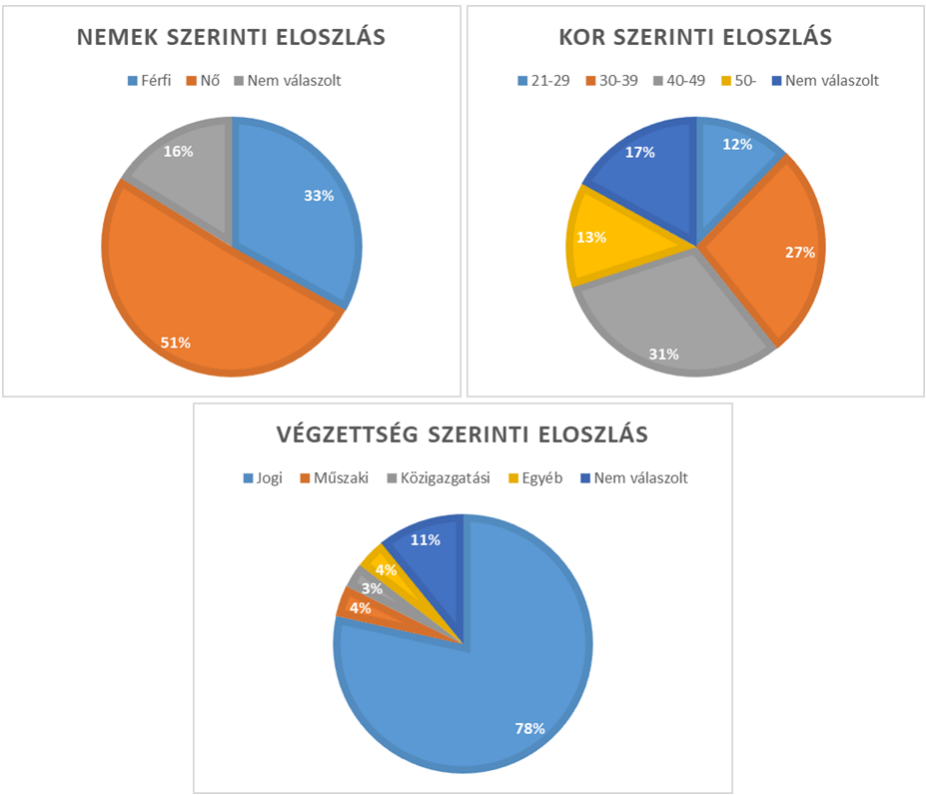
4.6.2.3. *A hallgatóság összetétele*

A hallgatóság összetételét az első, általános információbiztonság-tudatosság mérésére szolgáló teszt alapján vizsgáltuk nem, kor és végzettség szerint, amelyek eloszlását a 4-7. ábra szemlélteti. A teszt kitöltése előtt a hallgatók beleegyezését kértük azzal kapcsolatban, hogy a félév során összegyűjtött adatokat anonim módon a kutatásban felhasználhassuk, ezzel teljesítve az adatvédelmi követelményeket.

Összesen 130 hallgató töltötte ki a tesztet, 51%-uk nő (66 fő) és 33%-uk férfi (43 fő), a maradék 16% (21 fő) erre a kérdésre nem válaszolt. A nemek szerinti eloszlás alapján megállapítható, hogy a hallgatók többsége nő.

A kor szerinti eloszlás vizsgálatára négy életkori kategóriát állapítottunk meg. A hallgatók 12%-a (16 fő) 21-29 év közötti, 27%-a (35 fő) 30-39 év közötti, 31%-a (40 fő) 40-49 év közötti, 13%-a (17 fő) 50 éves vagy annál idősebb. Az életkorra vonatkozó kérdésre a hallgatók 17%-a, összesen 22 fő nem válaszolt. A kor szerinti eloszlás alapján a kérdésre válaszoló hallgatók többsége a 40-49 év közötti kategóriába tartozik.

[10] A Kahoot egy kvíz alapú oktatási platform, amely lehetővé tesz a hallgatók ismereteinek áttekintését, értékelését feleletválasztós kvíz tesztek segítségével. Bővebb információ elérhető a következő weboldalon: https://kahoot.com/

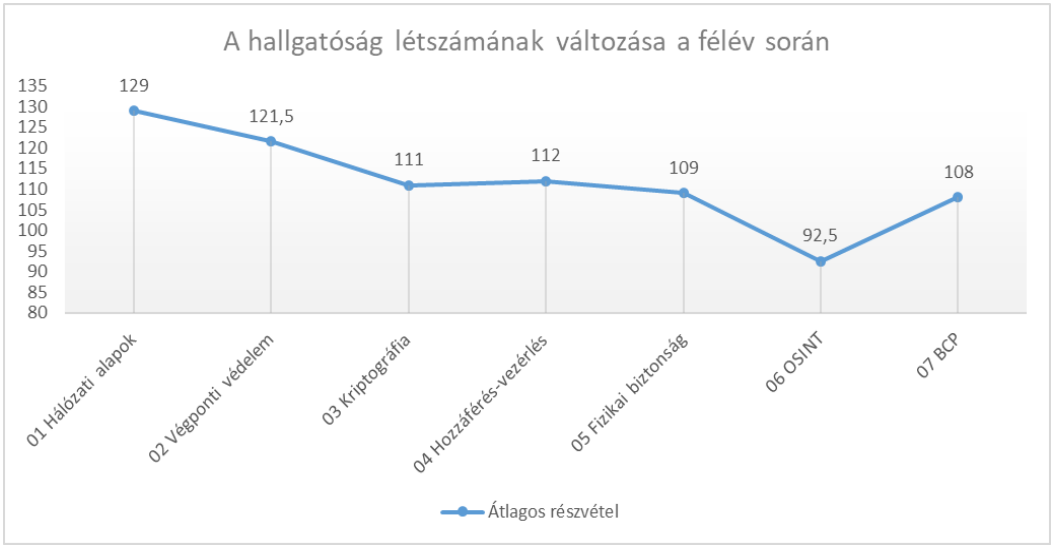


4-7. ábra A hallgatóság összetétele nem, kor, végzettség szerint

A hallgatók végzettségének megállapítására szintén négy kategóriát határoztunk meg. A hallgatók 72%-a (102 fő) jogi, 4%-a (5 fő) műszaki, 3%-a (4 fő) közigazgatási és 4%-a (5 fő) valamilyen egyéb területen szerzett végzettséget. Erre a kérdésre a hallgatók 11%-a (14 fő) nem válaszolt. Ezek alapján megállapítható, hogy a hallgatók túlnyomó többsége jogi végzettséggel rendelkezik, de más előképzettséggel rendelkező hallgatók is részt vettek a képzésen.

4.6.2.4. *A hallgatóság létszámának változása*

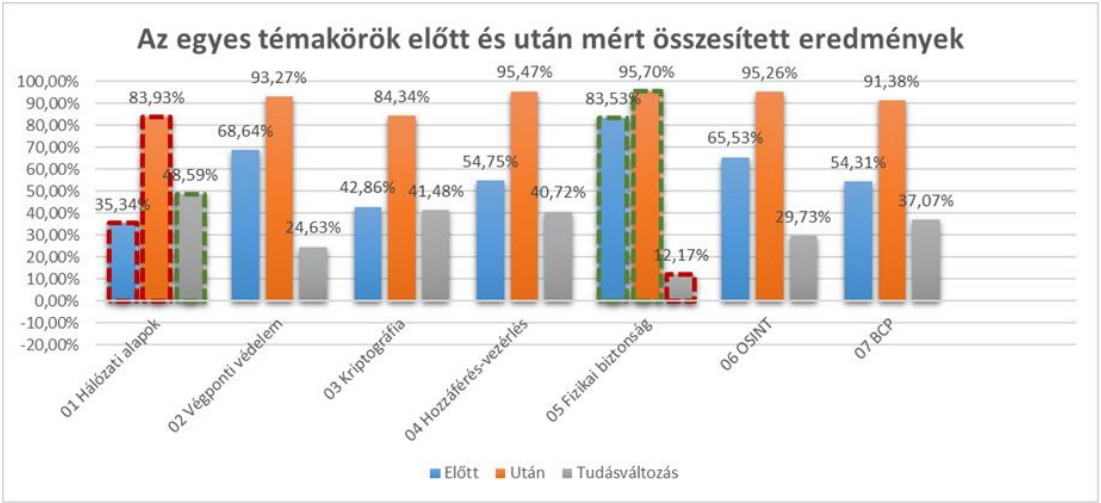
A mérés eredményeinek érvényességét befolyásolta a tesztet kitöltő hallgatók létszáma az adott témakör előadásán. A 4-8. ábra a hallgató létszámváltozását szemlélteti a félév során. Ezek alapján megállapítható, hogy kis mértékben, de folyamatosan csökkent a létszám. A hallgatói létszámcsökkenés számos okkal magyarázható, köszönhető többek között a féléves terhelésnek, a házi feladatok és zárthelyi dolgozatok gyakoriságának.



4-8. ábra A hallgatóság létszámának változása a félév során

4.6.2.5. *Adatelemzés, áttekintés*

Az egyes témakörök előtt és után kitöltött tesztek százalékos arányát, valamint az egyes témakörök tudástranszferjének hatékonyságát vizsgáltuk, aminek eredményeit a 4-9. ábra mutatja be.



4-9. ábra Az egyes témakörök előtt és után mért összesített eredmények

A 4-9. ábra eredményeibe minden olyan hallgató válasza beleszámít, akik részt vettek a teszt kitöltésében, függetlenül attól, hogy kitöltötték-e az első órán megtartott általános kérdőívet.

a) *1. témakör – Hálózati alapok:* Az első témakör a Hálózati alapok címet viseli, amely összefoglalja és részletezi a számítógép-hálózatokhoz kapcsolódó alapfogalmakat, alapismereteket. A téma oktatása előtt egy öt kérdésből álló tesztet töltöttek ki, amelyre a hallgatók 35,34%-ban válaszoltak helyesen. Az óra végén ugyanazt a kérdéssort kapták a hallgatók, amely esetén már 83,93%-ban választották ki a megfelelő megoldásokat. Ezen téma esetében 48,59%-os tudásváltozás állt be, amely azt mutatja, hogy az órán elhangzottak alkalmasak voltak tudásuk bővítésére. Jelen témakör esetében megállapítható, hogy az összes téma közül itt teljesítettek a legrosszabbul az oktatás előtti teszten a hallgatók (35,34%), és a tanítás utáni kérdéssorok esetében is (83,93%). Az összes témakörhöz viszonyítva ennek ellenére jelen témakörnél valósult meg a leghatékonyabb tudástranszfer, ugyanis a korábban említett 48,59%-os tudásváltozás a legmagasabb az összes témakör között.

b) *2. témakör – Végponti védelem:* A második, Végponti védelem című témakör a különféle kártékony programokat és az ezek elhárítására, megelőzésére szolgáló lehetséges alternatívákat, védelmi mechanizmusokat ismerteti. Ez esetben a tanítás előtti kérdéssorra 68,64%-os arányban érkeztek helyes válaszok, míg az előadás végén 93,27-os arányban. A hallgatók tudásának változása az előadás előtthöz viszonyítva 24,63%-os volt.

c) *3. témakör – Kriptográfia:* A harmadik téma a Kriptográfia kérdéskörét öleli fel, amelyben kifejtésre kerültek többek között a főbb alapfogalmak, a kriptográfia története és módszerei, valamint az elektronikus aláírás alapjai is. Az oktatás előtti tesztre a hallgatók 42,86%-os arányban válaszoltak helyesen, az előadás végén pedig 84,34%-os arányban érkeztek helyes válaszok. A Kriptográfia téma esetében a tudásváltozás az összes téma tekintetében a második legmagasabb, 41,48%-os volt.

d) *4. témakör – Hozzáférés-vezérlés:* A negyedik témakör a Hozzáférés-vezérlés címet viseli, amely részletezi a kapcsolódó fogalmakat, elveket, a hozzáférés-ellenőrzés típusait, az esetleges védelmi intézkedéseket és a mobilbiztonság alapvető elemeit, lehetőségeit. Az előadás előtti kérdéssorra 54,75%-ban érkeztek helyes válaszok, míg a végén 95,47%-ban, amely a második legjobbnak értékelhető az összes témakör között. A hallgatók tudásváltozása 40,72%-os volt a két teszt között.

e) *5. témakör – Fizikai biztonság:* Az ötödik, Fizikai biztonság nevű témakör összefoglalja a fizikai biztonság alapjait, szükségességét, módszereit, a különféle információbiztonsági követelmények tartalmát, valamint a biztonsági technológiák és eszközök fontosságát és lehetőségeit. Az oktatás előtti tesztre 83,53%-ban, míg az oktatást követően 95,70%-os arányban érkeztek helyes válaszok. Az összes témakör közül a Fizikai biztonság esetén érkezett a legtöbb jó válasz a témáról tartott előadás előtt és után is, kifejezetten magas értéket mutatott az előadás előtti teszt is, amelyből következik, hogy a tudásváltozás, a magas bemeneti értékeknek köszönhetően jelen témánál volt a legalacsonyabb, mindössze 12,17%.

f) *6. témakör – Nyílt forrású információszerzés (OSINT):* A hatodik téma az OSINT (Open Source Intelligence vagy másnéven nyílt forrású információszerzés) kérdéskörét felölelő előadás, amely tartalmazza többek között az ehhez kapcsolódó alapismereteket, a lehetséges eszközök és módszerek, valamint a védelem alternatíváit is. Az előadás előtti teszten a hallgatók 65,53%-os arányban, míg az előadást követően 95,26%-os arányban válaszoltak helyesen. Ezek alapján megállapítható a hallgatók tudásváltozása, amely 29,73%-os arányú volt.

g) *7. témakör –Üzletmenet-folytonossági terv (BCP):* A hetedik, vagyis az utolsó téma a BCP (Business Continuity Plan, másnéven üzletmenet-folytonossági terv, amely magában foglalja az üzletmenet-folytonosság alapjait, az ehhez szükséges dokumentációkat és azok tartalmát. A témából tartott előadás megtartása előtt a hallgatók 54,31%-os arányban teljesítették helyesen a tessztet, míg az oktatást követően 91,38%-os arányban, ezek alapján a tudásuk változása 37,07%-os volt.

Összességében megállapítható, hogy minden témakör esetén megvalósult valamilyen szintű tudásátadás, átlagosan 33,48%-os tudásváltozás volt jellemző az oktatást követően, az oktatást megelőző tudásszinthez viszonyítva. Az ötödik, fizikai biztonság nevű téma esetében rendkívül alacsony (12,17%-os) volt a tudástranszfer, amelyből további következtetések vonhatók le. Általában, amennyiben a tudásváltozás alacsony, úgy mélyebb, részletesebb tudásátadásra van szükség, tehát ilyen esetekben az adott témakör ismereteinek mélyítése indokolt. A konkrét esetben azonban magas bázisról indult a teszt, azaz a hallgatók jól ismerték a fizikai biztonsággal kapcsolatos

alaptéziseket, köszönhetően annak, hogy míg a kibertéri veszélyek a felmért csoport számára meglehetősen absztraktak, a fizikai tér kihívásait jól ismerik.

4.6.2.6. *Osztályozás és javaslatok*

A bemutatott témaköröket a korábban rögzített osztályozás módszer alapján az alábbi csoportokba lehet helyezni:

- 1. témakör – Hálózati alapok: *Jó*
- 2. témakör – Végponti védelem: *Kiváló*
- 3. témakör – Kriptográfia: *Jó*
- 4. témakör – Hozzáférés-vezérlés: *Kiváló*
- 5. témakör – Fizikai biztonság: *Kiváló*
- 6. témakör – OSINT: *Kiváló*
- 7. témakör – BCP: *Kiváló*

Ezen szempontrendszer és csoportosítás alapján megállapítható, hogy a célul kitűzött tudásmennyiséget szinte kiválóan sikerült átadni a hallgatók számára a tárgy keretében, hiszen a hét témakörből öt esetén 90% feletti eredményt értek el és a maradék két témakör is jó „osztályzatot” ért el.

Ahhoz, hogy a tárgy keretében minden témakör kiváló minősítést kapjon érdemes lenne a két „Jó” minősítéssel rendelkező témakört részletesebben oktatni, amely egyben azt is jelenti, hogy ezen előadások tekintetében az előadás hosszát, idejét növelni kell. Ennek következménye, hogy más témaköröknek az előadási idejét rövidíteni szükséges, célszerű azon témakörök előadásának hosszát csökkenteni, amelyek esetében a bemeneti tudás 80% feletti (pl. fizikai biztonság témaköre, ahol a témakör előtti teszt eredmények 83,53%-os volt).

A rosszabb eredményt elért témakörök esetén előfordulhat, hogy túl bonyolult volt a tananyag, ezért annak egyszerűsítése válik szükségessé.

További következtetések fogalmazhatók meg a „Kiváló” minősítéssel rendelkező témakörök esetében is. Ezen témakörök ismeretanyaga kellően részletes és megfelelően fedi a szükséges alapismereteket, így ezen előadások tartalmát tekintve további változtatási, módosítási teendő nincs. Kivételt képez ez alól a fentebb említett magas bemeneti értékű témakör, amely esetén a hallgatók alaptudása magas volt, így ezen témáknál lehetőség nyílik az előadások időtartamának rövidítésére a többi témakör javára.

4.6.2.7. *A részkutatást befolyásoló tényezők*

Jelen pontban szükséges megemlíteni a hatékonyság mérésére irányuló részkutatás eredményét befolyásoló egyéb tényezőket. A kutatás során számos olyan tényező befolyásolta a kutatás lefolytatását és annak eredményét, amelyet mindenképp szükséges figyelembe venni a kutatás értékelésekor, a hipotézisek megválaszolásakor, illetve a következtetések megfogalmazásakor. Ezek alapján felmerülhet a kérdés, hogy milyen tényezők befolyásolhatták az eredményeket?

Az első ilyen tényező, hogy jelen kutatásban kizárólag egy évfolyamot vizsgáltunk, mivel korábbi évek statisztikái nem állnak rendelkezésre. Így csak ezen évfolyam tekintetében tudunk következtetéseket megfogalmazni. Jelen részkutatásban ellenpéldát nem elemeztünk. Ennek következtében további megválaszolandó kérdések merülnek fel, például milyen eredmények születnének abban az esetben, ha nagyobb mennyiségű, illetve részletesebb ismeretanyagot adnának át a hallgatók számára?

Ezenkívül az eredmények kiértékelését nehezítette, valamint az elemezhető hallgatói eredmények számát csökkentette az a tény, hogy voltak olyan hallgatók, akik vagy az óra elején nem voltak még jelen, vagy pedig korábban távoztak az előadásról.

Továbbá meg kell még említeni, mint befolyásoló, illetve nehezítő körülményt, hogy a jelen értekezés alapjául szolgáló közszolgálati kiberbiztonsági képzés esetén csak feltételezéssel élünk a hallgatók előképzettségének aránya tekintetében, illetve nem tudhatjuk, hogy az adott ismeretanyagot milyen mértékben képesek elsajátítani az egyes területekről érkező személyek, még hogyha a tudásuk azonos szinten is van az adott témában. Mindemellett érdemes megvizsgálni a továbblépési lehetőségeket is, a tananyag hosszútávú beépülésével kapcsolatban. Ezt a félévi vizsga útján lehet megtenni. A vizsgált szemeszterben a vizsgáztatás során lehetővé tettük, hogy a hallgatók egy 24 órás időintervallumban megnyithassanak egy Moodle-alapú tesztfelületet és ott egy előre megkonstruált kérdéssort tölthessenek ki. Ez 20 kérdésből állt, és összesen 30 perc állt rendelkezésre a kitöltéshez. A számonkérés megkönnyítése érdekében a teszt mindenkinek ugyanaz volt, de a feleletválasztós tesztek és ezeken belül a lehetséges megoldások véletlenszerűen keverve jelentek meg. A kérdések a CISSP-vizsga mintakérdései közül kerültek ki. Összesen 218 kitöltés született, átlagosan a 93,58%-os végső eredménnyel. A magas sikerrátában szerepe van annak, hogy a jó megoldásokat az évfolyamon belül a hallgatók megosztották egymással, de mivel módszertanilag jelen részkutatásban nem volt célunk objektív

mérést végezni ezen a területen, pusztán a mérési módszertan lehetőségeit kívántuk kipróbálni, az eredmény nem befolyásolja megállapításainkat. További kutatásaink során azonban ezt a faktort is alaposabban tervezzük megvizsgálni.

Összességében megállapítható, hogy a korábban említett befolyásoló tényezők ellenére is jelen kutatás megfelelő kiindulóalapot jelent a tudástranszfer hatékonyságának méréséhez képzési programtól függetlenül.

4.7. KÖVETKEZTETÉSEK

Jelen fejezetben ismertetett kutatás egyfajta előkészítése és egyben bizonyítása volt az 4.1.1 pontban meghatározott alhipotézisek megválaszolásának.

A H-4.1 alhipotézis megfogalmazásakor abból a feltételezésből indultam ki, hogy meghatározható a magyar közszolgálat számára egy felsőoktatási kiberbiztonsági képzés. E hipotézis igazolására definiáltam a közszolgálati kiberbiztonsági képzés alapvető elemeit, képzési struktúráját, melynek keretében meghatároztam a képzés célját, valamint a képzés és annak alapjául szolgáló kibervédelmi képesség fogalmát. Emellett rögzítettem a bemeneti és kimeneti követelményeket, amely elengedhetetlen a képzés célcsoportjának vonatkozásában.

A H-4.2 alhipotézis a képzés alapvető elemét képező struktúra, tantervi háló és értékelési rendszer meghatározását tartalmazza, amely bizonyítására definiáltam a képzés struktúráját, elemeit, az elméleti és gyakorlati rész általános tartalmát, valamint a tantervi háló keretében meghatároztam a képzés egyes tantárgyait, azok rövid tartalmát és a kapcsolódó értékelési rendszer általános leírását.

A H-4.3 alhipotézis szerint vélelmeztem, hogy mérhető egy tantárgy oktatása során megvalósuló tudásátadás hatékonysága. Ennek bizonyítása során a képzés lehetséges fejlesztését, így az egyes tárgyak során átadott tudás hatékonyságának mérését vizsgáltam témavezetőmmel. Ennek keretében megállapítottuk, hogy definiálható egy szempontrendszer, amely alapján osztályozható, hogy a tantárgy keretében átadott tudás kellően részletes-e, amely egy, már folyamatban lévő rokon területen megvalósított képzés keretében oktatott tantárgy hatékonyságának elemzésével történt. A kutatás keretében megvizsgáltuk, hogy a tárgy keretében hatékony volt-e a tudástranszfer, amelynek érdekében definiáltuk a hatékonyság fogalmát és elemeztük az egyes tárgyak hatékonyságát. Emellett arra a kérdésre kerestük a választ, hogy a

tantárgy tematikája alkalmas-e a szükséges informatikai alapismeretek elsajátítására, átadására. Az állítottuk, hogy a korábbiakban meghatározott ismeretanyag megfelelően fedi a szükséges informatikai alapismeretek halmazát, amely magában foglalja az általunk kiválasztott ismertetett NICE és ECSF Keretrendszerben rögzített adatvédelmi tisztviselő munkakör betöltéséhez elsajátítandó informatikai alapismereteket. Ezért a vizsgált tantárgy a hipotézisben szereplő szükséges informatikai alapismeretek átadását maradéktalanul teljesíti. Továbbá extra témákat is érint (például OSINT), amely a kezdeti célokat túl is teljesíti.

4.8. ÚJ TUDOMÁNYOS EREDMÉNYEK

Jelen fejezetben bemutatott kutatás segítségével **bizonyítottam, hogy definiálható egy olyan, a közszolgálat fejlesztését célzó képzési program, amelynek teljesítése nem igényel informatikai előképzettséget (E4).**

Jelen fejezetben bemutatott kutatás alapján az alábbiakat tekintem új tudományos részeredménynek:

Tudományos részeredmény 1. Definiáltam a magyar közszolgálat számára egy felsőoktatási kiberbiztonsági képzést.

Tudományos részeredmény 2. Meghatároztam a képzés alapvető elemét képező struktúra komponenseit, tantervi hálóját és a képzés általános értékelési rendszerét.

Tudományos részeredmény 3. Egy, a képzés profiljába illeszkedő tantárgy oktatása során megvalósuló tudásátadás hatékonyságának mérésére szolgáló módszert dolgoztam ki, valamint definiáltam egy szempontrendszert, amely alapján osztályozható, hogy a tantárgy keretében átadott tudás kellően részletes-e.

Tudományos részeredmény 4. Javaslatot fogalmaztam meg az önkéntes tartalékos állomány kibervédelmi képességeinek fejlesztésére a közszolgálati kiberbiztonsági képzés felhasználásával és kibővítésével.

Jelen fejezet a [j1], [f1] és [f3] publikációkra épül, amelyek részletesen támasztják alá az első három tudományos részeredményt. A [j1] folyóiratcikkben definiáltam a közszolgálati kiberbiztonsági képzés struktúráját, elemeit, valamint a kétlépcsős gyakorlati képzés keretében megvalósuló elméleti és gyakorlati rész általános tartalmát, amely magában foglalja az elsajátítandó kiberédelmi mechanizmusokat, ismeretköröket. Az [j1] publikációban definiáltam a közszolgálati kiberbiztonsági képzést, annak be- és kimeneti követelményeit, valamint főbb elemeit a korábban meghatározott ismerethalmaz segítségével. Az [f3] publikációban meghatároztam a tudásátadás hatékonyságát mérő koncepciót, amely alapján megvizsgáltuk egy, a közszolgálati kiberbiztonsági képzés profiljába illeszkedő tantárgy tartalmának megfelelőségét, valamint az egyetemi oktatás során megvalósuló tudásátadás hatékonyságát.

5. MŰSZAKI KERETRENDSZER MEGHATÁROZÁSA

5.1. BEVEZETÉS

A kiberbiztonság szerepe egyre nagyobb teret nyer az infokommunikációs eszközök és technológiák folyamatos fejlődésének köszönhetően. A hackerek a felhasználók előtt járnak egy lépéssel, így mindig újabb és újabb kihívásokkal kell megküzdeni, ha biztonságban szeretnénk tudni információinkat és eszközeinket.

Számos kibertérből érkező támadás veszélyeztetheti a saját infokommunikációs eszközeinket így például hordozható számítógépünket, mobiltelefonunkat televíziónkat, okosóránkat és egyéb okos eszközeinket. Gyakran tapasztalható, hogy a felhasználók csak felületesen ismerik eszközeik biztonságának összetevőit, valamint a hatékony és eredményes védekezési módszereket. Ebből következik, hogy a kiberbiztonság egyik legnagyobb rizikóját a gyakorlati képességek hiánya okozza, amely számos tanulmányban is rögzítésre került. Conklin, Cline és Roosa szerint a kiberbiztonsági oktatás egyik legnagyobb problémája a hallgatók gyakorlati tapasztalatainak hiánya, amely azt eredményezi, hogy az elsajátított készségek nem felelnek meg a versenyszféra igényeinek. [38]

Több kutatás is vizsgálta már a kiberbiztonság oktatásának lehetőségeit, amelynek keretében olyan platformokat is kialakítottak, amelyek során a kibertámadások a gyakorlatban is kipróbálhatóak. A probléma azonban sajnos az, hogy a legtöbb felhasználó nem rendelkezik részletes informatikai szaktudással, ami miatt az így átadható tudást nehezen vagy egyáltalán nem képesek elsajátítani. A meglévő platformok bár lehetőséget adnak a védelmi stratégiák kipróbálására, azonban olyan jellegű megoldásokat nem lehet találni, amely elsősorban a védekezésre fókuszálna.

Emiatt fontos feladat egy olyan gyakorlati képzés kialakítása, ahol a résztvevő hallgatók valós helyzetekben élhetik át a kibertámadásokat és a védekezésre fókuszálnak úgy, hogy a támadás részletes felépítését, kialakítását, technikai hátterét nem szükséges ismerni. Egy ilyen gyakorlati képzés kialakítása komplex támadások implementációját igényli mind szervezeti szinten (szerver komponensek, VPN, egyéb perifériák stb.) mind személyes szinten (hordozható laptopok, mobiltelefonok stb.). Ezek alapján a gyakorlati képzést két szinten szükséges megvalósítani – igazodva a

közszolgálati kiberbiztonsági képzés tantervéhez - saját infokommunikációs eszközök védelme, illetve szervezeti szintű rendszerek üzemeltetése és védelme tantárgyak keretében.

A jelen értekezés alapjául szolgáló közszolgálati kiberbiztonsági képzés egy gyakorlatban is alkalmazható szakmai tudást, valamint problémafelismerő és -megoldó készséget nyújt résztvevőinek, amely elsajátításával képesek azonosítani, feltérképezni a kibertámadások támadási felületeit és képesek megelőző lépéseket tenni azok eredményes elhárítása érdekében.

Jelen fejezetben bemutatom a kétlépcsős gyakorlati képzés működési környezetét, ahol a hallgatók egy fiktív szervezeti infrastruktúra általános architektúráját, komponenseit, illetve azok védelmi mechanizmusait azonosítják, majd szimulált kibertámadások során védelmi stratégiákat alkalmaznak. Ennek megvalósítása érdekében azonosítom a gyakorlati képzés alapját képező szimulációs környezetet leíró keretrendszert, amely a közszolgálatban dolgozó személyek kibertámadások felismerésére és elhárítására irányuló felkészítését szolgálja. Emellett ismertetek egy egyszerűsített szimulációs környezetet, amelyet a közszolgálati kiberbiztonsági képzés kapcsolódó saját infokommunikációs eszközök védelmére vonatkozó gyakorlati oktatásra készítettem, ahol olyan kibertámadásokat mutatok be a gyakorlatban a hallgatóknak, amelyek elhárításához nem szükséges mély informatikai tudás.

5.1.1. HIPOTÉZISEK

Jelen fejezetben vizsgált hipotézis szerint azzal a feltételezéssel éltem, hogy **definiálható egy olyan műszaki keretrendszer, amely lehetőséget biztosít kibertámadások elleni védelmi stratégiák gyakorlatban történő alkalmazására (H5)**. Ennek igazolására az alábbi alhipotéziseket azonosítottam, a melyek megválaszolását tűztem ki célul jelen fejezetben bemutatom részkutatásommal. Az alhipotézisek a következők:

H-5.1. Definiálható egy szimulációs környezetet leíró keretrendszer, amely segítségével a közszolgálatban dolgozó személyeket fel lehet készíteni a kibertámadások elleni védekezésre.

H-5.2. Kialakítható egy automatizált értékelési rendszer, amely alkalmas a gyakorlati képzési rész során átadott tudásanyag számonkérésére.

H-5.3. Szimulálható olyan kibertámadás, amely azonosításához és megoldásához nem szükséges mély informatikai tudás.

H-5.4. A szimulációs keretrendszer felhasználható a közszolgálati kiberbiztonsági képzés során.

5.1.2. FELHASZNÁLT KUTATÁSMÓDSZERTAN

A H-5.1 alhipotézisek igazolására egy szimulációs környezetet leíró keretrendszert definiáltam dokumentumelemzés és tesztelés segítségével, ahol egy adatbázisban definiálhatóak különböző alkalmazás, illetve infrastruktúra szintű kibertámadások egy szervezetet reprezentáló hálózattal szemben.

A H-5.2 alhipotézis igazolására kibővítettem a kibertámadások definíció adatbázisát a szervezetet reprezentáló hálózat rész állapotaival, amelyek teljesülése folyamatosan monitorozható egy tanári számítógépen keresztül. A támadás elhárítása akkor tökéletes, ha minden részállapotot elér egy hallgató a támadás elleni küzdelem során.

A H-5.3 és H-5.4 alhipotézisek igazolására definiáltam egy egyszerűsített prototípus infrastruktúrát, amelynek két fő eleme van: egy támadó és egy áldozati gép, melyek egy hálózatban találhatóak. Ennek segítségével a támadó képes egy kibertámadást végrehajtani az áldozat gépe ellen, így valós támadás szimulálható a felhasználó számára. Majd ezek után három valós támadó forgatókönyvet definiáltam, amely a prototípus infrastruktúrán végre is hajtható, amelyhez virtuális gépek pillanatkép felvételét (snapshot) használtam fel. A szimulációs keretrendszert integráltam egy jelenleg népszerű e-learning platformra (Moodle), ahol a támadásokhoz egy-egy gyakorlatot és vizsgát is összeállítottam, amelyeket mély informatikai tudással nem rendelkező személyekkel teszteltettem.

5.1.3. FEJEZET SZERKEZETE

Az 5.2 alfejezetben bemutatom a gyakorlati oktatások sajátosságaival, műszaki keretrendszerek kialakításával összefüggő hazai és nemzetközi szakirodalmat, valamint egy előzetes fogalmi áttekintést rögzítek az azonos fogalomhasználat érdekében. Ezt követően az 5.3 alfejezetben ismertetem a szimulációs keretrendszert, amely alkalmazás és infrastruktúra szintekre bontható. Ezután az 5.4 alfejezetben bemutatok egy egyszerűsített szimulációs környezetet, amely felhasználható a köszszolgálati kiberbiztonsági képzés gyakorlati részének megvalósítása során és

amelyen kibertámadások szimulációja hajtható végre. Végezetül ugyanebben a fejezetben ismertetem az általam szimulált kibertámadásokhoz definiált oktatási anyagot és vizsgát, amelyeket a Moodle e-learning platformon alakítottam ki.

5.2. KAPCSOLÓDÓ SZAKIRODALMI ÁTTEKINTÉS

5.2.1. KIBERBIZTONSÁGI GYAKORLATI OKTATÁS KÖRNYEZETÉVEL KAPCSOLATOS TANULMÁNYOK

Topham és szerzőtársai tanulmányukban kifejtik, hogy rendkívül nagy igény mutatkozik a gyakorlati készségekkel rendelkező képzett kiberbiztonsági szakemberekre, hiszen a mindennapi életünk számtalan területén a technológiára támaszkodunk, amely zökkenőmentes működéséhez elengedhetetlen a szakértők bevonása, alkalmazása. A cikk betekintést nyújt a kiberbiztonság gyakorlati oktatásában alkalmazott módszerekbe, megközelítésekbe, valamint követelményeket és jó gyakorlatokat is meghatároznak a jövőbeli képzési módszerekkel kapcsolatban. Ennek keretében a szerzők bemutatják és összehasonlítják az egyes gyakorlati laboratóriumok típusait, azok jellemzése során néhány példát is elemeznek, majd javaslatokat, illetve követelményeket is meghatároznak a jövőbeli platformokra vonatkozóan. A szerzők három laboratórium típust azonosítanak, ezek a fizikai, szimulációs és a virtuális laboratóriumok. A tanulmány meghatározza azon tanítási folyamattal kapcsolatos követelményeket, amelyeknek minden kiberbiztonsági laboratóriumnak meg kell felelnie. Annak érdekében, hogy a tanárok valós helyzetek, támadások forgatókönyveit és gyakorlatait el tudják készíteni, a laboratóriumnak a rugalmasság elve mentén kell biztosítani a feltételeket a minél kreatívabb gyakorlatok végrehajtása céljából. Az oktatóknak képesnek kell lenniük a gyakorlati feladatok gyors és egyszerű megjelenítésére egyszerre több hallgató számára. A laboratórium infokommunikációs eszközeit és szoftvereit el kell különíteni a külső hálózatoktól. Lehetővé kell tenni a hallgatók számára a hozzájuk kijelölt géphez adminisztrációs jogok biztosítását, amely elengedhetetlen bizonyos kísérletek esetében. Garantálni kell a folyamatos tárolást és biztonsági mentést annak érdekében, hogy a hallgatók munkájának folytonossága és egy esetleg hiba esetén a helyreállítás biztosított legyen. [39]

Williems és szerzőtársai a gyakorlati kiberbiztonsági oktatás lehetőségeit kutatják, amely során a Tele-Lab platformot, annak működését, használatát mutatják be részletesen. A Tele-Lab egy olyan távoli virtuális laboratóriumi környezetben megvalósuló gyakorlati kiberbiztonsági képzési rendszert biztosít, amely mindenki számára elérhető. A szerzők felvázolják a klasszikus laboratóriumi képzésen alapuló gyakorlati kiberbiztonsági oktatás alapjait, annak hátrányait. Ilyen hátrány például, hogy a klasszikus számítógépes laboratóriumok eszközei nehezen mozdíthatók, megvásárlásuk és fenntartásuk drágának tekinthető, nem megengedett az internet hozzáférése, továbbá elengedhetetlen ezen eszközök elkülönítése más hálózatoktól. Ezen kívül számos további szoftverekkel, szimulációs rendszerekkel kapcsolatos hátrányt is említ a tanulmány. Ezek kiküszöbölésére ajánlják a szerzők a Tele-Lab projektet, amely internetalapú távoktatási rendszerként is értelmezhető, amely a hagyományos offline kiberbiztonsági gyakorlati laboratóriumoknak is megfelel. A Tele-lab alapvetően egy olyan web alapú oktatási rendszer, amely virtuális gépekkel felépített képzési környezetből áll, és amely gyakorlati feladatokból álló tanulási egységekkel biztosítja a szükséges kiberbiztonsági ismeretek elsajátítását. A virtuális gépek segítségével számos kibertámadási forma szimulálható, így a támadó és az áldozat oldala egyaránt szemléltethető. Ebbe beletartozik például a felhasználói viselkedés, a támadó cselekedeteinek szimulálása is, amely jelentősen hozzájárul a valós támadási helyzetet bemutatásához. A tanulási egységek tartalmára az elméleti és gyakorlati ismeretek egyaránt jellemzőek, a cél az elsajátított elméleti ismeretek konkrét gyakorlati helyzetekben történő alkalmazása. Minden tanulási egység tippet ad arra is, hogy az éppen aktuálisan ismertetett támadási módszer megelőzése, elhárítása hogyan valósítható meg. Ezt követően a szerzők ismertetik a Tele-Lab műszaki paramétereit, komponenseit és felépítését. [40]

Beuran és szerzőtársai rávilágítanak arra, hogy csak a gyakorlati oktatás segítségével érhető el, hogy a hallgatók ténylegesen megszerezzék a kibertámadások elhárításához szükséges ismereteket, készségeket, képességeket, amelyek elősegítik a valós eseményekre történő azonnal reagálást. Jelen tanulmányban a szerzők bemutatják az általuk kidolgozott CyTrONE nevű integrált kiberbiztonsági képzési keretet, annak felépítését, megvalósítását és hatékonyságát. A képzési tevékenységek három fő kategóriáját különítik el, a támadás orientált képzést, az elemzés orientált képzést, valamint a védelem orientált képzést nevesítik. A képzési keretrendszerben a

hagyományos nyomtatott és digitális tananyagokat egyaránt alkalmaznak, továbbá egy az erre a célra létrehozott képzési környezetben végrehajtható gyakorlati feladatokat biztosítanak a hallgatók számára. A szerzők szerint két követelmény megvalósulása szükséges a hatékony kiberbiztonsági képzési keretrendszer létrehozásához. Az egyik a módosítás és az új képzési tartalmak hozzáadásának képessége, a másik a képzési környezet automatikus létrehozásának és kezelésének képessége. Ezt követően a szerzők felvázolják a keretrendszer kialakítását, folyamatát és annak lépéseit, valamint jelen képzési típus előnyeit, felhasználhatóságát. Ezután bemutatják a keretrendszer egyes elemeit, így például a felhasználói felületet, a képzési adatbázist, a menedzsment modult, a további hozzáadható modulokat, valamint a szerverek és hálózati eszközök infrastruktúráját. A szerzők kifejtik, hogy jelen képzés előnye a belépési akadályok csökkenése, ugyanis a könnyű kezelési leírások elősegítik a bonyolult műszaki specifikációk megértését, továbbá egységesíti a képzés tartalmának és környezetének kezelését, amely jelentősen hozzájárul a működési és telepítési idő csökkentéséhez, továbbá a képzési tevékenységet egyfajta szabványba integrálja annak érdekében, hogy az egész kiberbiztonsági oktatási folyamatot támogathassa. Ezen kívül a keretrendszer nyilvános közzététele lehetővé teszi a széles körben történő hozzáférést és a további hatékony fejlesztését, bővítéseket. [32]

5.2.2. ELŐZETES TECHNIKAI ÉS FOGALMI ÁTTEKINTÉS

Ahhoz, hogy a jelen fejezetben definiált szimulációs keretrendszer prototípus minden részletre kiterjedő bemutatása megvalósulhasson, elengedhetetlen a kapcsolódó főbb fogalmak meghatározása.

Az első ilyen fogalom a kibertámadás, amely meghatározására számos definíció létezik. Az Egyesült Államok Kiberparancsnoksága által kiadott lexikon szerint a kibertámadás: számítógép vagy kapcsolódó hálózatok vagy rendszerek segítségével végrehajtott ellenséges cselekedet, amelynek célja egy ellenfél kritikus kiberrendszereinek, eszközeinek vagy funkcióinak megzavarása és / vagy megsemmisítése. [41] Hathaway és szerzőtársai szerint a kibertámadás minden olyan intézkedést magában foglal, amelyet politikai vagy nemzetbiztonsági célok elérése érdekében a számítógépes hálózat funkcióinak aláásása érdekében hajtanak végre. [42] Owens meghatározása alapján a kibertámadás olyan szándékos cselekedetek végrehajtása, amelynek célja az ellenfél számítógépes rendszereinek vagy

hálózatainak, illetve az ezekben a rendszerekben vagy hálózatokban maradó vagy azokon átmenő információk és/vagy programok megváltoztatása, megzavarása, megtévesztése vagy megsemmisítése. [43] Uma és Padmavathi szerint a kibertámadás a kibertér kiaknázása bizalmas információk megszerzése érdekében, amely magában foglalja például a kémkedést, a hálózatok letiltását, valamint adatok és pénz illetéktelen eltulajdonítását. [44]

A kibertámadások az alkalmazott technikától függően rendkívül sokfélék lehetnek, a teljesség igénye nélkül többek között ide sorolhatók a DoS, DDoS támadások, adathalászat, kártékony programok, keylogger programok, jelszavakra irányuló támadások, SQL injektálás, közbeékelődéses (man-in-the middle) támadás.

A jelen tanulmányban ismertetett prototípusban a szolgáltatás megtagadással járó támadás (DoS), az adathalászat (Phishing) és a hátsóajtó programok (backdoor) egy-egy alkalmazása kerül bemutatásra a gyakorlatban, így ezen fogalmak ismerete is elengedhetetlen.

A DoS (Denial of a Service) másnéven szolgáltatás megtagadással járó támadás lényege, hogy olyan sok kéréssel támadják meg a hálózatot, vagy azon keresztül valamelyik alkalmazást, amennyit a fogadó oldal már nem tud feldolgozni. Ennek következtében nem lesz elérhető az adott szolgáltatás, mivel nem tud kiszolgálni egyszerre ennyi kérést a szerver. [45] A támadás irányulhat a célpont hálózati kapcsolatának, vagy pedig a célpont rendszerben működő valamely - szolgáltatást nyújtó - alkalmazásának túlterhelésére, amely során a támadó célja a célpont erőforrásainak lefoglalása. [46]

Az adathalászat, más néven phishing lényege abban rejlik, hogy az adathalászok a felhasználókat, valamilyen elektronikus csatornán keresztül, - például e-mailben, azonnali üzenetben, vagy éppen szalagcím hirdetésekben - egy látszólag teljesen eredeti, valójában pedig egy hamis weboldalra irányítják, ahol arra kérik, hogy adja meg bizalmas adatait. Az adathalászatnak számos válfaja van, aszerint, hogy milyen módon, milyen elektronikus csatornán keresztül invitálják a felhasználót a hamis weboldalra. [47]

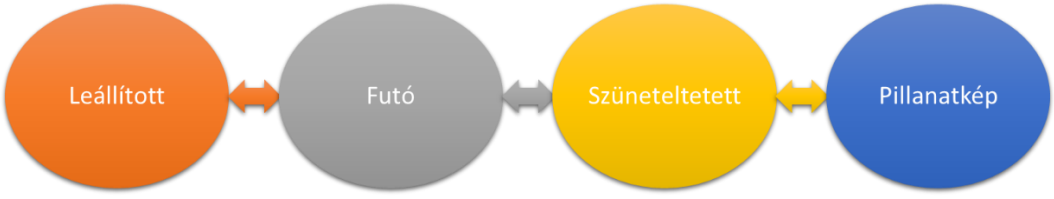
A hátsóajtó alkalmazás (backdoor) a felhasználók számára általában nem látható elem, amelyet a telepítést követően egy vagy több távoli személynek lehetőséget biztosít a számítógép elérésére és irányítására. Ennek segítségével a támadó megtekintheti a

másik eszközön tárolt adatokat, információkat, de akár módosíthatja vagy törölheti is ezeket. A program veszélyessége abban rejlik, hogy nem csak távoli elérést biztosíthat idegeneknek, hanem rendszeradminisztrációs jogok megszerzését is lehetővé teheti. [f6]

A virtualizáció több számítógép szimulációja egy hardverkonfiguráción, vagyis hardverek emulációja szoftveres környezetben. Ez lehetővé teszi egy eszköz erőforrásainak felosztását több környezet között. A virtualizáció céljai közé tartozik a meglévő erőforrások kihasználtságának maximalizálása, az IT szolgáltatások rugalmasságának fejlesztése, a rendszerek biztonságának növelése és a leállások szükséges idejének csökkentése, valamint a meglévő rendszerek kezelésének egyszerűsítése, költségeinek csökkentése. [w14]

A virtualizációt csoportosíthatjuk például aszerint, hogy a fizikai eszközöktől milyen szinten választják el a rendszert. Jelen tanulmányban a prototípus elkészítése szempontjából releváns virtualizáció típus az operációs rendszer virtualizáció és hardver emuláció. Amikor operációs rendszert virtualizálunk, általában egy gazda (host) operációs rendszeren futtatunk egy vagy több vendég (guest) operációs rendszert. [w14]

Egy virtuális gép állapotait, általános struktúráját szemlélteti az 5-1. ábra, illetve látható, hogy mely állapotokból mely állapotokba juthat. A virtuális gépek először is leállított formában kerülnek létrehozásra. A leállított virtuális gépet el lehet indítani, amelynek hatására futó állapotba kerül. A futó állapotban természetesen a virtuális gép leállítható, illetve szüneteltethető. A szüneteltethető állapotban a virtuális gép nem áll le, csak felfüggesztjük a működését és elmentjük a memória tartalmát. A szüneteltetésből azonnal folytatható a működés, ekkor futó állapotba kerül, illetve pillanatkép készíthető. A pillanatképből a virtuális gép automatikusan elindítható úgy, hogy a szüneteltetett állapotba kerül.



5-1. ábra Virtuális gépek állapotai

Kibergyakorlatok csoportosítása

A gyakorlati kiberbiztonsági ismeretek átadására már számos technológia áll rendelkezésünkre. Fő szempont, amely megkülönbözteti őket egymástól, hogy a támadók és a védekezők aktív vagy passzív szerepet vállalnak a kibergyakorlatokban. Ezek alapján az alábbi típusokat különböztethetjük meg:

a) **aktív-aktív**: a támadó és a védekező oldalt is valós személy képviseli avagy valós személy irányítja a támadást, illetve a védekezést. Elsősorban csapatjátékok, ahol az egyik csapat megpróbálja feltörni a másik csapat rendszerét, miközben a másik csapat védekezik. Ilyenek például a Capture the Flag, Red-Blue Team gyakorlatok.

b) **aktív-passzív**: az áldozat egy passzív rendszer, míg a gyakorlat során a hallgatóknak kell a támadó szerepét megszemélyesíteni annak érdekében, hogy az áldozat infrastruktúra gyenge pontjait felderítve adatokat szerezzenek meg.

c) **passzív-aktív**: A támadó egy passzív rendszer, mely előre beállított támadási szekvenciát játszik le automatizáltan külső felügyelet nélkül, míg a hallgatóknak az áldozat szerepét kell megvalósítaniuk, amely során fel kell ismerniük az aktuális támadásokat és azokat meg kell akadályozniuk, helyre kell állítaniuk és reagálniuk kell a már bekövetkezett eseményekre.

d) **passzív-passzív**: Elsősorban tesztelési célból, illetve kibertámadások szemléltetésére alkalmazzák, valamint többek között olyan automatizált kibervédelmi rendszerek tesztelésére, amelyeknek célja helyettesíteni, kiváltani az áldozatot, ezáltal külső felügyelet nélkül megakadályozni a kibertámadásokat.

e) **általános**: Olyan kiberbiztonsági gyakorlatok végrehajtására alkalmas platformok, amelyeken az előbb felsorolt típusok bármelyike megvalósítható. Legtöbb esetben hálózatok és számítógépek emulálását végzik, amelyen keresztül tetszőleges kibergyakolat szimulálható.

f) **egyéb**: Olyan kiberbiztonsági gyakorlatok, amelyek az előző kategóriákba nem sorolhatók, de szorosan kapcsolódnak a kibergyakorlatokhoz és a kiberbiztonsági ismeretek gyakorlati oktatásához, így különösen társasjátékok, számítógépes játékok.

5.2.3. KIBERVÉDELMI GYAKORLATOKHOZ KAPCSOLÓDÓ PLATFORMOK

Érdemes áttekinteni a kibervédelmi gyakorlatokhoz kapcsolódó platformokat, amelyeket a korábban bevezetett csoportosítás alapján mutatok be. Az 5-1. táblázat szemlélteti kategóriánként a rendelkezésre álló releváns technológiákat, platformokat és azok jellemzőit.

Technológia	*Kategória*	*Elérhetőség*	*Célközönség*	*Telepítés*
KYPO	aktív-aktív	online	akadémia/kutatás	×
CDX	aktív-aktív	offline	szakértők	×
Emulab	általános	offline	akadémia/kutatás	komplex
Cytrone	általános	offline	akadémia/kutatás	komplex
Leaf	általános	offline	szakértők	komplex
Cyber-Physical Security Test Bed	általános	offline	szakértők	komplex
VulnHub	aktív-passzív	offline	szakértők	szabadkéz
TryHackMe	aktív-passzív	online	szakértők	×
WebGoat	passzív-aktív	online	szakértők	×
Metasploitable	aktív-passzív	offline	szakértők	szabadkéz
Blackjack	passzív-passzív	offline	szakértők	komplex
ACD	passzív-passzív	offline	szakértők	komplex
Cyber Defence Tower Game	egyéb	offline	minden korosztály	egyszerű
Riskio	egyéb	offline	minden korosztály	×

5-1. táblázat: Kapcsolódó munkák áttekintése

5.2.3.1. Kategória

A feldolgozott technológiákat, eszközöket több csoportba lehet sorolni az alapján, hogy a kibergyakorlatok korábban nevesített osztályozása alapján melyik típusba sorolhatóak.

Az Emulab, a Cytrone, a Leaf és a Cyber Security Testbed általános platformokat definiálnak. Az Emulab [48] egy olyan rugalmas felépítésű gyakorlati kurzus, amely során valódi hacker támadások végrehajtásával mutatják be a kibertámadások egyes módszereit, amely segítségével irányítható környezetet biztosít a támadó és védekező kiberbiztonsági kísérletek előkészítésére és mérésére. A Cytrone [32] nevű integrált kiberbiztonsági képzési keretrendszer magában foglalja a támadásorientált, az elemzésorientált, valamint a védelemorientált képzést. Ennek keretében speciálisan

erre a célra létrehozott képzési környezetben végrehajtható gyakorlati feladatokat biztosítanak a hallgatók számára. A keretrendszer elemei közé sorolhatók a következők: a felhasználói felület, a képzési adatbázis, a menedzsment modul, lehetséges további hozzáadható modulok, valamint a szerverek és hálózati eszközök infrastruktúrája. A Leaf [49] kiberinfrastruktúrák szimulálására, valósághű IoT forgatókönyvek reprodukálására és versenyképes kiberbiztonsági tréningek végrehajtására szolgáló nyílt forráskódú platform. A Cyber Security Testbed [50] egy kiberfizikai biztonsági platform, amely alkalmas kibertámadások szimulálására és kiértékelésére, valamint a segítségével végrehajtott behatolástesztek által feltárhatók az elektromos hálózatokra irányuló kibertámadások következményei és hatásai.

A KYPO és a CDX elsősorban olyan környezetet határoznak meg, ahol Capture The Flag jellegű feladatok hajthatóak végre, vagyis mind a támadó, mind a védekező félnek aktívnak kell lennie. A KYPO [51] egy kibergyakorlati és kutatási platform, amely komplex számítógépes rendszerek és hálózatok modellezésére és szimulálására összpontosít. A platform virtualizált környezetet biztosít előre meghatározott forgatókönyv szerinti komplex kibernetikai támadások végrehajtásához egy szimulált kritikus infrastruktúra ellen. A CDX [52] gyakorlat sajátossága, hogy a résztvevő csapatoknak saját magunknak kell kialakítani hálózatukat, azon a biztonsági beállításokat elvégezni, amely a támadás külső fél általi végrehajtása követ. A biztonsági kihívások megértése és az incidensekre való reagálás, valamint a csapatmunkával kapcsolatos készségek fejlesztése egyaránt célja a gyakorlatnak. [53]

A Vulnhub [w25], a TryHackMe [w22] és a Metasploitable [54] elsősorban a támadó felek számára biztosítanak lehetőséget a fejlődésre (aktív-passzív), míg a Webgoat [w20] alkalmazás elsősorban védekezés orientált (passzív-aktív).

Automatizált kibervédelemmel kapcsolatos technológiák a Blackjack [55], illetve az ACD [56], amelyek célja, hogy emberi beavatkozás nélkül képesek legyenek a támadások elhárítására, emiatt ők a passzív-passzív kategóriába sorolhatók.

Végül a Cyber Defence Tower Game [57] egy egyszerű számítógépes Tower Defense játék, míg a Riskio [58] egy társas táblajáték, amelyek inkább kedvcsináló és ösztönző eszközök lehetnek az oktatásban, mint sem konkrét tudásátadásra használható technológiák.

5.2.3.2. Elérhetőség

A technológiák kiválasztásánál fontos szempont lehet az is, hogy a felhasználó képes-e internet elérés nélkül is használni a technológiát. Ez alapján a vizsgált platformok, eszközök lehetnek:

a) online elérhetőek, vagyis internethálózatra van szükség ahhoz, hogy a feladatokat megoldják.

b) offline elérhetőek, vagyis nem szükséges az internethálózat, a felhasználó a saját lokális számítógépén is előállíthatja a környezetet.

Míg a KYPO, a TryHackMe és a Webgoat esetében szükséges az internetelérés, addig a többi esetben offline elérhető technológiákról beszélhetünk.

5.2.3.3. Célközönség

A különböző technológiák különböző célközönséget szólítanak meg. Ez alapján az alábbiak lehetnek:

a) **akadémia/kutatás**: elsősorban az akadémiai életben használják a technológiát, leginkább prototípus szinten, mintsem termékként. Az elért eredményeket pedig kutatási célokra is felhasználják.

b) **szakértők**: olyan kiforrott már maga a technológia, hogy arra már termékként is tekinthetünk, amelyeken szervezett oktatás zajlik kiberbiztonsági szakértők számára, akik már jártasak az informatikai ismeretekben is.

c) **minden korosztály**: azok a technológiák, amelyek elsősorban figyelemfelhívásra, a tudatosság növelésére, esetleg kedvcsinálásra és motiválásra alkalmasak.

A KYPO, a Cytrone és az Emulab rendszer elsősorban akadémiai célból készült, míg a Riskio, valamint a Cyber Defence Tower Game a biztonságtudatosság növelését célozza minden korosztály számára. A többi technológia a célcsoportot tekintve a szakértők kategóriába sorolható, vagyis mély informatikai tudással rendelkező, önmagukat képezni kívánó szakembereket szólítanak meg.

5.2.3.4. Telepítés

A vizsgált technológiák kategorizálhatók aszerint, hogy a kibergyakorlatok során alkalmazott technológiák telepítése hogyan történik:

a) **komplex**: mely során komplex rendszereket, többféle alkalmazást, programot szükséges telepíteni, továbbá számos nem triviális beállítás, végrehajtása indokolt.

b) **szabadkéz**: nincs meghatározva, hogy mit kell telepítenie a felhasználónak, egy virtuális gépet kap, amelyet szabadon felhasználhat.

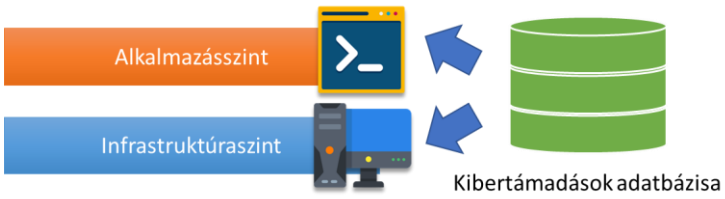
c) **egyszerű**: a telepítéshez nem szükséges mélyebb informatikai tudás.

A Vulnhub és a Metasploit nem definiál részletes környezetet a gyakorlatok elvégzéséhez, mindössze egy-egy virtuális gépet kell letöltenie a felhasználónak, amelyeket ezt követően oly módon használ, ahogyan csak szeretne. Az Emulab, a Cytrone, a Leaf és a Cyber-Physical Security Test Bed esetén egy teljes architektúrát kell előállítani különböző programok segítségével, amelyhez bár részletes leírás tartozik, mégis egy komplex műveletnek tekinthető. Végül a Cyber Tower Defence Game esetében egy egyszerű programról van szó, amelyet a számítógépünkre kell telepíteni. A többi technológiához kapcsolódóan nincs szükség külön telepítés elvégzésére.

5.3. SZIMULÁCIÓS KERETRENDSZER

A gyakorlati oktatás során fontos egy olyan környezet kialakítása, amelyen keresztül a hallgatók szembesülhetnek ismert kibertámadási technikákkal és egy szimulált környezetben kipróbálhatják a képzés során megismert védelmi mechanizmusokat. Emiatt szükséges egy olyan keretrendszert definiálni, amely képes támogatást nyújtani a képzés során az egyéni infokommunikációs eszközök védelmének megismeréséhez, illetve a szervezeti szintű védelmi mechanizmusok használatához.

A keretrendszer definiálása során célszerű az alkalmazási réteget és az infrastrukturális réteget megkülönböztetni, mivel a gyakorlati tapasztalatok alapján a kibertámadások is csoportosíthatóak hardveres és szoftveres hibákat kihasználó esetekre. Illetve szükséges egy kibertámadási adatbázist definiálni, amely tartalmazza az egyes támadások végrehajtásához szükséges lépéseket (5-2. ábra).



5-2. ábra Alkalmazás- és infrastrukúraszint bevezetése

Alkalmazásszint: a szoftveres kibertámadások bemutatásához szükséges alkalmazások, operációs rendszerek halmaza.

Infrastruktúraszint: a hardveres kibertámadások bemutatásához szükséges architektúra.

Kibertámadások adatbázisa: az egyes kibertámatások definíciója, amely alapján a támadás megvalósítható a szimulált környezetben.

5.3.1. INFRASTRUKTÚRASZINT

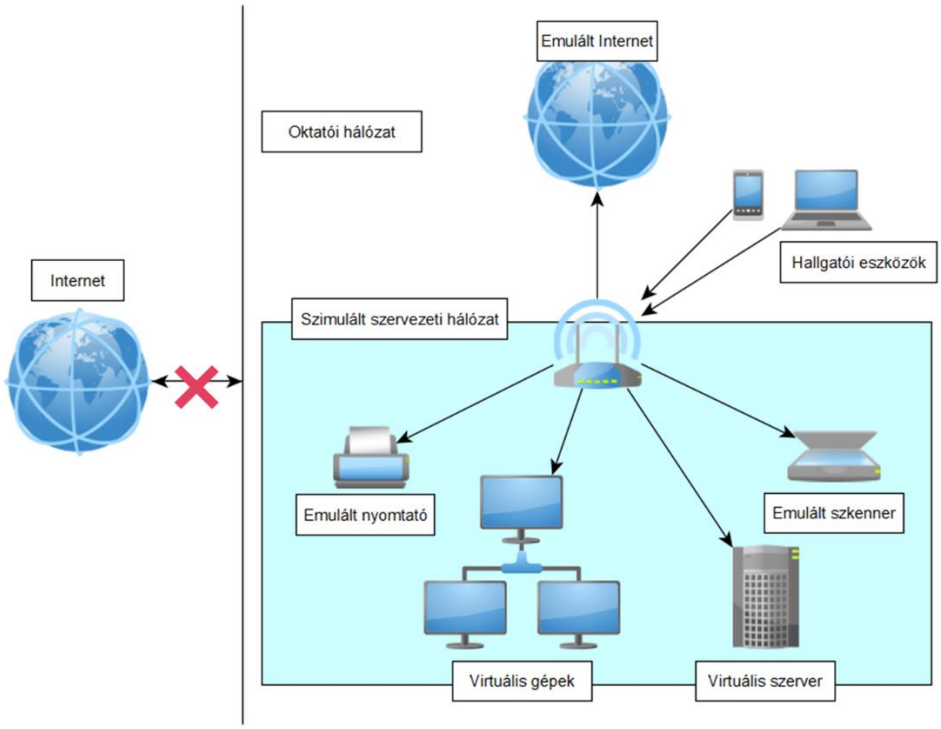
A keretrendszer infrastruktúra szintjének meghatározása során a fő szempontok az alábbiak voltak:

- Ne legyen elérhető az internet a szimuláció során az adatvédelmi, jogi és egyéb szabályozások miatt, valamint annak érdekében, hogy elkerülhessük a kibertérből érkező fenyegetések bekövetkezését.
- Egyéni infokommunikációs eszközök is könnyen csatlakoztathatóak legyenek.
- A közszolgálati infrastruktúra jellemző elemei megjelenjenek.
- Olyan kibertámadások kerüljenek bemutatásra, szimulálásra, amelyekkel a felhasználók a különféle munkakörök betöltése során találkozhatnak.

5.3.1.1. Hardver architektúra

Az általam definiált architektúratervet az 5-3. ábra szemlélteti. A keretrendszerben szereplő összes elem egy oktatói hálózatban található, amelynek nincs kapcsolata a külvilággal, vagyis az internettel. Az architektúra központi eleme egy vezetéknélküli router, amely kapcsolatot teremt a rendszer összes elemével. Ehhez tudnak csatlakozni a hallgatók saját infokommunikációs eszközei, illetve a szervezeti infrastruktúrát reprezentáló elemek: nyomtatók, szkennerek, szerverek és személyi számítógépek. A szervezethez kapcsolódó eszközök emuláltak, tehát nincs szükség a tényleges létükre, elég csak a szoftveres megfelelőjüket használni, amely azt a látszatot kelti, mintha a

valóságban is jelen lennének. A szerverek és személyi számítógépek kialakítására pedig egy privát felhő alapú virtualizációt célszerű megalkotni, amelynek segítségével tetszőleges számú gépet lehet a keretrendszerbe illeszteni. További fontos hozzáadott elem az emulált internet szerepe az architektúrával, amelyen keresztül ismert weboldalak másolatát (pl.: google.com, facebook.com stb.) hosztolja a rendszer és teszi elérhetővé a szimulációban résztvevő személyek számára.



5-3. ábra A szimulált hálózat architektúrája

5.3.1.2. Kibertámadás szimulációja hardver szinten

Az infrastruktúra-szintű támadás megvalósításához egy külső komponens csatlakoztatása szükséges az oktatói hálózatba, illetve a szimulált szervezeti hálózatba. Az oktatói hálózatba csatlakoztatott eszköz képes lehet olyan szervezeti hálózat elleni támadások végrehajtására, mint például portszkennelés, DDoS stb. A szervezeti hálózatba csatlakozott komponens képes lehet továbbá MAC cím lopásra (pl.: nyomtatónak kiadni magát, így eltulajdonítva a nyomtatásra küldött anyagokat), memória módosításokra, vagy akár szerver adatok törlésére is.

5.3.1.3. Bővíthetőség

A hálózat sajátosságainak köszönhetően a rendszerbe könnyedén lehet újabb és újabb komponenseket csatlakoztatni. Emellett a privát felhő alapú megoldásnak

köszönhetően további virtuális elemekkel is bővíthető a rendszer. A virtuális gépek pedig lehetőséget biztosítanak további komponensek csatlakoztatására is, pl.: USB stick, programozható egér és billentyűzet, stb.

5.3.2. ALKALMAZÁSSZINT

Az alkalmazásszint épít az infrastrukturális szinten meghatározott elemekre, vagyis a meglévő keretrendszerben megtalálható személyi számítógépeket és szervereket szoftveres elemekkel ruházza fel.

5.3.2.1. Alapértelmezett alkalmazások

A keretrendszer alkalmazásszintjének meghatározása során a legfőbb szempont az volt, hogy a közszolgálati feladatkörökre jellemző alkalmazások is megjelenjenek.

a) Szerver komponensek:
   - Levelező szerver
   - Munkaidőnyilvántartó adatbázis
   - Dokumentumtároló adatbázis
   - Webszerver szervezeti oldalak hosztolásához
   - Egyéb

b) Személyi számítógép komponensek
   - Windows Operációs rendszer
   - Böngésző alkalmazások (Chrome, Firefox, Internet Explorer)
   - Levelező kliens
   - Munkaidőnyilvántartó alkalmazás
   - Dokumentumszerkesztő
   - Egyéb

5.3.2.2. Kibertámadás szimulációja alkalmazásszinten

Az alkalmazásszintű támadás megvalósításához egy külső komponens csatlakoztatása szükséges az oktatói hálózatba, illetve a szimulált szervezeti hálózatba. Az oktatói hálózatba csatlakoztatott eszköz képes lehet adathalász e-mail küldésére, amely az emulált internet egy kártékony oldalára hivatkozik, vagy olyan csatolt fájlokat tartalmaz, amelyek megnyitása kártékony kódot futtat az számítógépen. A szervezeti hálózatba csatlakozott komponens képes lehet SQL injection jellegű támadásra annak

érdekében, hogy bizalmas dokumentumokhoz, esetleg személyes adatokhoz férhessen hozzá.

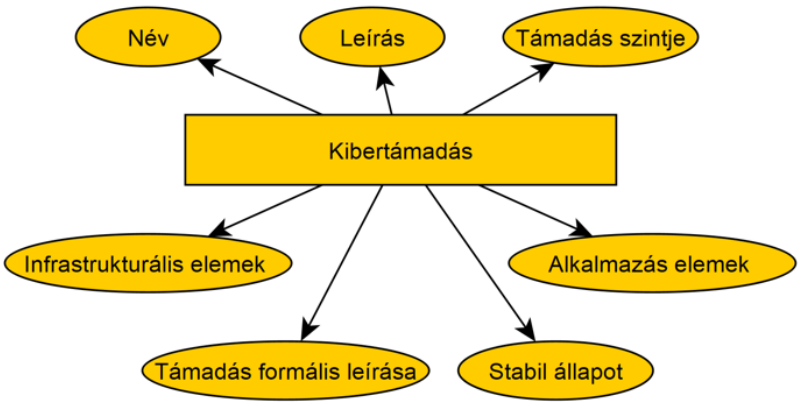
5.3.2.3. Bővíthetőség

Mivel a személyi számítógépek és a szerverek is virtualizált környezetben helyezkednek el, így könnyedén bővíthetőek extra szolgáltatásokkal és alkalmazásokkal. A virtuális gépek összeállításához, úgynevezett virtuális képeket (virtual image) szükséges használni, amely leírja, hogy egy virtuális gépen milyen operációs rendszer, hardverigények és szoftverek találhatóak meg. A virtuális képeket ezután a terítés folyamata során lehet a privát felhőben többszörözni és elindítani.

5.3.2.4. Kibertámadások adatbázisa

Ahogyan azt korábban meghatároztam a kibertámadások adatbázisa definiálja az egyes támadástípusok végrehajtását a szimulált környezetben. Egy új támadási típus meghatározásához a következő paraméterek megadására van szükség (5-4. ábra):

a) a támadás neve,
b) a támadás jellegének leírása,
c) a támadás szintje: Alkalmazásszint/Infrastruktúraszint/Kombinált,
d) a végrehajtáshoz szükséges infrastruktúra elemek,
e) a végrehajtáshoz szükséges alkalmazások listája,
f) a támadás formális leírása,
    - annak érdekében, hogy a támadás automatizáltan is végrehajtható legyen, és
    - tartalmazza azokat az adminisztratív feladatokat is, amelyek előkészítik a támadást (pl.: e-mail cím létrehozása a hallgatónak, hozzáférések beállítása);
g) a támadás elhárításának állapota
    - a szimuláció során, ha a rendszer ebbe az állapotba kerül, akkor a támadás elhárítottnak tekinthető.

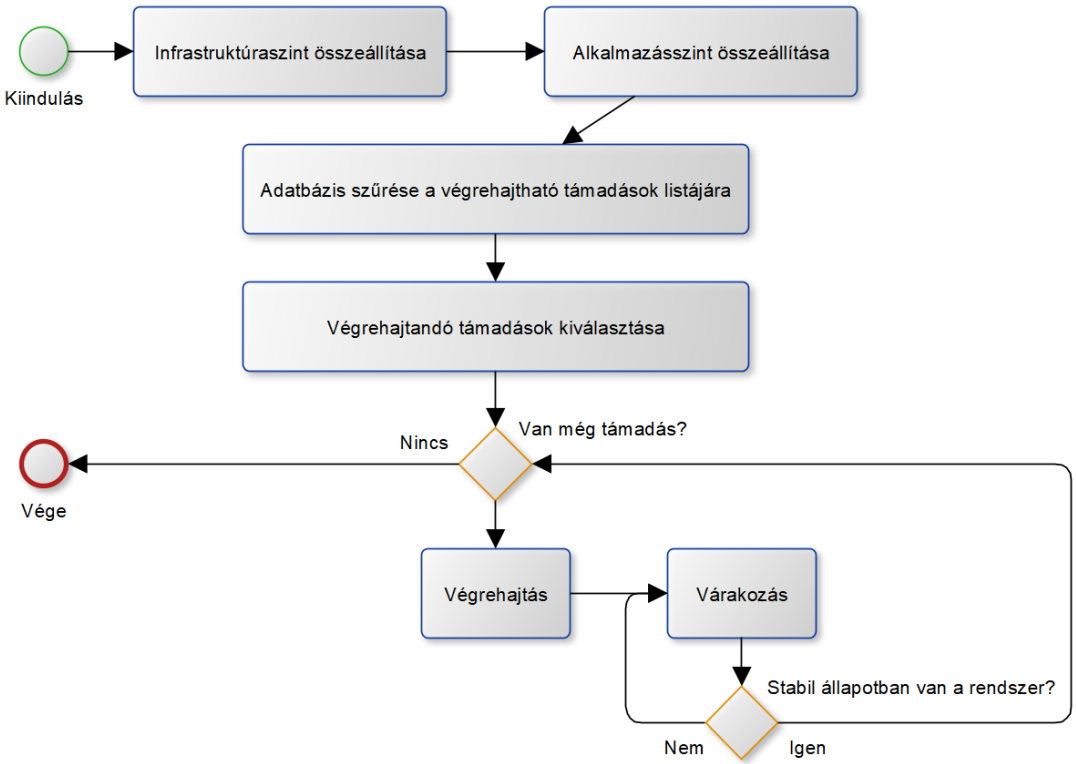


5-4. ábra Kibertámadások definíciója

A szimulált környezet kialakítása során törekedni kell arra, hogy a lehető legtöbb kibertámadás megvalósítható legyen, de természetesen ez nem minden esetben kivitelezhető. A keretrendszer bővíthetősége miatt, ezért könnyedén átkonfigurálható egy-egy speciális esetre is.

5.3.2.5. Szimuláció folyamata

A szimulációs folyamatot az 5-5. ábra szemlélteti, ahol először az infrastruktúra-, és az alkalmazásszint összeállítása történik. Mivel az alkalmazások listája adott és az infrastruktúra nem lehet képes minden típusú támadási technika kezelésére, ezért a kibertámadási adatbázison szükséges egy előszűrést elvégezni, hogy csak olyan támadást lehessen végrehajtani, amely a gyakorlatban tényleg meg is valósítható. Ezt követően a megmaradt támadásokból a szimuláció során választunk néhányat. A kiválasztási folyamat történhet manuálisan az oktató által, vagy véletlenszerűen is, amelyet esetlegesen egy vizsga alkalmával lehet használni. Paraméterezhető az is, hogy hány ilyen támadás fog végrehajtásra kerülni. A folyamatábrán egyértelműen látszik, hogy egyszerre csak egy támadást hajt végre a szimuláció és addig vár, amíg a hallgatók olyan stabil állapotba nem hozzák a rendszert, amely a kibertámadási adatbázisban célállapotként lett megjelölve. Ha ez teljesült, akkor egy újabb támadás kerül végrehajtásra. Ha nincs már több támadás, amit végre lehetne hajtani, akkor a folyamat befejeződik.



5-5. ábra A szimuláció folyamata

5.3.3. TÁVOKTATÁS TÁMOGATÁSA A KÉPZÉS SORÁN

Az elmúlt években megjelenő pandémiás helyzet (covid-19) is azt bizonyítja, hogy a távoktatás megvalósítása elengedhetetlen a külső, sokszor előre nem látható körülmények által jelentősen befolyásolt gyakorlati oktatás eredményes végrehajtásához. Éppen ezért fontos, hogy az ilyen események okozta nehézségekre is felkészült legyen az oktatási környezet. Az elméleti tudás átadására számos megoldás létezik, a videó-, és fájlmegosztást lehetővé tevő virtuális osztálytermeket létrehozó platformoktól kezdve, a különféle streaming-szolgáltatók alkalmazásáig számtalan lehetőség áll a rendelkezésünkre, azonban fontos, hogy a korábban személyes jelenlétet igénylő gyakorlati foglalkozások is megtarthatók legyenek online formában. Ennek megoldását célozza a hallgatók virtuális magánhálózaton (VPN) keresztül történő csatlakozása, amely segítségével távolról elérhető a korábban felvázolt szimulációs keretrendszer. Ennek köszönhetően a szimulációs környezetben rendelkezésre álló feladatok ugyanúgy megoldhatók, mint tantermi környezetben. Emellett a hallgatók rendelkezésére kell bocsátani a támadások elhárításához szükséges lépéseket tartalmazó oktatóanyagokat és videófájlokat az ezt a célt szolgáló e-learning portálon. Továbbá fontos, hogy az oktató online órák megtartásával

segítheti ezen anyagok megértését, gyakorlati alkalmazását. Ezek segítségével a hallgatók képesek lesznek elsajátítani a kibertámadások elhárítására szolgáló intézkedéseket.

5.3.4. ÉRTÉKELÉSI RENDSZER

A H-5.2 hipotézis szerint kialakítható egy automatizált értékelési rendszer, amely alkalmas a gyakorlati képzési rész során átadott tudásanyag számonkérésére. A következőkben e hipotézis igazolására a szimulációs környezetben megvalósuló oktatás értékelési rendszere, valamint annak jellemzői kerülnek definiálásra. A cél egy olyan automatizált értékelési rendszer kialakítása, amely oktatói felügyelet nélkül is képes a hallgatók munkájának ellenőrzésére és értékelésére. Ahhoz, hogy ez megvalósuljon, az alábbi kihívások megoldására van szükség a szimulációs keretrendszer bővítésével:

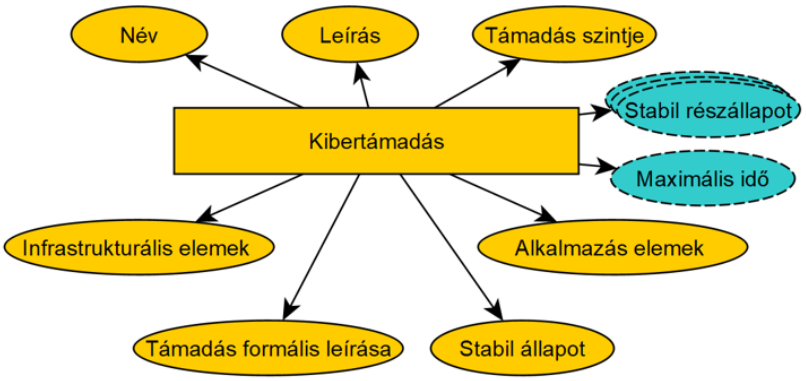
a) **Védekezés sikerességének számszerűsítése**: A szimulációs környezetben végrehajtott támadások elleni védelmi intézkedések minőségét és sikerességét számszerűsíteni kell. A hallgatók értékelése során fontos az elvégzett munka alapján történő érdemjegy azonosítása, amely egy egyértelmű és következetes metrika definiálásával valósítható meg.
b) **Tárolás és újrajátszás:** A számonkérés során végrehajtott cselekménysorozatot tárolhatóvá és manuálisan újra végrehajthatóvá kell tenni, amelynek célja, hogy a vizsgafeladat megoldását követően az oktató és a hallgató számára is azonosíthatóvá váljon az adott feladatra kapott pontok száma, illetve érdemjegy.

5.3.4.1. Védelmi intézkedések minősítése és számszerűsítése

A hallgatók értékelése során fontos az elvégzett munka alapján történő érdemjegy azonosítása, amelyhez szükséges egy egyértelmű és következetes metrikát definiálni. Két ilyen metrikát különböztethetünk meg:

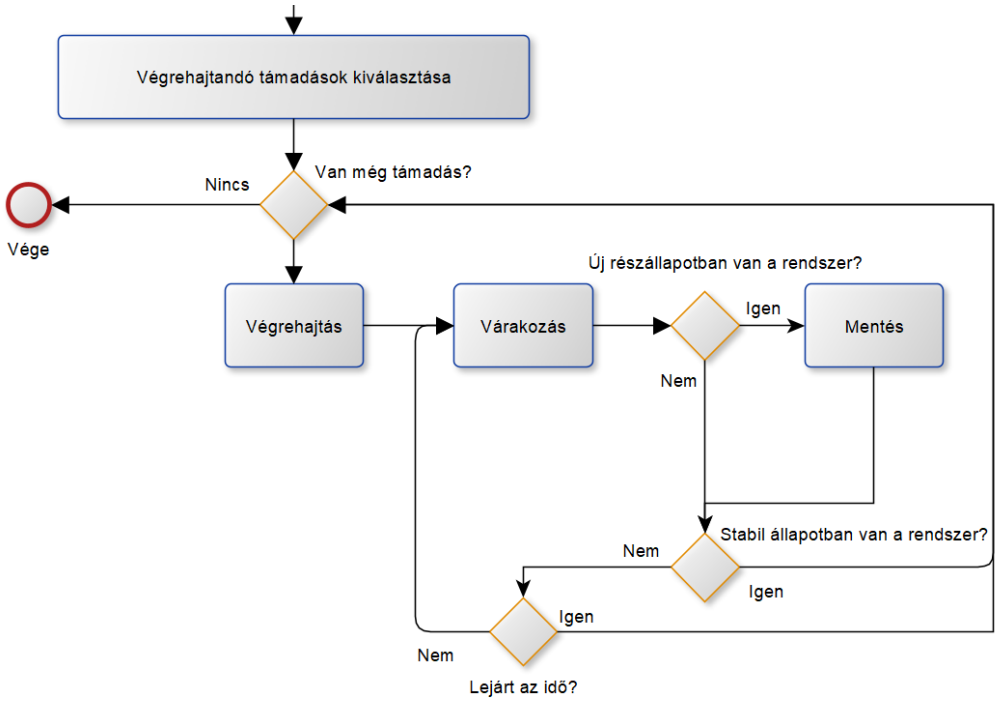
1) *Elhárított kibertámadások száma:* a szimuláció során több kibertámadást kell a hallgatónak elhárítania. Ahány támadást sikerült megoldania a hallgatónak, annyi pontszámot ért el a számonkérés során.
2) *Elért részállapotok száma egy kibertámadás során:* a szimuláció folyamán egy komplex kibertámadást kell a hallgatónak elhárítania, de részmegoldásra is adható pont a hallgatónak.

Az 1) metrika már a jelenlegi szimulációs keretrendszerrel is megvalósítható, azonban a 2) a metrika alkalmazásához a kibertámadási leírók bővítése szükségeltetik további állapotdefiníciókkal, amelyek meghatározzák, hogy a rendszer olyan állapotba jutott-e, amely megfelel egy részmegoldásnak. Mindazonáltal, a számonkérések során limitált idő áll a hallgatók rendelkezésére, ezért ezzel az információval is bővülnie kell a kibertámadási leírónak (5-6. ábra).



5-6. ábra A kibertámadások definíciójának bővítése

Ezáltal a szimulációs folyamatot is bővíteni kell újabb döntési és végrehajtási elemekkel , ahogyan azt az 5-7. ábra szemlélteti (jelen ábra a korábbi teljes folyamat ábrának csak az alsó, kibővített részét mutatja).



5-7. ábra A szimulációs folyamat bővítése

A várakozás akció végrehajtása után meg kell vizsgálnunk, hogy a rendszer új részállapotba jutott-e (hiszen ekkor új pontot kaphat a hallgató). Amennyiben új állapotba került, akkor ezt elmentjük, hogy egy következő alkalommal ellenőrizni tudjuk, hogy másik állapotot talált-e meg a hallgató. Ezután megvizsgáljuk, hogy a rendszer stabil állapotban van-e, hiszen ha igen, akkor az azt jelenti, hogy az adott támadás elhárítása sikeres volt. Amennyiben nem, megvizsgáljuk, hogy az adott feladatra szánt idő lejárt-e, ha nem akkor tovább várakozunk, ha pedig a rendszer stabil állapotban van vagy az idő lejárt, akkor a következő feladat végrehajtására ugrunk (feltéve, ha még van feladat).

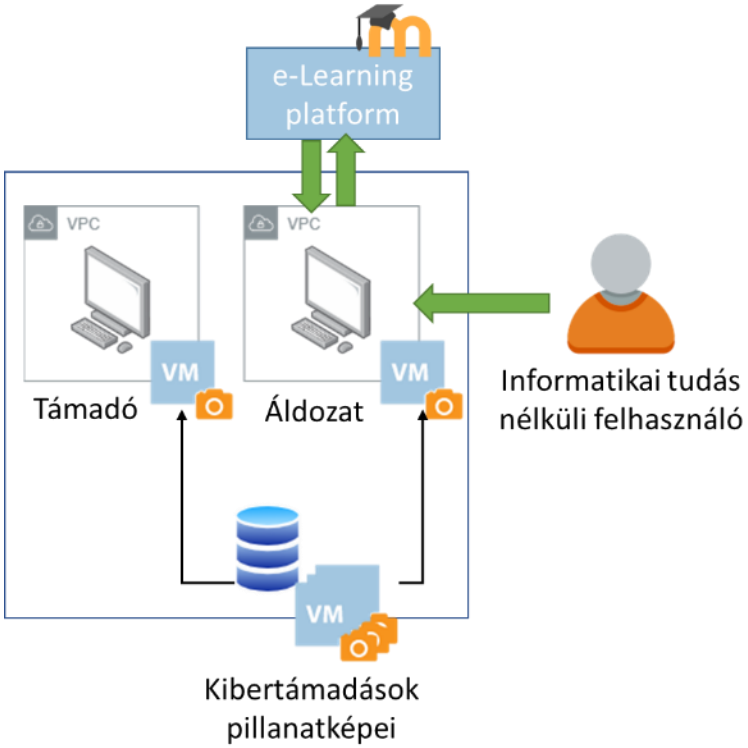
5.3.4.2. Védelmi intézkedések tárolása és ismételt végrehajthatósága

A hallgató által végrehajtott védelmi intézkedések tárolásának és ismételt végrehajthatóságának célja, hogy a vizsgafeladat megoldását követően az oktató és a hallgató számára is azonosíthatóvá váljon az adott feladatra kapott pontok száma. Ezen kívül ennek segítségével a vizsgafeladat megoldását követően az oktató is végre tudja hajtani a hallgató által elvégzett műveleteket, így azonosíthatók az egyes hiányosságok, hibák és az esetleges kérdéses pontok. Amennyiben a hallgató nem ért egyet a kapott pontszámokkal, úgy a tárolhatóságnak és az ismételt végrehajthatóságnak köszönhetően nyomon követők a kibertámadás elhárítására tett konkrét intézkedések.

A tárolás során biztosítani kell, hogy a végrehajtott módosításokat naplózzuk. Egyszerű megoldás a dokumentáció elkészítése a hallgatók által képernyőképek elhelyezésével, vagy egy bonyolultabb, magasabb szintű megoldás a hallgatói gépről kiadott összes operációs rendszer-specifikus utasítás loggolásra. Az utóbbi megoldás bár sokkal pontosabb visszajátszási lehetőséget biztosít, jóval nagyobb idő és erőfeszítés befektetésére van szükség az oktató részéről.

5.4. EGYSZERŰSÍTETT SZIMULÁCIÓS KÖRNYEZET

A H-5.3 és H-5.4 hipotézisek igazolására nem indokolt bonyolult, komplex platform alkalmazása, ennek értelmében egy egyszerűbb szimulációs környezetet implementáltam, amelynek architektúráját az 5-8. ábra szemlélteti.

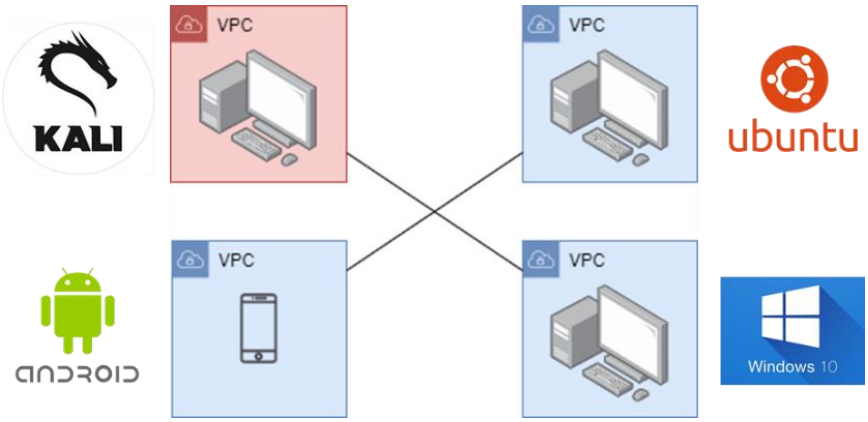


5-8. ábra Szimulációs hálózat

Az architektúrának két fő eleme van: egy támadó és egy áldozati gép, amelyek egy hálózatban találhatóak. Ennek segítségével a támadó képes kibertámadást végrehajtani az áldozat gépe ellen, így valós támadás szimulálható a felhasználó számára. A prototípus során a támadó-forgatókönyveket a támadó és az áldozat által elindítandó virtuális gépek pillanatfelvételeként lehet meghatározni. Ezáltal a támadásokhoz kapcsolódó virtuális gépeket olyan állapotban lehet elindítani, amely az adott támadást automatikusan végrehajtja. A konkrét prototípus elkészítése során a Moodle platformot használtam oktatási anyag megosztására és a vizsgáztatás lebonyolítására.

5.4.1. Infrastruktúra

Az infrastruktúra (lásd 5-9. ábra) összesen négy elemből épül fel, amelynek célja egy támadó komponens, illetve több infokommunikációs eszköz szimulálása, amelyet a közszolgálatban dolgozó emberek is használhatnak a mindennapjaik során. Minden komponens egy-egy virtuális gép, amelyekre különböző operációs rendszereket telepítettem.



5-9. ábra Egyszerűsített infrastruktúra a szimuláció végrehajtásához

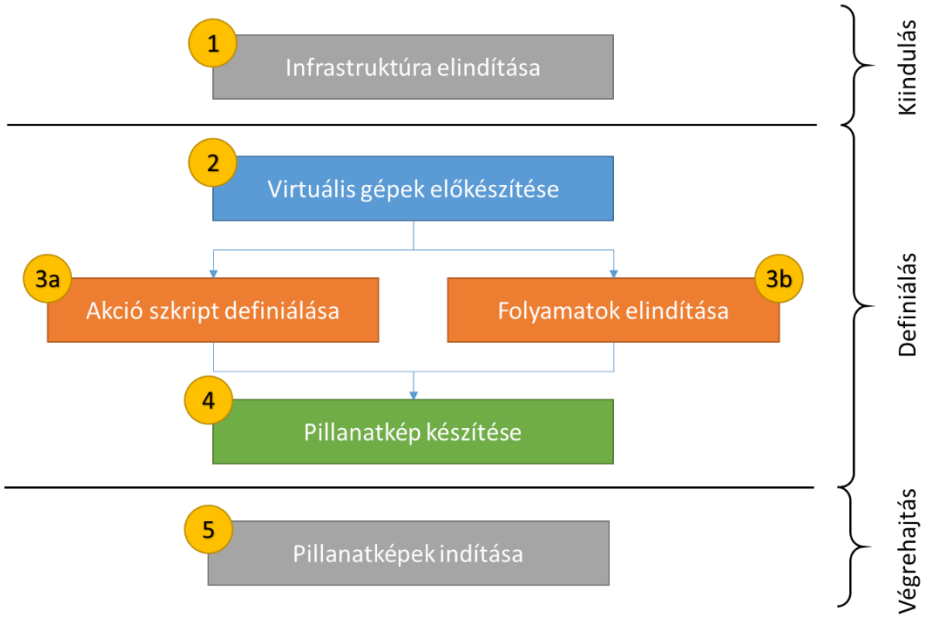
- Kali Linux: Sérülékenységvizsgálatra és behatolástesztelésre kialakított Linux disztribúció. Olyan alkalmazásokat és eszközöket tartalmaz előre telepített formában, amelyek segítségével etikus támadások indíthatóak a hálózatban található eszközök ellen.
- Ubuntu: Az egyik legszélesebb körben használt Linux alapú operációs rendszer. Fő erőssége, hogy a mindennapokban szükséges feladatok elvégzéséhez is található rajta megfelelő alkalmazás. A kiválasztás oka, hogy sok szervezeten belül gyakran találkozhatunk Linux/Unix alapú operációs rendszerekkel.
- Windows: A legelterjedtebb operációs rendszer személyi számítógépekre, amelyet egyetemek, vállalatok és közszolgálati szervezetek is előszeretettel használnak.
- Android: Az egyik legelterjedtebb mobil operációs rendszer, amely megtalálható mobiltelefonokon, tableteken és egyéb infokommunikációs eszközökön egyaránt.

Az összes virtuális komponenst egyetlen hálózatra csatlakoztattam, amelyen keresztül képesek egymással kommunikálni. Minden komponensnek fix hálózati címet állítottam be (IP cím), ezáltal minden egyes újraindítás során ugyanazon a címen érhetőek el.

5.4.2. TÁMADÁS MEGHATÁROZÁSA ÉS VÉGREHAJTÁSA

A definiált infrastruktúrán felvehetőek, rögzíthetőek és végrehajthatóak kibertámadások a komponensek között. A támadó fél minden esetben a Kali Linux-szal rendelkező virtuális gép volt. A támadás meghatározásához az 5-10. ábra által

meghatározott feladatokat szükséges elvégezni. A meghatározás során elsődleges cél, hogy a támadás elmenthető és automatizáltan újra végrehajtható legyen.



5-10. ábra: Támadás szimulációjának előkészítése

A támadás szimulációjának előkészítése három szakaszból áll. A kiindulás szakaszában kerül sor első lépésként az **infrastruktúra elindítására**, amely mindössze annyit jelent, hogy azokat a virtuális gépeket, amelyeknek szerepük lesz a szimuláció során, elindítjuk.

A definiálás folyamat során a virtuális gépeket úgy módosítjuk, hogy a kibertámadás végrehajtható legyen. Ezen módosítások magában foglalják a virtuális gépek előkészítését, az akció szkript definiálása és a támadáshoz kapcsolódó folyamatok elindítását, valamint pillanatkép elkészítését.

A **virtuális gépek előkészítése** során az egyes virtuális gépeken elvégezzük a szükséges támadásspecifikus módosításokat, beállításokat. Ha szükséges, ezek érvényre juttatásához újraindítjuk őket.

A következő lépést jelentősen meghatározza, hogy a támadás komplex, több lépésből álló szekvenciális folyamat (3a), vagy folyamatos támadás lesz (3b), amelyekhez olyan szolgáltatásokat kell elindítani, amelyek megállás nélkül futhatnak.

A szekvenciális folyamat során **akció szkript definiálása** indokolt, ahol lépések sorozatát írjuk le. Az egyik lépés felhasználhatja az előző lépés kimenetét, de minden esetben, minden lépés befejeződik a támadás végrehajtása során. A támadás lépései

shell szkript[11] segítségével definiálhatóak a Kali Linux-ot kiszolgáló virtuális gépen, amelyet az asztalon található *start.sh* fájlban kell eltárolni. Ennek a fájlnak sajátossága, hogy hozzáadtam a *crontable* konfigurációhoz, emiatt minden újraindításkor automatikusan végrehajtódik a fájl tartalma. Ha a szkript írása befejeződött, és elmentettük, akkor a gépet leállítjuk, továbbá a többi komponenst is leállíthatjuk.

Folyamatos támadás esetén kerül sor a **folyamatok elindítására**, amely során a támadáshoz kapcsolódó szolgáltatásokat kell elindítani, amelyek folyamatosan futni fognak a támadás során. Ebben az esetben a virtuális gépeket nem állítjuk le, csak szüneteltetjük. (Természetesen ez a fajta folyamat is megoldható lenne a 3a lépés segítségével, azonban ebben az esetben nincs szükség a szkript megírására, ezáltal sokkal gyorsabb és könnyebb a támadás definiálása.)

Az eddig bemutatott lépésekkel sikeresen elindíthatók a támadások, azonban a cél, hogy ezek a támadások könnyen hordozhatók és újra végrehajthatók legyenek. Emiatt szükséges a folyamat utolsó lépése. Mivel a virtuális gépeken módosításokat hajtottunk végre, ezért pillanatképeket kell készíteni róluk. A pillanatkép készítésének célja, hogy a számítógépet abba az állapotba töltsük vissza, amikor a kibertámadás éppen zajlott. Minden elindított komponens esetén azonos nevet adtam a pillanatképeknek, hogy könnyen azonosítható legyen, mely támadáshoz mely pillanatkép tartozik.

Utolsó lépésként a támadások szimulálásához az előzőekben ismertetett módon elkészített **pillanatképeket** kell **elindítani**. Ez a jelenlegi implementációban manuálisan történt meg, de a virtuális gépek automatikusan is indíthatóak. Fontos, hogy a támadások inicializálásakor mindig az áldozatok gépét kell először elindítani, hogy amikor a támadógép is a hálózatra kerül, már minden gép elérhető legyen.

5.4.3. KIBERTÁMADÁSOK SZIMULÁCIÓJA

A szimulációs környezetben három korábban ismertetett kibertámadási típust implementáltam le: szolgáltatás megtagadással járó támadást (DoS), az adathalászat (phishing) és hátsóajtó programot (backdoor) telepítettem. Ezeket úgy alakítottam ki, hogy különböző infokommunikációs eszközökön, operációs rendszereken lehessen szimulálni.

[11] GNU, P. (2007). Free Software Foundation. Bash (3.2. 48) [Unix shell program]

Minden egyes támadás leírása során a következő felosztást alkalmazom:

1. **Támadógép beállítása**: bemutatja, hogy melyek azok a fontosabb lépések, amelyeket a támadógépen elvégeztem a támadás szimulációjához.
2. **Áldozatgép beállítása**: bemutatja, hogy melyek azok a fontosabb beállítások, amelyeket az áldozat eszközén végrehajtottam annak érdekében, hogy a támadás sikeres legyen.
3. **Támadás érzékelése**: bemutatja, hogy az áldozat/támadó mit tapasztal a támadás során.
4. **Megszerezhető tudás**: bemutatja, hogy mi az a tudáshalmaz, amit a szimuláció során az áldozat megismerhet.

5.4.3.1. *Szolgáltatásmegtagadással járó támadás (DoS)*

a) **Támadógép beállítása***:* A DoS támadáshoz a Kali Linux-on előretelepített *hping3*[12] alkalmazást használtam az alábbi paraméterezéssel:

```
hping3 10.0.2.5 --icmp –flood
```

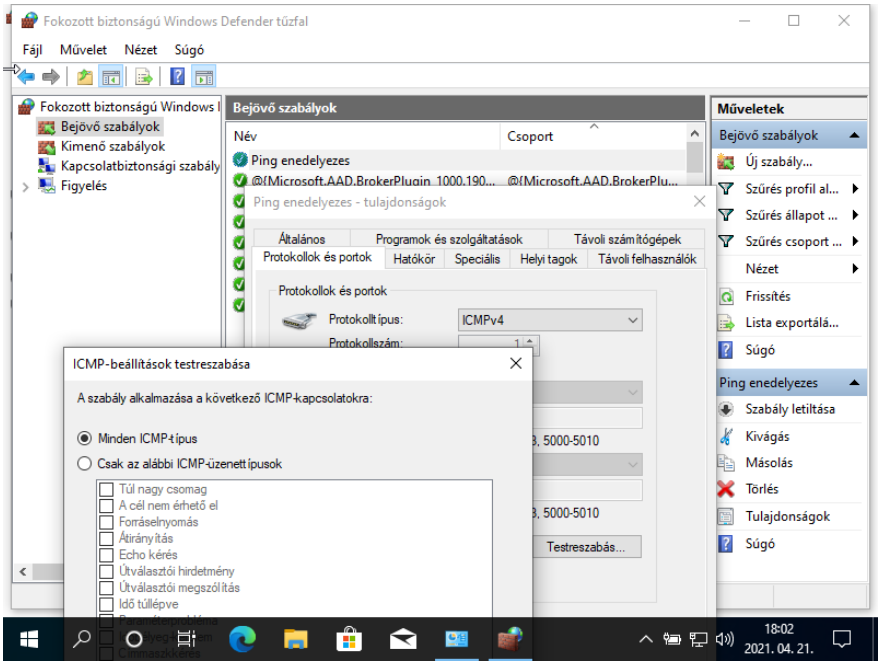
A kiadott parancs hatására a támadógép a hálózaton található 10.0.2.5 IP címmel rendelkező eszközt szólítja meg az úgynevezett Internet Control Message Protocol13 (ICMP) protokollban meghatározott kérésekkel. A támadógép pillanatképét akkor készítettem el, amikor a parancsot kiadtam. Ezáltal újraindítás után a kiadott parancs fog futni. Az áldozat pillanatképét a szabály aktiválása után kikapcsolt állapotban készítettem el.

b) **Áldozatgép beállítása***:* A DoS támadáshoz kapcsolódóan a Windows operációs rendszerrel rendelkező virtuális gépet választottam. A Windows alapértelmezetten nem reagál az ICMP kérésekre, ezért módosítottam a tűzfalat úgy, hogy egy olyan bemenő szabályt vettem fel, amely engedélyezi az ICMP kérésekre történő válaszadást. (5-11. ábra) Az áldozat pillanatképét a szabály aktiválása után kikapcsolt állapotban készítettem el.

c) **Támadás érzékelése**: A szimulációs környezet elindítása után, amikor az áldozat gépe csatlakozik a hálózathoz, teljes mértékben használhatatlanná válik a rengeteg kérés kiszolgálása miatt. Elsősorban a processzor lesz túlterhelve, amely miatt az áldozat nem képes a rendszert használni.

[12] hping3, Kali Tools, https://tools.kali.org/information-gathering/hping3
[13] ICMP, IETF Standards, https://tools.ietf.org/html/rfc792

d) **Megszerezhető tudás**: Az áldozat ebben a szimulációban szembesül azzal, hogy fizikai beavatkozásra is szükség van ahhoz, hogy egy kibertámadást elhárítson, hiszen a hálózati kábelt ki kell húznia a gépből (esetleg a routert le kell állítani). Ezen kívül megismerkedik az áldozat a Windows tűzfal beállításaival és képes lesz értelmezni a bejövő és kimenő szabályokat.



5-11. ábra Windows tűzfal szabályok beállítása

5.4.3.2. Adathalászat (phishing)

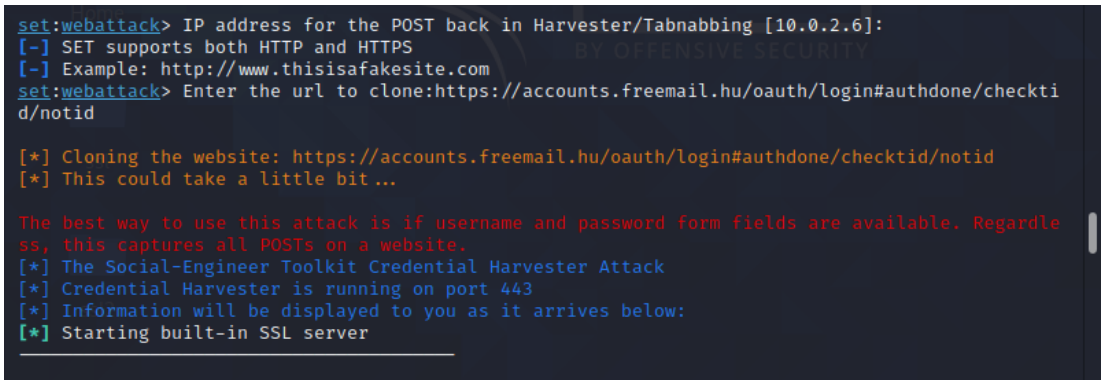
a) **Támadógép beállítása**: Ehhez a támadáshoz a Kali Linux-on megtalálható *SEToolkit* csomagjában található *credential harvester* alkalmazást használtam, annak érdekében, hogy lemásoljam a https://freemail.hu levelező weboldal bejelentkező felületét, továbbá megszerezzem az áldozat e-mail címét és jelszavát. A beállítás során engedélyeztem a biztonságos *https* kapcsolatot, amelyhez az *openssl* alkalmazás segítségével létrehoztam egy tanúsítványt is. Ennek célja, hogy a felhasználóval elhitessük, hogy egy biztonságos weboldalra látogat.

A pillanatkép elkészítéséhez két fontos alkalmazásnak kellett futnia:

1. Egy egyszerű webszerver fut abban a mappában, amelyben megtalálható az a tanúsítvány, amelyet a kliensnek telepítenie kell a böngészőben.

```
python2 -m SimpleHTTPServer 80
```

2. A credential harvester fut, vagyis várja, hogy az áldozat meglátogassa a támadó által klónozott weboldalt (5-12. ábra).

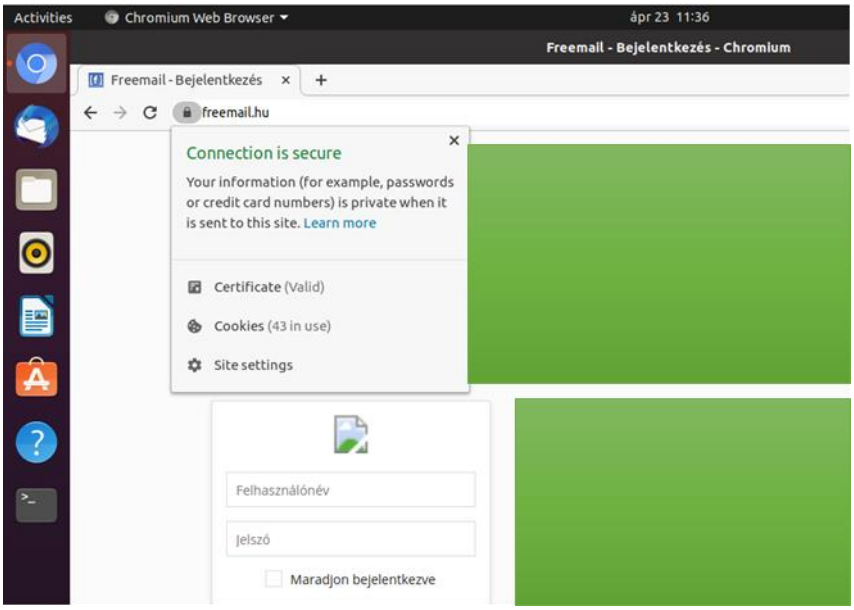


5-12. ábra: a támadógép várakozik, hogy valaki meglátogassa az áloldalt

b) **Áldozatgép beállítása**: Az áldozat gépe jelen támadás során az Ubuntu operációs rendszerrel rendelkező virtuális gép, amelyen az előkészület során két fontos módosítást kellett végrehajtani. Először is az alapértelmezett böngészőn keresztül letöltöttem és telepítettem a megfelelő tanúsítványt úgy, hogy az engedélyezze a támadógépen lévő oldallal történő biztonságos kommunikációt. Majd az */etc/hosts* fájlhoz kellett felvennem az alábbi sort:

```
10.0.2.4        freemail.hu
```

Ennek segítségével a támadó által előállított weboldal az ismert domain címen keresztül is elérhető, ahogy azt az 5-13. ábra is mutatja:

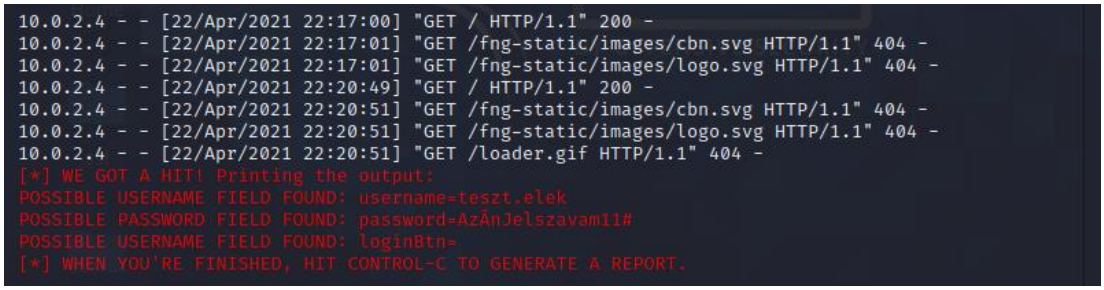


5-13. ábra: A kliens oldalon biztonságosnak tűnő megtévesztő oldal

c) **Támadás érzékelése**: A felhasználó megpróbál belépni az email fiókjába, beírja felhasználónevét és jelszavát, azonban az oldal elsőre újratöltődik, viszont másodjára sikeresen be lehet jelentkezni az e-mail fiókba. A támadás

észlelését korlátozza, hogy a kommunikáció biztonságos, mivel a megfelelő tanúsítványok rendelkezésre állnak. Azonban a weboldalhoz kapcsolódó domain névhez tartozó IP cím lekérdezésével láthatóvá válik, hogy a hálózaton belüli szerverhez kapcsolódik a felhasználó, amelyből már sejthető, hogy támadás érte felhasználót.

Fontos feladat az áldozat számára megmutatni a támadó felhasználói felületét és jelezni, hogy ténylegesen megkapja a támadó a beírt adatokat, hiszen ennek segítségével még valóságosabbá válik a támadás. (5-14. ábra).



5-14. ábra: A támadó sikeresen ellopta az adatokat

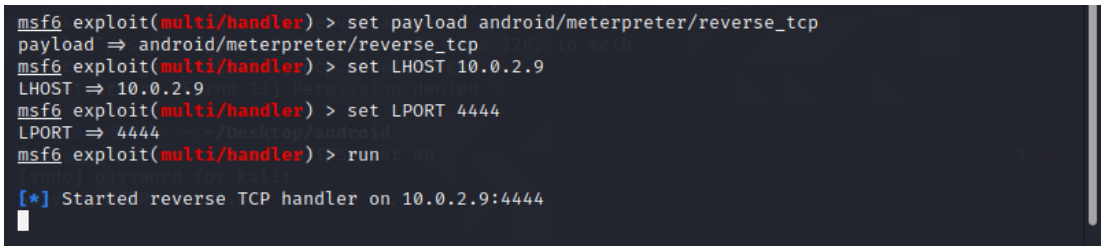
d) **Megszerezhető tudás***:* Az áldozat megismerkedik a tanúsítványok (certificate) szerkezetével és jellemzőivel, a böngészők limitációival, illetve az SSL kapcsolat jelentésével. Ezen kívül a DNS szolgáltatás alapjaival, a domain név feloldásával, illetve az operációs rendszerek *hosts* fájljával.

5.4.3.3. *Hátsóajtó program (Backdoor)*

a) **Támadógép beállítása***:* A Kali-Linux-on található *metasploit* keretrendszer segítségével lehetőség van olyan Android-os telepítő alkalmazás létrehozására, amely egy hátsó kaput nyit azon az Android-os eszközön, amely telepíti az így létrehozott alkalmazást. Az alkalmazást az alábbi paranccsal lehet létrehozni, ahol azt az IP címet és portot kell megadni, amelyen a támadó gép figyelni fog és várni fogja, hogy az áldozat elindítsa az alkalmazást:

```
msfvenom -p android/meterpreter/reverse_tcp
LHOST=10.0.2.4 LPORT=4444 R
```

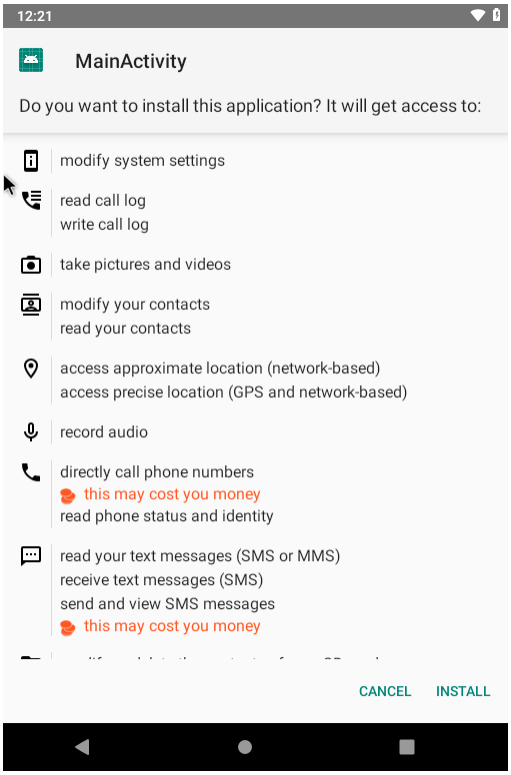
Az alkalmazás elkészülte után el kell indítani a várakozást, amelyhez a *metasploit* keretrendszer exploit/multi/handler alkalmazását szükséges elindítani megfelelő paraméterezéssel (5-15. ábra).



5-15. ábra: A támadógép várakozik backdoor indítására

Végül ahhoz, hogy az áldozathoz is eljusson a kívánt telepítő, egy üzenetet küldtem az áldozat e-mail címére a letöltő linkkel együtt (5-16. ábra). Az ilyen típusú támadásoknál célszerű az áldozat egyik ismerősét megszemélyesíteni, ugyanis e kapcsolat valamilyen szintű bizalmat feltételez, amely segítségével egy esetleges „nem biztonságos” figyelmeztető üzenet ignorálása elérhető. A tesztüzenet ezt hivatott szemléltetni.

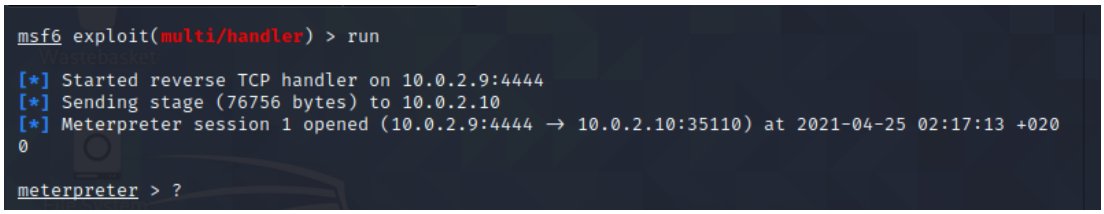
5-16. ábra Megtévesztő email



5-17. ábra: Alkalmazás telepítése

b) **Áldozatgép beállítása***:* Az áldozat gépe az Android operációs rendszert futtató virtuális gép, amely megszemélyesíthet mobiltelefont, tabletet, televíziót vagy bármilyen egyéb okos eszközt. Az áldozat gépén jóvá kellett hagyni az ismeretlen alkalmazások telepítésének engedélyezését a Google Chrome alkalmazásból, amelynek hatására az áldozat olyan alkalmazásokat, is képes telepíteni az eszközére, amelyeket nem a hitelesített Play Áruházból tölt le.

c) **Támadás érzékelése***:* A támadás érzékeléséhez az áldozatnak telepítenie kell a létrehozott alkalmazást (5-17. ábra). Ahhoz, hogy az áldozat lássa milyen hatása lehet annak, ha egy ilyen alkalmazást telepít, érdemes megmutatni neki a támadó terminálját (5-18. ábra), amelyen keresztül néhány parancs beírásával könnyedén szembesülhet azzal, hogy mi minden elérhető távolról. A teljesség igénye nélkül az alábbi parancsokat lehet érdemes megmutatni:
   - *dump_sms*: az összes sms letöltése a támadógépére
   - *dump_contacts*: az összes névjegy letöltése a támadógépére
   - *webcam_stream*: a kamera képének továbbítása a támadó gépére
   - *geolocation*: a telefon helyzetének elküldése a támadó gépére



5-18. ábra: A backdoor aktivizálódott a támadó gépén

d) **Megszerezhető tudás***:* Az áldozat szembesül a megtévesztő e-mailek céljával és legfőbb típusával, az Android-hoz kapcsolódó telepítő fájlokkal és beállításokkal, a Play Protect és egyéb alkalmazások fontosságával.

5.4.4. INTEGRÁLÁS E-LEARNING PLATFORMOKHOZ

A szimulációs környezetben végrehajtott kibertámadások elsődleges célja a hallgatók felkészítése a hasonló eseményekre történő hatékony és eredményes reagálás érdekében. Ehhez kapcsolódóan az egyes szimulált kibertámadásokhoz gyakorlati oktatást és vizsgát is definiáltam, amelyeket a Moodle e-learning platformon alakítottam ki.

5.4.4.1. Gyakorlatok

A gyakorlati oktatás során a hallgatók egy tárgy keretein belül a három szimulált kibertámadáshoz kapcsolódó témával ismerkedhetnek meg. Az adott témán belül a hallgatók bevezető kérdések segítségével sajátíthatják el a támadáshoz szükséges alapvető ismereteket, valamint a támadás elleni védelmi mechanizmusokat a virtuális gépek segítségével a gyakorlatban is végrehajthatják. Az elméleti felvezetés és a kérdések előnye, hogy azok folyamatosan vezetik a hallgató által teljesítendő

feladatokat. A kérdések kitöltését követően a hallgatók a helyes válaszok megismerése után többször is végrehajthatják a védelmi intézkedéseket.

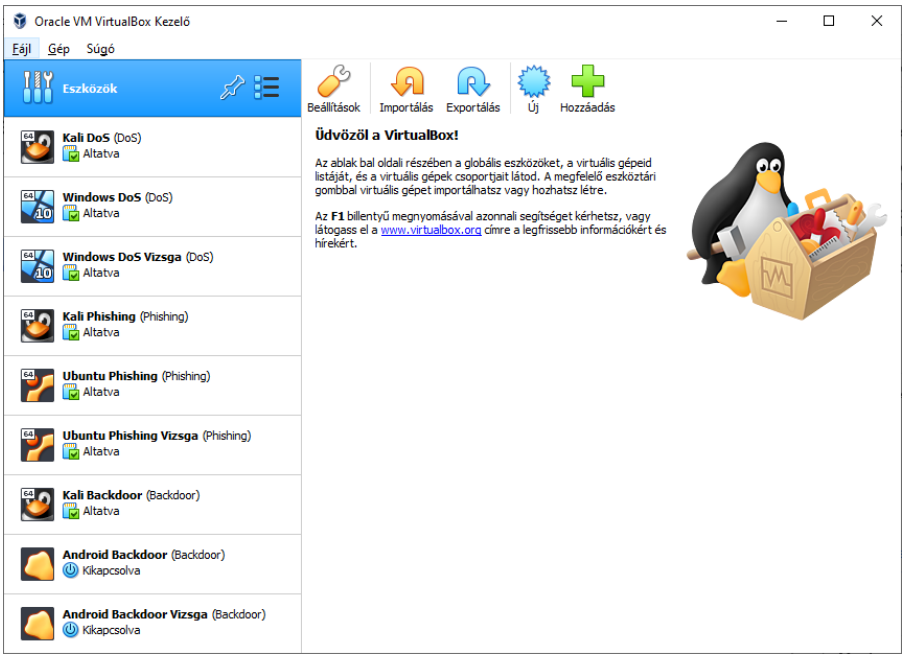
A szimuláció során a támadások végrehajtásának célja, hogy a hallgatók egy szimulált környezetben kibertámadás áldozatává váljanak, amely segítségével valós helyzetben szemléltethető számukra, hogy egy támadó milyen információkat képes megszerezni az áldozat infokommunikációs eszköze segítségével, illetve hogyan tudja ellehetetleníteni az áldozatot. Ezen kívül a szimuláció célja azonosítani azokat a védelmi mechanizmusokat, amelyekkel a támadások elháríthatók, megelőzhetők. A hallgatók kibertámadásban történő részvétele azért elengedhetetlen, mert így a „saját bőrükön” tapasztalhatják meg, hogy egy kibertámadás hogyan is néz ki a valóságban, milyen védelmi mechanizmus segítségével hárítható el, illetve előzhető meg.

5.4.4.2. Vizsgák

A vizsga elvégzésének célja, hogy felmérjük a hallgatók gyakorlati oktatás és a szimuláció során elsajátított tudását és a tudásátadás hatékonyságát. A vizsga kérdései hivatkoznak a már megszerzett tudásra.

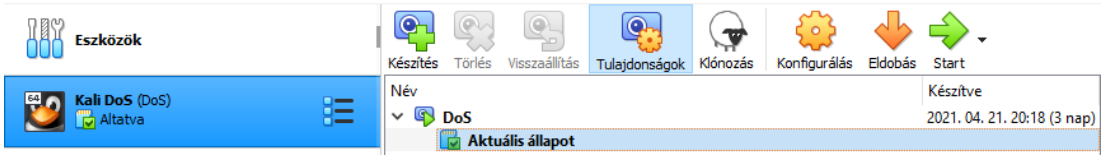
5.4.4.3. Szimulációs környezet használata

A szimulációs környezetet az 5.4.1 alfejezetben definiált módon állítottam össze. A gyakorlat és vizsga feladatok megoldásaihoz az 5-19. ábra szerinti virtuális gépeket alakítottam ki.



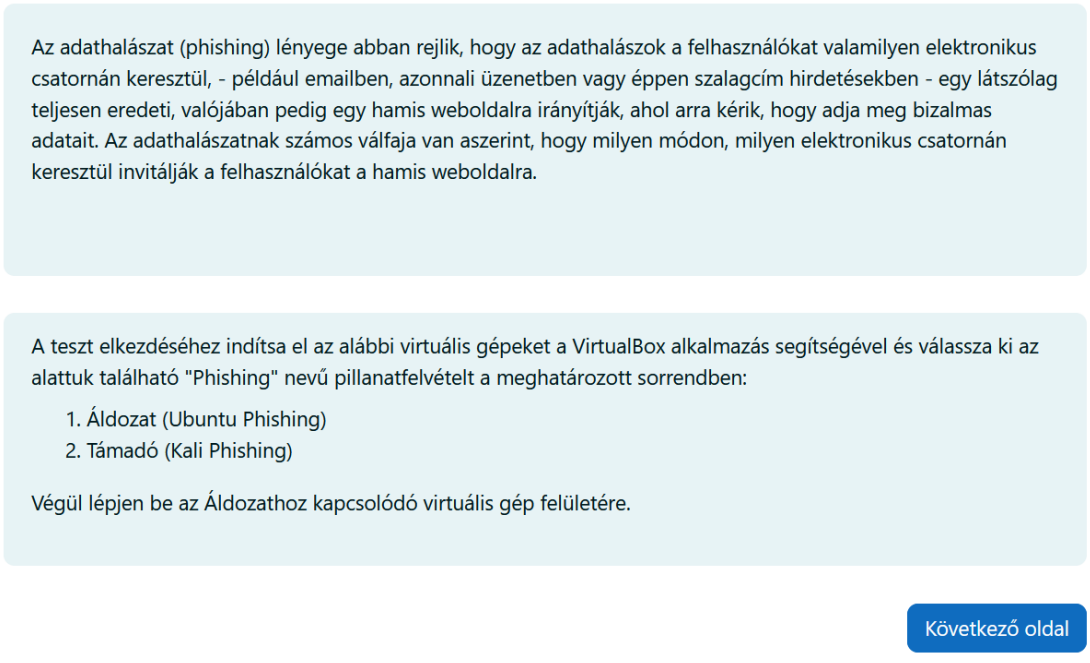
5-19. ábra: Oktatási célból készített virtuális gépek

A virtuális gépekhez az e fejezetben definiált módon készítettem el a pillanatképeket, ahogy az 5-20. ábra is mutatja mintaként a DoS támadáshoz kapcsolódó pillanatkép.



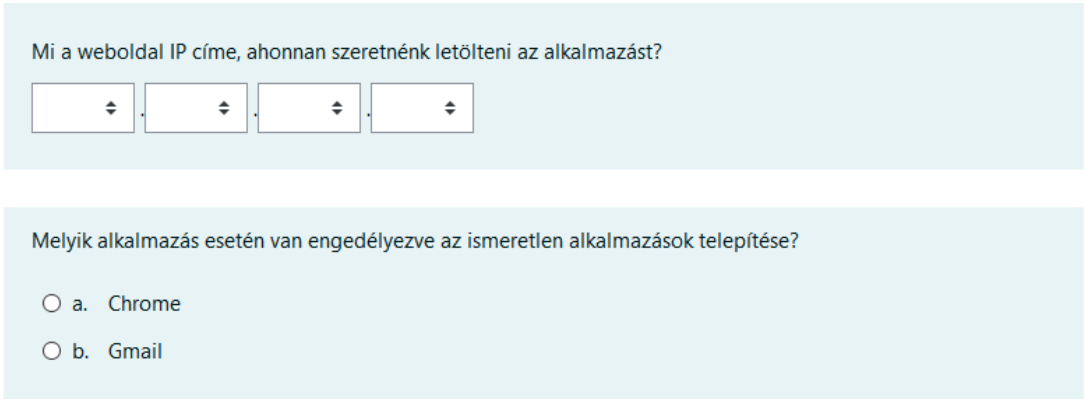
5-20. ábra: Pillanatképek használata a gyakorlatban

A gyakorlatok és vizsgák végrehajtása a Moodle rendszer segítségével történik. A Moodle rendszerben a felhasználók a Saját infokommunikációs eszközök védelme nevű kurzuson belül találják meg az ahhoz tartozó gyakorlatot és vizsgát. A gyakorlat a három korábban említett támadásra vonatkozó témából áll, amelyre rákattintva a hallgatók elindíthatják a gyakorlati oktatást. A kurzus gyakorlati részére vonatkozó példát az 5-21. ábra szemlélteti. Ebben a részben a hallgatók alapismeretekkel, alapfogalmakkal ismerkednek meg, valamint számos instrukciót kapnak a virtuális gépek megfelelő módon történő elindításával és a védekezési intézkedések gyakorlati végrehajtásával összefüggésben.



5-21. ábra A kurzus gyakorlati részének első feladata

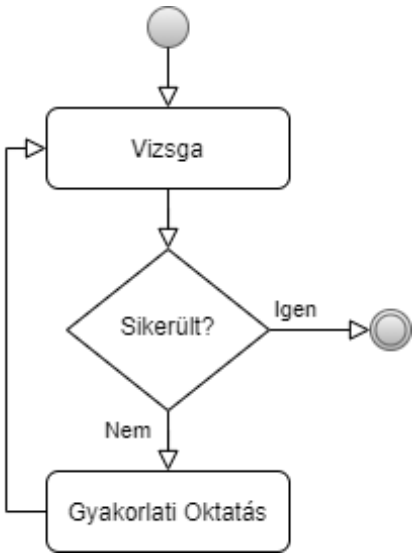
A kurzus vizsga részét a hallgatók külön a vizsga elvégzésének céljára létrehozott virtuális gépek elindításával kezdik, majd a védekezési intézkedések végrehajtásával és a kérdések megválaszolásával folytatják. Az 5-22. ábra szemléltet két példát a vizsgában található kérdésekre.



5-22. ábra A kurzus vizsga részéhez tartozó mintakérdések

5.4.5. KIÉRTÉKELÉS

A kiértékelést úgy folytattam le, hogy egy előre kiválasztott felhasználói csoporton kísérletet hajtottam végre, amely során a szimuláció működését és alkalmazhatóságát teszteltem a gyakorlatban. A kísérlet célja, hogy a közszolgálati kiberbiztonsági képzés célcsoportjához illeszkedő résztvevőkkel elemezhessem a szimuláció és gyakorlati képzés hatékonyságát és eredményességét. A kiértékelés során a cél az volt, hogy igazoljam a H-5.4 alhipotézist, amely szerint az általam definiált egyszerűsített szimulációs keretrendszer felhasználható a közszolgálati kiberbiztonsági képzés során. Ehhez két feltételt kellett ellenőrizni. A résztvevők technikai segítségnyújtás nélkül képesek a gyakorlatot és a vizsgát teljesíteni, illetve a résztvevők mély informatikai tudás nélkül is képesek teljesíteni a vizsgát és a gyakorlatot.



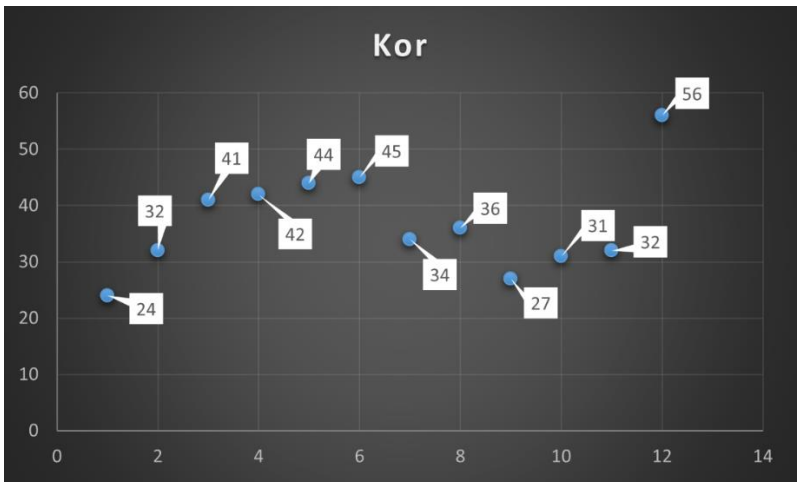
5-23. ábra Kiértékelés folyamata

A kiértékelés menetét az 5-23. ábra mutatja be, miszerint a résztvevők először megpróbálkoztak a vizsga teljesítésével, amennyiben az rosszul sikerült, akkor a gyakorlati oktatás keretében sajátították el a vizsga teljesítéséhez szükséges ismereteket, amelyet követően ismételten megpróbálkoztak a vizsga végrehajtásával. A gyakorlati oktatást addig hajtották végre, amíg a vizsga sikeresen nem zárult. Annak az oka, hogy a résztvevőket rögtön a vizsgakérdésekkel szembesítettem mindössze az volt, hogy ellenőrizhessem tényleg szükséges-e a gyakorlati oktatás megtartása és elvégzése vagy esetleg rendelkeznek-e már a megfelelő informatikai tudással.

A hallgatók által a környezet összeállítása és a vizsga végrehajtása teljesen önállóan zajlott. A gyakorlati oktatás során személyesen is jelen voltam, melynek fő célja, hogy az oktatási anyag minőségét fejlesszem. Abban az esetben, ha valamilyen oktatási rész nehezen érthető volt, vagy a résztvevő érdeklődését felkeltette az adott téma, személyesen válaszoltam a felmerült kérdésekre.

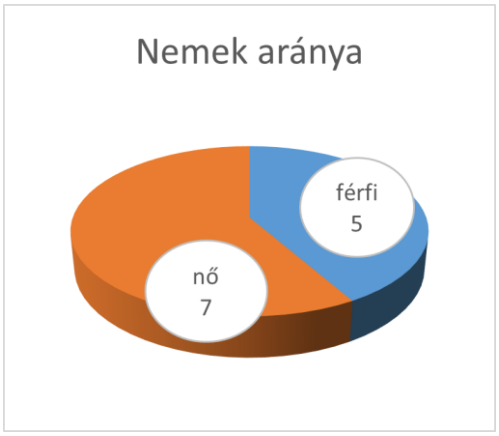
5.4.5.1. *Résztvevők*

Összesen 12 résztvevővel végeztem el a kísérletet, akik között vegyesen találhatóak nők és férfiak is. A 24-56 korosztályból megfelelően elosztott mértékben választottam személyeket többségében a közszolgálatból, de egyéb szakmák is képviseltették magukat, ahol az informatikai tudás nem jelentkezett követelményként, előfeltételként.



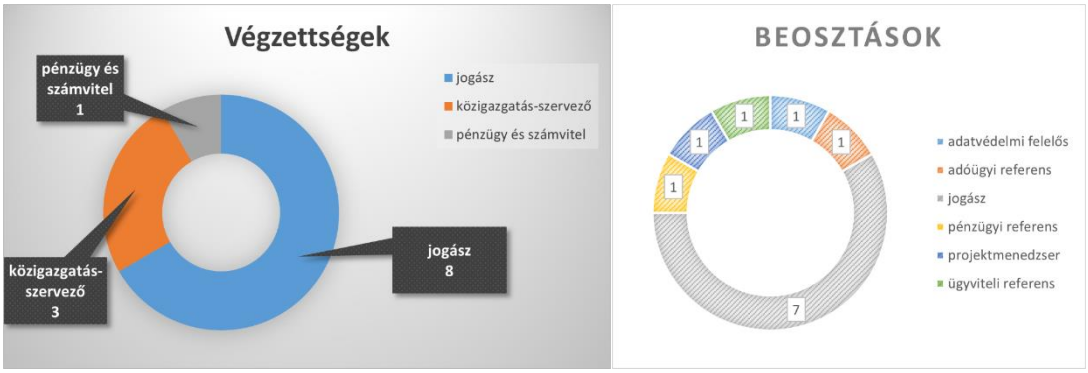
5-24. ábra A kiértékelésben résztvevők kora

Az 5-24. ábra mutatja be a mérésben résztvevők életkorát. Megállapítható, hogy a kísérletben 24 éves kortól 56 éves korig bezárólag többféle korosztály is képviselte magát, de jellemzően a résztvevők többsége a 30-40 éves korosztályba tartozik.



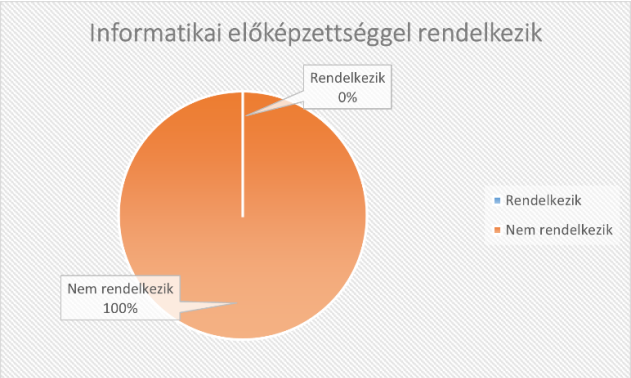
5-25. ábra A kiértékelésben résztvevők nemek szerinti aránya

A 5-25. ábra ismerteti a résztvevők nemek szerinti eloszlását, mely szerint a kísérletben résztvevők 58%-a nő, 42%-a pedig férfi. Ezek alapján megállapítható, hogy mindkét nem megfelelő számban képviselte magát.



5-26. ábra Végzettségek és beosztások szerinti eloszlás

Az 5-26. ábra célja bemutatni, hogy a kiértékelés során releváns közszolgálati feladatokat ellátó személyek vettek részt elsősorban jogi, közigazgatási és pénzügyi végzettségekkel. Ennek megfelelően, ahogyan azt az 5-27. ábra is szemlélteti, a résztvevők nem rendelkeztek mély informatikai tudással.



5-27. ábra A kiértékelés során informatikai előképzettséggel rendelkezők aránya

5.4.5.2. Végrehajtás

A végrehajtás során az F2. függelékben található gyakorlati és vizsgasort használtam. A mérés kezdetekor a résztvevők első feladata a vizsgakérdések megoldása volt. Ennek oka mindössze az volt, hogy ellenőrizhessem tényleg szükséges-e a gyakorlati oktatás megtartása és elvégzése vagy esetleg a résztvevők rendelkeznek-e már a megfelelő informatikai tudással és képesek sikeresen végrehajtani a vizsgafeladatokat. A résztvevők közül senki sem volt képes a vizsga eredményes teljesítésére, ahogyan azt az 5-28. ábra is szemlélteti, ezért mindannyian gyakorlati oktatásban részesültek.

5-28. ábra Vizsgaeredmény az oktatás végrehajtása előtt

Ezen oktatás során sajátíthatták el a résztvevők a vizsga teljesítéséhez szükséges ismereteket. Az oktatás nem a vizsgafeladat vezetett megoldását tartalmazta, hanem elméleti hátteret biztosított a különböző támadási és védekezési technikáknak, illetve bemutatta a különböző operációs rendszerek védelmi eszköztárát, amit egy támadás során a vizsgázó használhat.

Ezt követően a kísérletben résztvevők ismételten megpróbálkoztak a vizsga végrehajtásával. A gyakorlati oktatást követő vizsgát minden résztvevő (12 fő) sikeresen teljesítette, ahogyan azt az 5-29. ábra is mutatja.

5-29. ábra Oktatás utáni vizsgaeredmények aránya

5.4.5.3. *Eredmények*

A kiértékelés során a személyek azonos teljesítményt értek el, mindössze a teljesítés idejében voltak eltérések. Egyetlen résztvevő sem volt képes a vizsgát gyakorlati oktatás nélkül teljesíteni, viszont az összes résztvevő képes volt a gyakorlati oktatás után a vizsgát sikeresen teljesíteni.

A virtuális gépek előkészítése és elindítása a résztvevők többsége számára könnyedén ment, de néhány esetben indokolt volt a technikai segítségnyújtás arra vonatkozóan, hogy a virtuális gépeket és a pillanatképeket milyen módon lehet kiválasztani és elindítani.

5.4.5.4. *Mérést befolyásoló tényezők*

Jelen pontban szükséges megemlíteni a mérés eredményét befolyásoló egyéb tényezőket. A kutatás során olyan körülmények befolyásolták a kutatás lefolytatását és annak eredményét, amelyet mindenképp szükséges megjegyezni, elemezni.

Fontos kiemelni, hogy a résztvevők létszáma és a végzettségek aránya csak egy kis szeletét azonosítják a közszolgálatban dolgozóknak és a későbbiekben érdemes a kiértékelést megismételni nagyobb résztvevői létszámmal és további végzettségekkel. Azonban kiemelném, hogy a kiértékelés célja a prototípus esetében elsősorban annak a vizsgálata volt, hogy lehetséges-e informatikai tudás nélkül az oktatást és a vizsgát végrehajtani. Ebből a szempontból a résztvevői létszám elégségesnek tekinthető.

Az informatikai előképzettség csak önbevalláson alapult, illetve nem történt hivatalos felmérés a részvevők informatikai tudásához kapcsolódóan. Ez alapján nem bizonyított, hogy a résztvevők ténylegesen nem rendelkeztek semmilyen informatikai tudással. A jövőben érdemes lenne a mérést kibővíteni az informatikai tudás szintjének előzetes felmérésével. Azonban a vizsga első teljesítése és az oktatás végrehajtása során meggyőződtem, hogy a résztvevők csak alapszintű, a mindennapi munkájukhoz elengedhetetlen informatikai tudással rendelkeztek (böngészés, szövegszerkesztő program ismerete, email-ek olvasása stb.). Az oktatás és a vizsga újbóli végrehajtása között csak limitált idő állt rendelkezésre. Ennek oka, hogy a résztvevők a munkájuk során egy dedikált időt tudtak rászánni a mérésre. Lehetséges, hogy ha az oktatás és a vizsga között több idő telik el (órák, napok), akkor az újbóli vizsga kevesebb résztvevő esetén lett volna sikeres. Azonban ilyen esetben már egyéb tényezők is befolyásolták volna a mérést, mint a tudásátadás hatékonysága, az oktatási anyag részletessége stb. Mivel a mérés célja továbbra is csak annak eldöntése, hogy megvalósítható-e az oktatás és vizsga az adott keretek között, így ezt nem tartottam a mérést túlzóan befolyásoló tényezőnek.

5.4.5.5. Tapasztalatok

A résztvevők többsége korábban nem tapasztalt a gyakorlat során bemutatottakhoz hasonló kibertámadásokat, kizárólag e-mailben érkező adathalász támadással találkoztak, amelyet a legtöbb esetben az üzenet helytelen magyarsággal íródott tartalma miatt ismertek fel. Éppen ezért a szimulációs oktatás előnyeként emelték ki a különféle támadási technikák bemutatását, azok felismerésének lehetőségeit, hiszen a támadás elhárítására irányuló intézkedések csak akkor alkalmazhatók eredményesen, ha a támadás észlelése megtörtént.

A támadások szimulálása során a résztvevők felismerték, hogy a kibertámadások típusai és céljai rendkívül sokrétűek. A szimulációs gyakorlati oktatást követően a résztvevők azt nyilatkozták, hogy a jövőre nézve sokkal elővigyázatosabbak lesznek, továbbá sokkal tudatosabban használják majd különféle infokommunikációs eszközeiket és online platformokat, kiemelt figyelmet fordítva az általános védelmi intézkedésekre és az esetleges fenyegetések felismerésére.

Minden résztvevő kiemelte, hogy a támadó gépének megmutatása a támadás után sokkal jobban motiválta és meglepte őket, mintha csak az áldozat gépén kellett volna végrehajtaniuk a védelmi intézkedéseket a gyakorlat során, hiszen így azt is

megtapasztalhatták, hogy milyen információkhoz férhet hozzá a támadó, így még valósághűbbnek tűnt a gyakorlat. Több résztvevő is jelezte, hogy a támadások valóságos átélése ráébresztette őket a biztonságtudatosság fontosságára, a szükséges védelmi intézkedések megismerésének, betartásának és kivitelezésének szerepére a kibertérből érkező fenyegetések káros következményeinek mérséklése érdekében. A gyakorlat előnyeként került megfogalmazásra az a vélemény, hogy segítségével nem csak elméletben tanulják meg, hogyan reagáljanak a különféle támadásokra, hanem a „saját bőrükön" tapasztalják milyen szembesülni egy valódi kibertámadással, így sokkal hatékonyabban képesek megjegyezni a védekezés során alkalmazandó intézkedéseket, hiszen nem csak elméletben ismerik meg azokat, hanem a gyakorlatban ki is próbálhatják az egyes lépéseket.

Összegezve, a tapasztalatok alapján megállapítható, hogy a szimulációs gyakorlat során olyan tudás került átadásra, amelyek segítségével elérhető, hogy a résztvevőket ne érje váratlanul egy valós támadás, illetve a már megszerzett tudást éles helyzetekbe is képesek legyenek átültetni.

5.5. KÖVETKEZTETÉSEK

Jelen fejezetben ismertetett kutatás egyfajta előkészítése és egyben bizonyítása volt az 5.1.1 pontban meghatározott alhipotézisek megválaszolásának.

A H-5.1 alhipotézisben azt vélelmeztem, hogy definiálható egy szimulációs környezetet leíró keretrendszer, amely segítségével a közszolgálatban dolgozó személyeket fel lehet készíteni a kibertámadások elleni védekezésre. E hipotézis igazolására egy szimulációs környezetet leíró keretrendszer definiálását tűztem ki célul. Ennek érdekében a keretrendszert alkalmazás és infrastrukturális rétegekre bontottam, valamint azonosítottam a keretrendszer alapjául szolgáló kibertámadások adatbázisát. Ezt követően felvázoltam a keretrendszer hardver architektúráját és bemutattam annak komponenseit, valamint a kibertámadások szimulációját hardver és alkalmazásszintre lebontva. Ez utóbbinak konkrét folyamatát meghatároztam, majd bemutattam, hogyan valósítható meg a távoktatás egy ilyen szimulációs környezetben.

A H-5.2 alhipotézis során azzal a feltételezéssel éltem, hogy kialakítható egy automatizált értékelési rendszer, amely alkalmas a gyakorlati képzési rész során átadott tudásanyag számonkérésére. Ennek bizonyítására definiáltam a szimulációs

környezetben megvalósuló gyakorlati oktatás egy lehetséges értékelési rendszerét. Ennek keretében a cél egy olyan automatizált értékelési rendszer megalkotása volt, amely oktatói felügyelet nélkül is képes a hallgatók munkájának ellenőrzésére és értékelésére. Ennek érdekében az elvégzett munka alapján történő érdemjegy azonosítását egy egyértelmű és következetes metrikák definiálásával határoztam meg. Az egyik ilyen metrika az elhárított kibertámadások száma, míg a másik az elért részállapotok száma. Ez utóbbi alkalmazásához a kibertámadási leírók bővítése szükségessé vált további állapot definíciókkal, amelyek meghatározzák, hogy a rendszer olyan állapotba jutott-e, amely megfelel egy részmegoldásnak. Ezen kívül a szimulációs folyamat bővítése is indokolttá vált, ezért további elemekkel bővítettem azt. Az értékelési rendszer részét képezi a hallgató által végrehajtott védelmi intézkedések tárolásának és ismételt végrehajthatósága, amelynek célja, hogy a vizsgafeladat megoldását követően az oktató és a hallgató számára is azonosíthatóvá váljon az adott feladatra kapott pontok száma.

A H-5.3 alhipotézis megfogalmazása során abból a feltételezésből indultam ki, hogy szimulálható olyan kibertámadás, amely azonosításához és megoldásához nem szükséges mély informatikai tudás. Egy egyszerűsített architektúrát azonosítottam a kibertámadások automatikus szimulációjára. A kibertámadások során virtuális gépeket lehet használni, amelyeket akár a saját számítógépünkön is elindíthatunk. A szimulációk definiálásra pillanatképeket lehet használni, illetve szükség szerint szkripteket is lehet írni, amelyek a virtuális gépek indításakor automatikusan lefutnak. A kialakított architektúrán megvalósítottam egy DoS, egy backdoor és egy phishing támadást is különböző platformokon, amelyek más és más infokommunikációs eszközt szimbolizáltak (asztali számítógép, mobiltelefon, tablet stb.). A szimulációhoz kapcsolódóan a feladatokat csak az áldozat gépen kellett végrehajtani, de szemléltetésképpen a támadógépen található konzolt is meg lehetett tekinteni. Az architektúrát és a támadásokat is összekapcsoltam a Moodle e-learning platformmal, ahol az egyes támadásokhoz gyakorlati oktatást és vizsgát is definiáltam.

A H-5.4 alhipotézis alapján a szimulációs keretrendszer felhasználható a közszolgálati kiberbiztonsági képzés során. Ennek igazolására a kialakított rendszert különböző mély informatikai tudással nem rendelkező személyekkel teszteltem le. Mindenki az előre elkészített szimulációs környezetében próbálta ki a vizsga feladatokat és a gyakorlati oktatást. A résztvevők rendkívül kreatívnak, izgalmasnak és interaktívnak

tartották a feladatokat. Kifejezetten örültek, hogy a támadásokkal a gyakorlatban is szembesülhettek és ténylegesen láthatták, hogy a támadó fél milyen adatokat képes megszerezni a szimulált kibertámadások során.

5.6. ÚJ TUDOMÁNYOS EREDMÉNYEK

Jelen fejezetben bemutatott kutatás által **bizonyítottam, hogy definiálható egy olyan műszaki keretrendszer, amely elsődleges a kiberbiztonsági tudatosság kialakítását és fejlesztését célozza, valamint lehetőséget biztosít kibertámadások elleni védelmi technikák, mechanizmusok gyakorlatban történő alkalmazására (E5).**

Kutatásom alapján az alábbiakat tekintem új tudományos részeredménynek:

Tudományos részeredmény 1. Definiáltam egy szimulációs környezetet leíró keretrendszer, amely segítségével a közszolgálatban dolgozó személyeket fel lehet készíteni a kibertámadások elleni védekezésre.

Tudományos részeredmény 2. Meghatároztam egy automatizált értékelési rendszert, amely alkalmas a gyakorlati képzési rész során átadott tudásanyag számonkérésére.

Tudományos részeredmény 3. Olyan kibertámadásokat szimuláltam, amelyek azonosításához és megoldásához nem szükséges mély informatikai tudás.

Tudományos részeredmény 4. A szimulációs keretrendszer felhasználható a közszolgálati kiberbiztonsági képzés során.

Jelen fejezet a [j1] és [f7] publikációkra épül, amelyek részletesen támasztják alá mind a négy tudományos részeredményt. A [j1] folyóiratcikkben egy szimulációs környezetet leíró keretrendszert definiáltam, valamint felvázoltam a keretrendszer hardverarchitektúráját és bemutattam annak komponenseit, a kibertámadások szimulációját hardver és alkalmazás szintre lebontva. Emellett meghatároztam a szimulációs környezetben megvalósuló gyakorlati oktatás automatizált értékelési rendszerét. Az [f7] tanulmányban egy, a kibertámadások automatikus szimulációjára alkalmas egyszerűsített architektúrát mutattam be, amelyen

keresztül különféle kibertámadásokat szimuláltam. A kialakított rendszer hatékonyságát és alkalmazhatóságát a közszolgálati kiberbiztonsági képzés célcsoportjához illeszkedő résztvevők segítségével teszteltem le.

6. ÖSSZEGZETT KÖVETKEZTETÉSEK

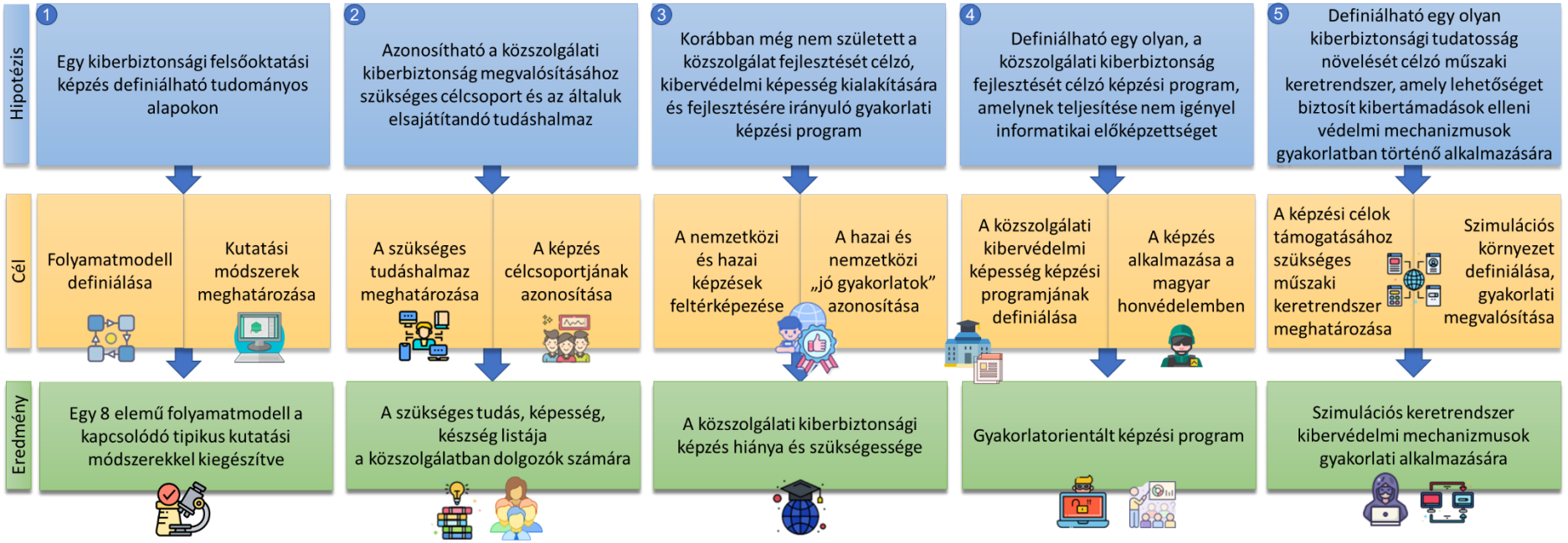
A kibertámadások száma exponenciális növekedést mutat, amelyek jelentős hatással vannak a gazdaságra, a társadalomra, valamint a szervezetek alapvető működésére nézve egyaránt. Egyre komplexebb és kifinomultabb kibertámadásokkal kell szembenéznünk nap mint nap, amelynek következtében új típusú kihívások jelennek meg a szervezetek életében. Ezzel összefüggésben szükséges kiemelni a szervezet és az abban dolgozó alkalmazottak kibervédelmi képességeinek kialakítását és fejlesztését, hiszen a megfelelő szintű felhasználói biztonságtudatosság jelentősen hozzájárulhat a kibertámadások bekövetkezési valószínűségének csökkentéséhez, valamint a támadások káros következményeinek mérsékléséhez.

A releváns kiberbiztonsági képességekkel rendelkező szakemberek felkutatása és foglalkoztatása során számos nehézséggel találkozhatunk, tekintettel a jelenleg fennálló kiberbiztonsági munkaerőhiányra, valamint ezen munkaerő iránti kereslet folyamatos növekedésére. A kibertámadások eredményes megelőzése és elhárítása érdekében elengedhetetlen a kibervédelmi képességek kialakítása és folyamatos fejlesztése. E képességek elsajátítására számtalan lehetőség áll rendelkezésünkre, a felsőoktatási képzésektől kezdve, a tudatosító kampányokon át, egészen a kibergyakorlatok megvalósításáig rendkívül széles skálán mozognak az elérhető kiberbiztonsági képzési programok. A megfelelő típusú képzés kiválasztásánál számos szempontot érdemes figyelembe venni, így például – a teljesség igénye nélkül - azok megvalósulási formáját, időtartamát, bemeneti követelményeit, a korábbi résztvevők gyakorlati tapasztalatait, tartalmát, valamint az elmélet és gyakorlat arányát.

A kibertámadások észlelése és előrejelzése komoly kihívásként jelentkezik, amelyek kezelésének alapvető eleme a felhasználók elméleti és gyakorlati kibervédelmi képességeinek kialakítása, fejlesztése. E célt hivatott szolgálni jelen értekezésben bemutatott közszolgálati kiberbiztonsági képzés definiálása, tekintettel arra, hogy a kiberbiztonsági oktatás rendkívül fontos szerepet tölt be a jelenlegi és a jövőbeli szakemberek kiberbiztonsági felkészítésében.

Jelen disszertációban definiált célkitűzések mentén azonosítottam azon hipotéziseket, amelyek bizonyításával e célok megvalósíthatók.

Értekezésem azon tudományos problémán alapul, hogy világszinten kiberbiztonsági munkaerőhiány jelentkezik, amely a közszolgálat alapvető működésének vonatkozásában is jelentős korlátot, akadályokat eredményezhet. Így például a megfelelő kompetenciákkal rendelkező szakemberek hiánya egy kibertámadás bekövetkezése esetén a szervezet üzletmenetfolytonosságát is jelentősen befolyásolhatja. E káros hatások mérséklését és megelőzését szolgálja disszertációm legfőbb célkitűzéseként definiált közszolgálati kibervédelmi képesség kialakítását célzó képzési program tudományos alapokon történő definiálása. Ennek érdekében végrehajtott kutatásom összefüggéseit a 6-1. ábra segítségével mutatom be:



6-1. ábra A disszertáció hipotéziseinek, céljainak és eredményeinek áttekintése

Kutatásom kezdetekor abból a feltételezésből indultam ki, hogy egy felsőoktatási képzés definiálható tudományos alapokon. Annak érdekében, hogy e hipotézist bizonyítsam, **definiáltam egy nyolcelemű folyamatmodellt, amely meghatározza a tudományos alapokon nyugvó felsőoktatási képzések tervezésének lépéseit, valamint azonosítottam azon kutatási módszereket, amelyek szükségesek a képzés tudományos alapokon történő meghatározására**. A bemutatott folyamatmodell és a kapcsolódó kutatási módszerek alkalmazhatóságát a közszolgálati kiberbiztonsági képzés teljeskörű definiálásával igazoltam.

Kutatásom célkitűzéseinek megfelelően vélelmeztem, hogy azonosítható a közszolgálati kiberbiztonság megvalósításához szükséges célcsoport és az általuk elsajátítandó tudáshalmaz. Ennek igazolására a képzési program megalkotásának kritériumfeltételeként **azonosítottam a közszolgálati kiberbiztonság megvalósításához szükséges célcsoportot, valamint az általuk elsajátítandó tudás-, képesség-, készséghalmazt,** amely segítségével a közszolgálatban megjelenő kiberbiztonsági feladatok az aktuális kiberbiztonsági kihívásokhoz igazodva végrehajthatók. Ennek oka, hogy a célcsoport és az elsajátítandó ismerethalmaz elengedhetetlen a képzés szükségességének igazolásához, a hasonló típusú képzések feltárásához, valamint a kapcsolódó gyakorlati tapasztalatok azonosításához. Ahhoz, hogy e célcsoport és ismerethalmaz minél teljesebb körű definiálása megvalósulhasson, mélyinterjú és dokumentumelemzés segítségével meghatároztam a kibertér aktuális kihívásait, amelyhez szorosan igazodik a képzés során elsajátítandó tudáshalmaz.

Jelen értekezés azon a feltételezésen alapszik, hogy korábban még nem született konkrétan a közszolgálat fejlesztését célzó, kibervédelmi képesség kialakítására és fejlesztésére irányuló gyakorlati képzési program. Ennek bizonyítására egy általam definiált összehasonlítási szempontrendszer alapján összehasonlítottam és elemeztem a hazai, valamint nemzetközi kiberbiztonsággal összefüggő felsőoktatási képzéseket. Az összehasonlítással célom volt a képzési program megvalósíthatóságának lehetőségeinek feltárása, tekintettel a képzésduplikáció elkerülésére, hiszen amennyiben már létezik a jelen értekezésben célul kitűzött képzéssel tartalmában azonos képzés, nem indokolt annak megtervezése. Mindemellett az összehasonlítás segítségével feltártam a vizsgált képzések hiányosságait, valamint az alkalmazott „jó gyakorlatokat”. A hazai és nemzetközi tapasztalatok implementálásának előnye, hogy

ezek már olyan hazai és nemzetközi színtéren kipróbált és bevált gyakorlatok, amelyek hatékonyságát az egyetemek eredményei már korábban igazolták, így azok hazai képzési rendszerbe történő átültetése jelentősen hozzájárulhat a képzés színvonalának növeléséhez, továbbá minőségének megteremtéséhez. A fentiek segítségével **bizonyítottam, hogy szükséges egy olyan eddig még nem létező képzési program megalkotása a hazai képzési környezetben, amely lehetőséget nyújt a közszolgálatban dolgozó, nem informatikai végzettségű személyek kibervédelmi képességének kialakítására.**

Kutatási célkitűzéseim meghatározásakor vélelmeztem, hogy definiálható egy olyan, a közszolgálat fejlesztését célzó képzési program, amelynek teljesítése nem igényel informatikai előképzettséget. E hipotézis bizonyítása érdekében **definiáltam a közszolgálati kiberbiztonsági képzés programját, a képzés alapjait, valamint a kapcsolódó alapfogalmakat, bemeneti és kimeneti követelményeit**. Ennek keretében azonosítottam a képzés struktúráját és egy tantervi háló segítségével definiáltam a képzés elméleti és gyakorlati része során elsajátítandó ismerethalmaz egyes témaköreit, illetve azok tartalmát. Ezt követően a közszolgálati kiberbiztonsági képzés Önkéntes Tartalékos Rendszerben történő alkalmazásának lehetőségére tettem javaslatot a korábban definiált képzés kibővítésével. Emellett meghatároztam a képzés során megvalósuló tudásátadás hatékonyságának mérésére szolgáló szempontrendszert és mérési módszert, amelynek segítségével a képzés tárgyainak fejlesztése folyamatosan biztosítható.

Kutatásom során azzal a feltételezéssel éltem, hogy definiálható egy olyan műszaki keretrendszer, amely lehetőséget biztosít kibertámadások elleni védelmi stratégiák gyakorlatban történő alkalmazására. E hipotézis igazolására **meghatároztam a kétlépcsős gyakorlati képzés működési környezetét. Azonosítottam a gyakorlati képzés alapját képező szimulációs környezetet leíró keretrendszert, valamint definiáltam egy automatizált értékelési rendszert**, amely alkalmas a gyakorlati képzési rész során átadott tudásanyag számonkérésére. A szimulációs környezetet leíró keretrendszer szükségességét jelzi, hogy segítségével a közszolgálatban dolgozó személyeket fel lehet készíteni a kibertámadások észlelésére és esetleges bekövetkezése esetén azok következményeinek elhárítására, mérséklésére. A keretrendszer gyakorlati tapasztalatokra épül, amely egyéni és csoportos tanulási környezetet biztosít a hatékony és eredményes kibervédelmi technikák elsajátítására.

A keretrendszer segítségével előre definiált specifikációk alapján automatizmusok útján hajtható végre a kibertámadások szimulálása és az azokkal szemben alkalmazható védelmi mechanizmusok gyakorlati alkalmazása.

6.1. ÚJ TUDOMÁNYOS EREDMÉNYEK

E1. Definiáltam egy nyolc elemből álló folyamatmodellt, amely meghatározza a tudományos alapokon nyugvó felsőoktatási képzések tervezésének lépéseit és a kapcsolódó kutatási módszereket.

E2. Azonosítottam a közszolgálati kiberbiztonsági képzés célcsoportját és az általuk elsajátítandó tudáshalmaz-, képesség- és készséghalmazt.

E3. Bebizonyítottam, hogy szükséges egy olyan eddig még nem létező képzési program megalkotása a hazai képzési környezetben, amely lehetőséget nyújt a közszolgálatban dolgozó, nem informatikai végzettségű személyek kibervédelmi képességének kialakítására, amely nemzetközi szinten is releváns.

E4. Definiáltam az informatikai előképzettséget nem igénylő közszolgálati kiberbiztonsági képzés struktúráját, képzési programját, egyes komponenseit, valamint általános értékelési rendszerét.

E5. Definiáltam egy olyan műszaki keretrendszert, amely lehetőséget biztosít kibertámadások elleni védelmi stratégiák gyakorlatban történő alkalmazására.

6.2. AJÁNLÁSOK ÉS GYAKORLATI FELHASZNÁLATÓSÁG

Kutatásom során részletesen definiáltam egy, a közszolgálati kiberbiztonság fejlesztését célzó képzési programot, amely lehetőséget biztosít a nem informatikai előképzettséggel rendelkező, közszolgálatban dolgozó szakemberek releváns kibervédelmi képességeinek elsajátítására. Ebből következik, hogy értekezésem gyakorlati felhasználását ajánlom:

a) a közszolgálati képzési rendszer fejlesztéséért felelős szakemberek számára, a közszolgálati kiberbiztonsági képzés vagy annak egyes elemeinek implementálása érdekében;

b) a közszolgálatban dolgozó szakemberek számára az elsajátítandó ismerethalmaz alapján képességeik fejlesztése, ismereteik bővítése céljából;
c) közszolgálati szervezetek vezetőinek a szervezet foglalkoztatottjainak kibervédelmi felkészítése érdekében;
d) felsőoktatási intézmények részére a kapcsolódó felsőoktatási képzések felülvizsgálatának, kialakításának tervezésekor a jelen értekezésben bemutatott képzési program elemeinek implementálásához;
e) az Önkéntes Tartalékos Rendszer döntéshozóinak az önkéntes tartalékos állomány kibervédelmi képességeinek fejlesztését szóló képzés kialakításában.

6.3. JÖVŐBELI TERVEK

Annak érdekében, hogy a kutatásomban elért eredmények gyakorlatban történő alkalmazása, hasznosíthatósága hosszútávon biztosítható legyen, célszerű meghatározni jelen értekezésben bemutatott kutatásom lehetséges folytatásának lehetőségeit.

A kutatás egyik legfőbb célja egy olyan gyakorlati képzés kialakítása volt, amely a közszolgálatban dolgozó személyek kibervédelmi képességeinek kialakítását és fejlesztését célozza. Ahhoz, hogy e képzési program gyakorlati felhasználása eredményesen megvalósulhasson, továbbá nemzetközi szinten is megfelelő értéket képviseljen elengedhetetlen a kutatás továbbfejlesztése. Ennek legfőbb alkotóelemét képezi egy olyan **közös platform, illetve fórum létrehozása, amely lehetőséget biztosít a kiberbiztonsági képzéseket szolgáltató hazai és nemzetközi egyetemek számára, hogy megoszthassák tapasztalataikat és alkalmazott „jó gyakorlataikat**”. A tudás- és tapasztalatmegosztás célja a kapcsolódó képzések folyamatos fejlesztése, a hiányosságok feltárása, valamint a releváns „jó gyakorlatok” saját képzésbe történő adaptálása. E platform segítségével az egyetemek a tudásátadás hatékonyságának mérésére szolgáló módszer alkalmazásával, valamint folyamatos vizsgálatok lefolytatásával, elemzések elkészítésével feltárhatják hogyan fejleszthető a saját képzésük, továbbá milyen módosításokat, változtatásokat szükséges eszközölni a képzés minőségének javítása érdekében.

PUBLIKÁCIÓK

publikációk száma	**13**
lektorált idegen nyelvű publikációk száma	2
lektorált folyóiratban megjelent közlemények száma	11

PUBLIKÁCIÓK ÉS TÉZISEK KAPCSOLATA

Tudományos eredmény	Könyvfejezet	Idegen és magyar nyelvű folyóiratcikk	
1. tézis	[k2],		
2. tézis		[j2]	[f3]
3. tézis			[f2], [f3]
4. tézis		[j1]	[f1], [f3]
5. tézis		[j1]	[f6], [f7]

MAGYAR NYELVŰ KÖNYVFEJEZET

[k1] Angyal I, Arató Gy, Bakos B, Baranya Zs, Bocsok V, Bogáncs T, Bonnyai T, Buttyán L, Csatár J, Danyek M, **Deák Veronika**, Görgey P, Gyebnár G, Illés G, Krasznay Cs, Molnár F, Pongrácz P, Szabó-Nyakas Zs, Szádeczky T, Szent-Királyi B, Winter G: Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyve – www.seconsys.eu (2021).

[k2] **Deák Veronika**: *A közszolgálati kiberbiztonsági képzés tervezése tudományos alapokon* – Földi László (szerk): Szemelvények a katonai műszaki tudományok eredményeiből II., Ludovika Egyetemi Kiadó, 2020. Budapest

[k3] **Deák Veronika**, Dévai Dóra, Krasznay Csaba, Ambrus Éva, Haig Zsolt, Koczka Ferenc, Koller Marco, Kovács László, Legárd Ildikó, Molnár Anna Éva, Molnár Dóra, Nyári Gábor, Üveges András: Taktikák és stratégiák a kiberhadviselésben (Megjelenés alatt: Ludovika Egyetemi Kiadó)

LEKTORÁLT NEMZETKÖZI IDEGEN NYELVŰ FOLYÓIRATCIKKEK

[j1] **Deák Veronika**: *Simulation Framework for Practical Cyber Security Training in the Public Service* – Security and Defense Quarterly: Non-military aspects of security in the changing international order, 33. évfolyam, 1. szám (2021), 87-104.

LEKTORÁLT HAZAI IDEGEN NYELVŰ FOLYÓIRATCIKKEK

[j2] **Deák Veronika**: *Finding differences on cyber security between public and private sectors* – National Security Review, 1. szám (2021), 169-180.

LEKTORÁLT MAGYAR NYELVŰ FOLYÓIRATCIKKEK

[f1] Krasznay Csaba, **Deák Veronika**: *Adatbiztonsági informatikai alapismeretek átadásának vizsgálata egy szakirányú továbbképzés keretében* – Hadmérnök, XVI. évfolyam 4. szám (2021), 112-132

[f2] **Deák Veronika**: *A közszolgálati kiberbiztonsági képzés helye nemzetközi viszonylatban* – Hadmérnök, XV. évfolyam 4. szám (2020), 157-178

[f3] **Deák Veronika**: *A közszolgálati kiberbiztonsági képzés lehetősége Magyarországon* – Hadmérnök, XV. évfolyam 3. szám (2020), 157-178.

[f4] **Deák Veronika**: *A nyílt forrású információszerzés szerepe a kibertámadások végrehajtása során* – Hadmérnök, XIII. évfolyam 3. szám (2018), 391-402

[f5] **Deák Veronika**: *Biztonságtudatosság az információs környezetben* – Szakmai Szemle, XV. évfolyam, 3. szám, 2017. november, 59-77.

[f6] **Deák Veronika**: *Kártékony programok terjedése social engineering technikákon keresztül* – Hadmérnök, XIV. Évfolyam 2. szám (2019), 256-271

[f7] **Deák Veronika**: *Prototípus implementáció kibervédelmi technikák gyakorlati oktatására* – (Elbírálás alatt)

[f8] **Deák Veronika**: *Social engineering alapú információszerzés a kibertérben megvalósuló lélektani műveletek során* – Hadmérnök, XIV. Évfolyam 12. szám (2019), 95-111

HIVATKOZÁSOK

IRODALOMJEGYZÉK

[1] (ISC)², „Cybersecurity Workforce Study," 2021. [Online]. Available: https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx.

[2] H. Júlia, A tudományos kutatás elmélete és módszertana, Budapest: Nemzeti Közszolgálati Egyetem, 2014.

[3] G. István, Tudományelmélet és kutatásmódszertan alapjai, Budapest: ZMNE, 2010.

[4] C. Williams, „Research methods," *Journal of Business & Economics Research,* 5. kötet, 3. szám, pp. 65-72, 2007.

[5] E. Babbie, A társadalomtudományi kutatás gyakorlata, Budapest: Balassi Kiadó, 2008.

[6] W. Newhouse, S. Keith, B. Scribner és G. Witte, „National initiative for cybersecurity education (NICE) cybersecurity workforce framework," *NIST special publication,* 800. kötet, 2017. szám, pp. 1-181, 2017.

[7] ENISA, European Cybersecurity Skills Framework (ECSF), Draft v0.5, 2022.

[8] P. S. Dapzury Valenzuela, Szerző, *Interview as a Method for Qualitative Research.* [Performance]. Southern Cross University and the Southern Cross Institute of Action Research (SCIAR), 2002.

[9] B. F. C. Barbara DiCicco-Bloom, „The qualitative research interview," *Medical Education,* 40. kötet, 4. szám, p. 314–321, 2006.

[10] B. R. Rowe és M. P. Gallaher., „Private sector cyber security investment strategies: An empirical analysis.," in *Workshop on the Economics of Information Security (WEIS),* England, 2006.

[11] M. T. Siponen, „A conceptual foundation for organizational information security awareness," *Information Management & Computer Security,* 8. kötet, pp. 31-41, 2000.

[12] L. A. Gordon, M. P. Loeb, W. Lucyshyn és L. Zhou, „Increasing cybersecurity investments in private sector firms," *Journal of Cybersecurity,* 1. kötet, 1. szám, pp. 3-17, 2015.

[13] B. W. Wirtz és J. C. Weyerer, „Cyberterrorism and cyber attacks in the public sector: how public administration copes with digital threats.," *International Journal of Public Administration,* 40. kötet, 13. szám, pp. 1085-1100, 2017.

[14] P. Cooke, „Digital tech'and the public sector: what new role after public funding?," *European Planning Studies,* 25. kötet, 5. szám, pp. 739-754, 2017.

[15] C. Luigi, S. D'Antonio, G. Mazzeo, L. Romano és L. Sgaglione, „How to Protect Public Administration from Cybersecurity Threats: The COMPACT Project.," *32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA),* pp. 573-578, 2018.

[16] K. J. Andreasson, Cybersecurity: public sector threats and responses, Boca Raton: CRC press, 2011.

[17] I. Alsmadi, „Cybersecurity Education Based on the NICE Framework: Issues and Challenges," *ISACA Journal,* 3. kötet, pp. 1-6, 2018.

[18] M. E. Armstrong, K. S. Jones és A. S. Namin, „Framework for Developing a Brief Interview to Understand Cyber Defense Work: An Experience Report," *Proceedings of the Human Factors and Ergonomics Society 2017 Annual Meeting,* 61. kötet, 1. szám, pp. 1318-1322, 2017.

[19] A. C. Estes, D. J. Kim és T. A. Yang, „Exploring How the NICE Cybersecurity Workforce Framework Aligns Cybersecurity Jobs with Potential Candidates," in *The 14th International Conference on Frontiers in Education: Computer Science and Computer Engineering (FECS'18),* Las Vegas, USA, 2018.

[20] V. P. P. Ernest L. McDuffie, „The Future of Cybersecurity Education," *Computer,* 47. kötet, 8. szám, pp. 67-69, 2014.

[21] A. Zsolt, „A közszolgálati kommunikáció eredményességére ható tényezők – A közszféra és a versenyszféra kommunikációs gyakorlatát befolyásoló különbségek,” *Vezetéstudomány,* 49. kötet, 4. szám, pp. 68-76, 2018.

[22] H. Zoltán, Közszolgálati jogunk a változó nemzetközi és hazai térben, PhD-értekezés: PTE, 2009.

[23] K. Csaba, „A kiberbiztonság stratégiai vetületeinek oktatási kérdései a közszolgálatban,” *Nemzet és Biztonság: Biztonságpolitikai szemle,* 10. kötet, 3. szám, pp. 38-53, 2017.

[24] N. T. Veronika és K. László, „Az információbiztonsági vezető szakirányú továbbképzés tapasztalatai,” *Pro Publico Bono – Magyar Közigazgatás,* 3. kötet, 4. szám, pp. 86-99, 2015.

[25] S. Zoltán, „Az információbiztonság fejlesztési lehetőségei az EIV képzésen keresztül,” *Társadalom és Honvédelem,* 20. kötet, 2. szám, pp. 167-175, 2016.

[26] S. Béla, „Kiberbűnözés elleni képzésfejlesztés,” *Magyar Rendészet,* 18. kötet, 3. szám, pp. 193-207, 2018.

[27] C. Krzysztof, D. Domingos, Z. Kotulski és A. Respício, „Cybersecurity education: Evolution of the discipline and analysis of master programs,” *Computers & Security,* 75. kötet, p. 24–35, 2018.

[28] B. Bystrova, „Comparison of the educational cybersecurity programs of the United States and Ukraine universities,” *Comparative professional pedagogy,* 7. kötet, 4. szám, pp. 114-119, 2017.

[29] S. Pratt és C. Adams, „How to create a degree course in radiography: a recipe,” *Radiography,* 9. kötet, 4. szám, pp. 317-322, 2003.

[30] P. Wang, „Designing a doctoral level cybersecurity course,” *Issues in Information Systems,* 19. kötet, 1. szám, pp. 192-202, 2018.

[31] R. Sabillon, J. Serra-Ruiz és V. Cavaller, „An effective cybersecurity training model to support an organizational awareness program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada.,” in

Research Anthology on Artificial Intelligence Applications in Security, USA, IGI Global, 2021, pp. 174-188.

[32] R. Beuran, D. Tang, C. Pham, K.-i. Chinen, Y. Tan és Y. Shinoda, „Integrated framework for hands-on cybersecurity training: CyTrONE," *Computers & Security,* 78. kötet, pp. 43-59, 2018.

[33] M. J. Dupuis, „Cyber Security for Everyone: An Introductory Course for Non-Technical Majors," *Journal of Cybersecurity Education, Research and Practice,* 2017. kötet, 1. szám, pp. 1-17, 2017.

[34] P. K. Patricia Toth, „A role-based model for federal information technology/cyber security training," *NIST special publication,* 800. kötet, 16. szám, pp. 1-152, 2013.

[35] Országgyűlés hivatala, „Kiberfenyegetések és kibervédelem," *infojegyzet,* 44. kötet, pp. 1-4, 2016.

[36] K. Csaba, A magyar elektronikus közigazgatási alkalmazások információbiztonsági megoldásai, Doktori (PhD) értekezés, 2011.

[37] K. Geers, Cyber war in perspective: Russian aggression against Ukraine, Tallin: EVG Print, 2022.

[38] W. A. Conklin, R. E. Cline és T. Roosa, „Re-engineering cybersecurity education in the US: an analysis of the critical factors," in *IEEE,* 2014 47th Hawaii international conference on system sciences, 2014.

[39] L. Topham, K. Kifayat, Y. A. Younis, Q. Shi és B. Askwith, „Cyber security teaching and learning laboratories: A survey," *Information & Security,* 35. kötet, 1. szám, p. 51, 2016.

[40] C. Willems és C. Meinel, „Online assessment for hands-on cyber security training in a virtual lab," in *IEEE,* Proceedings of the 2012 IEEE Global Engineering Education Conference (EDUCON), 2012.

[41] G. J. Cartwright, „Memorandum for Chiefs of the Military Servs., Commanders of the Combatant Commands, Dirs. of the Joint Staff Directories on Joint

Terminology for Cyberspace Operations 5," *Depatment of Defense, Washington DC,* 2011.

[42] O. Hathaway, R. Crootof, P. Levitz, H. Nix, A. Nowlan, W. Perdue és J. Spiegel, „The law of cyber-attack," *California Law Review,* 100. kötet, 4. szám, p. 817–885, 2012.

[43] W. Owens, K. Dam és H. Lin, Technology, policy, law, and ethics regarding US acquisition and use of cyberattack capabilities, National Academies Press, 2009.

[44] M. Uma és G. Padmavathi, „A Survey on Various Cyber Attacks and their Classification.," *International Journal of Network Security,* 15. kötet, 5. szám, p. 390–396, 2013.

[45] K. Fehér, Kezdő hackerek kézikönyve, Budapest: BBS-INFO Könyvkiadó és Informatikai Kft., 2016.

[46] S. Gányi, „DDOS támadások veszélyei és az ellenük való védekezés," *Hadmérnök,* Különszám. kötet, 2007.

[47] L. Muha és C. Krasznay, Az elektronikus információs rendszerek biztonságának menedzselése, Budapest: Nemzeti Közszolgálati Egyetem, 2018, p. 51.

[48] C.-C. Kuo, K. Chain és C.-S. Yang, „Cyber attack and defense training: Using EMULAB as a platform," *International Journal of Innovative Computing, Information and Control,* 14. kötet, p. 2245–2258, 2018.

[49] M. Ficco és F. Palmieri, „Leaf: An open-source cybersecurity training platform for realistic edge-IoT scenarios," *Journal of Systems Architecture,* 97. kötet, p. 107–129, 2019.

[50] J. Hong, R. Nuqui, D. Ishchenko, Z. Wang, T. Cui, A. Kondabathini, D. Coats és S. Kunsman, „Cyber-physical security test bed: A platform for enabling collaborative cyber defense methods," in *PACWorld Americas Conference*, Glasgow: PACWorld Americas Conference, 2015.

[51] P. Čeleda, J. Čegan, J. Vykopal és D. Tovarňák, „Kypo–a platform for cyber defence exercises," *M&S Support to Operational Tasks Including War Gaming, Logistics, Cyber Defence. NATO Science and Technology Organization*, 2015.

[52] W. Schepens és J. James, „Architecture of a cyber defense competition," Washington: 2003 IEEE International Conference on Systems, Man and Cybernetics, 2003.

[53] A. Szabó, „Technikai kiberbiztonsági gyakorlatok–Nemzetközi kitekintés," *Hadmérnök,* 13. kötet, 1. szám, pp. 286-301, 2018.

[54] D. Kennedy, J. O'gorman, D. Kearns és M. Aharoni, Metasploit: the penetration tester's guide, San Francisco: No Starch Press, 2011.

[55] K. Heckman, M. Walsh, F. Stech, T. O'boyle, S. DiCato és A. Herber, „Active cyber defense with denial and deception: A cyber-wargame experiment," *Computers & Security,* 37. kötet, p. 72–77, 2013.

[56] M. Herring és K. Willett, „Active cyber defense: a vision for real-time cyber defense," *Journal of Information Warfare,* 13. kötet, 2. szám, p. 46–55, 2014.

[57] G. Jin, M. Tu, T.-H. Kim, J. Heffron és J. White, „Game based cybersecurity training for high school students," Baltimore: 49th ACM Technical Symposium on Computer Science Education, 2018.

[58] S. Hart, A. Margheri, F. Paci és V. Sassone, „Riskio: A serious game for cyber security awareness and education," *Computers & Security,* 95. kötet, 2020.

INTERNETES FORRÁSOK

[w1] Arizona State University – Cybersecurity policy and management (MA). https://asuonline.asu.edu/online-degree-programs/graduate/cybersecurity-policy-and-management-ma/

[w2] Australian National University – Master of Public Administration. https://programsandcourses.anu.edu.au/program/MPUAD

[w3] California State University, San Bernardino – Master of Public Administration. https://jhbc.csusb.edu/mpa)

[w4] Carnegie Mellon University – Information Security Policy & Management (MSISPM). https://www.heinz.cmu.edu/programs/information-security-policy-management-master/

[w5] Eindhoven University of Technology – Mastertrack Information Security Technology. https://www.tue.nl/en/education/graduate-school/mastertrack-information-security-technology/

[w6] ELTE: Adatbiztonsági és adatvédelmi szakjogász szakleírás, https://jotoki.elte.hu/content/adatbiztonsagi-es-adatvedelmi-szakjogasz.t.406.
[w7] Felvi.hu minden, ami felsőoktatás nevű portál. https://www.felvi.hu/
[w8] Felvi.hu szakleírások: Nemzeti Közszolgálati Egyetem - Bűnügyi alapképzési szak - Kiber nyomozó szakirány, https://www.felvi.hu/felveteli/egyetemek_foiskolak/!IntezmenyiOldalak/meghirdetes.php?meg_id=20905&elj=20a.
[w9] Felvi.hu szakleírások: Nemzeti Közszolgálati Egyetem – Kiberbiztonsági mesterképzés, https://www.felvi.hu/felveteli/szakok_kepzesek/szakleirasok/!Szakleirasok/index.php/szak/20554/szakleiras.
[w10] Felvi.hu szakleírások: Óbudai Egyetem – Biztonságtechnikai mérnök alapképzési szak – Információbiztonsági specializáció, https://www.felvi.hu/felveteli/szakok_kepzesek/szakleirasok/!Szakleirasok/index.php/szak/36/szakleiras.
[w11] Gábor Dénes Főiskola: Adatvédelmi és információbiztonsági menedzser szakirányú továbbképzés tartalma, http://gdf.hu/szakiranyu-tovabbkepzesek/adatvedelmi-es-informaciobiztonsagi-menedzser/
[w12] Harvard University: Master in Public Administration. https://www.hks.harvard.edu/educational-programs/masters-programs/master-public-administration
[w13] London School of Economics and Political Science: Executive Master of Public Administration (EMPA) http://www.lse.ac.uk/school-of-public-policy/empa
[w14] M. Varga, „Számítógépes virtualizáció," 2010, https://docplayer.hu/2946347-Szamitogepes-virtualizacio.html
[w15] Nemzeti Közszolgálati Egyetem: Elektronikus információbiztonsági vezető szakleírás, https://kti.uni-nke.hu/szakiranyu-tovabbkepzesek/szakiranyu-tovabbkepzesi-szakok/elektronikus-informaciobiztonsagi-vezeto/altalanos-informaciok.
[w16] Nemzeti Közszolgálati Egyetem: Európai uniós adatvédelmi szaktanácsadó szakleírás, https://kti.uni-nke.hu/szakiranyu-tovabbkepzesek/szakiranyu-tovabbkepzesi-szakok/europai-unios-adatvedelmi-szaktanacsado/altalanos-informaciok
[w17] Nemzeti Közszolgálati Egyetem: Védelmi infokommunikációs rendszertervező – Információbiztonsági szakirány szakleírás, tematika, https://hhk.uni-nke.hu/oktatas/mesterkepzes/vedelmi-vezetestechnikai-rendszertervezo.
[w18] Óbudai Egyetem: Információbiztonsági szakmérnök/szakember képzés tartalma, http://www.bgk.uni-obuda.hu/hu/kepzeseink/tovabbkepzesek/informaciobiztonsagi-szakmernokszakember.
[w19] Óbudai Egyetem: Kiberbiztonsági szakmérnök/szakember képzés tartalma, http://bmi.nik.uni-obuda.hu/kiber_kovetelmeny.
[w20] OWASP – WebGoat Project. https://owasp.org/www-project-webgoat/
[w21] TopUniversities weboldal. https://www.topuniversities.com/
[w22] TryHackMe, https://tryhackme.com

[w23] University College of London: Information Security MSc. https://www.ucl.ac.uk/prospective-students/graduate/taught-degrees/information-security-msc
[w24] University of Washington: Master of Science in Cybersecurity Engineering. https://www.uwb.edu/cybersecurity
[w25] VulnHub, https://vulnhub.com
[w26] Warsaw Summit Communiqué, www.nato.int/cps/en/natohq/official_texts_133169.htm
[w27] Nemzeti Közszolgálati Egyetem: Védelmi infokommunikációs rendszertervező mesterképzés https://hhk.uni-nke.hu/oktatas/mesterkepzes/vedelmi-infokommunikacios-rendszertervezo

JOGSZABÁLYOK

[Alaptörvény, XXXI. cikk] Magyarország Alaptörvénye, XXXI. cikk
[2011. évi CCIV. törvény] 2011. évi CCIV. törvény a nemzeti felsőoktatásról
[2011. évi CXIII. törvény 26. § (1)] A honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény, 26. § (1) bekezdése
[2011. évi CXIII. törvény 36. § (2)] A honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény, 36. § (2) bekezdése
[2011. évi CXIII. törvény 40. § (1)] A honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény, 40. § (1) bekezdése
[2011. évi CXIII. törvény 40. § (2)] A honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény, 40. § (2) bekezdése
[2011. évi CXIII. törvény 40. § (5)] A honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény, 40. § (5) bekezdése
[2011. évi CXIII. törvény 62/A. § (1)] A honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény, 62/A. § (1) bekezdése

[2011. évi CXIII. törvény] 2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről

[2013. évi L. törvény] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

[2021. évi CXL. törvény 71. § (3)] A honvédelemről és a Magyar Honvédségről szóló 2021. évi CXL. törvény 71. § (3) bekezdése

[2021. évi CXL. törvény 71. §] A honvédelemről és a Magyar Honvédségről szóló 2021. évi CXL. törvény 71. §

[3/2022. HM utasítás] 3/2022. (I. 27.) HM utasítás honvédelmi szervezet 2022. évi kiemelt feladatainak, valamint a 2023-2024. évi fő célkitűzéseinek meghatározásáról

[32/2021. HM utasítás 1. §] A Magyar Honvédség Kiber- és Információs Műveleti Központ kialakításával összefüggő egyes feladatokról szóló 32/2021. (VII. 23.) HM utasítás 1. §

[32/2021. HM utasítás] 32/2021. (VII. 23.) HM utasítás a Magyar Honvédség Kiber- és Információs Műveleti Központ kialakításával összefüggő egyes feladatokról

[60/2013. HM utasítás (7)] A Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról szóló 60/2013. (IX. 30.) HM utasítás 7. pontja

[60/2013. HM utasítás] 60/2013. (IX. 30.) HM utasítás A Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról

[87/2015 Korm. rendelet] 87/2015. (IV. 9.) Korm. rendelet a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény egyes rendelkezéseinek végrehajtásáról

[1393/2021 Korm. hat.] A Kormány 1393/2021. (VI. 24.) Korm. határozata Magyarország Nemzeti Katonai Stratégiájáról

ÁBRAJEGYZÉK

TÁBLÁZATJEGYZÉK

FÜGGELÉK

F1. INTERJÚ

Deák Veronika (DV)*: *Szembesültek-e már kiberbiztonsági incidenssel? Megelőzni sikerült-e vagy reagálni a már bekövetkezett eseményekre? Sérült-e az adatok CIA-ja?

Otti Csaba (OCS): Igen, szembesültünk már kiberbiztonsági incidenssel. Ilyen eseménynek tekinthető, hogy például a Production szerver, amelyen az általunk nyújtott cloud szolgáltatás fut, nem volt elérhető, illetve az általunk elvégzett sérülékenységvizsgálatok eredményei kapcsán talált problémákat folyamatosan javítjuk, ezzel segítve a jövőbeni események megelőzését, illetve a már bekövetkezett eseményekre történő hatékony reagálást. A bizalmasság és sértetlenség elve nem, azonban a szerver elérhetetlenségének köszönhetően a rendelkezésre állás elve sérült.

Muha Lajos (ML): Szembesültünk már kiberbiztonsági incidenssel. Nem tudjuk naplózni azokat a lehetséges kiberbiztonsági incidenseket, amelyek az intézkedések segítségével sikerült megelőzni, de szembesültünk olyannal, amely, mint incidens megtörtént, azonban az esetek döntő többségében sikerült ezeket korai szakaszban hatékonyan kezelni. Súlyos eredményekkel járó incidenst – szerencsére – nem tapasztaltunk. Előfordult például adathalász támadás, illetve rosszindulatú kódok továbbítása e-mail-ek csatolmányaként. Ezen esetekben a CIA alapelvek érdemi sérülése nem következett be.

DV: *Milyen főbb informatikai infrastrukturális komponensei vannak a szervezetnek?*

OCS: A szervezetnek van egy telephelye, ahol a belső adatok és a munkát végző személyek eszközei külön hálózaton találhatóak. A belső hálózatban találhatóak adatbázis szerverek, alkalmazás szerverek, belső adattárolók, illetve a tűzfal, amin keresztül az Internet elérhető. A munkavégzéshez használt hálózaton nyomtatók, szkenner, mobil eszközök és fejlesztői számítógépek találhatóak, amik a belső hálózaton keresztül kapcsolódnak az Internetre. A szervezet kapcsolatban áll egy cloud szolgáltatóval is, mely a céghez kapcsolódó felhő alapú szolgáltatásokat hostolja. A távoli munkavégzés során VPN-en keresztül csatlakozhatnak a belső hálózathoz az alkalmazottak. Az ügyfelek viszont csak a cloud szolgáltatáson keresztül kommunikálnak a szervezet eszközeivel.

ML: Komplett infrastruktúrával rendelkezünk a tűzfalaktól kezdve szervereken keresztül a különböző munkaállomásokig. Alapvetően a Nemzeti Távközlési Gerinchálózat (NTG) biztosítja az Internetre történő kijárást, valamint az egyes telephelyek közötti összeköttetést. Speciális esetekben a szervert, az operációs rendszert, az adatbázist is a NISZ üzemelteti és csak az alkalmazásüzemeltetés valósul meg szervezetünk által.

DV: *Milyen kibertámadási felületek vannak a szervezetnél?*

OCS: A Cloud infrastruktúránkon a sérülékenységvizsgálat által feltárt sérülékenységek, valamint a kollégákon keresztüli adathalászat, mint például a különféle adathalász üzenetek, rosszindulatú kódra történő rákattintás kiemelt kockázatot jelenthetnek szervezetünkben. Ezen kívül szükséges megemlíteni az adatszivárgást, amikor például egy kolléga letölt egy ügyféltől érkező Excel táblázatot és nem úgy kezeli az ügyféladatokat, ahogy azt a szabályzataink rögzítik.

ML: Korábban adathalász levél és a kártékony program e-mail mellékletként történő csatolása fordult elő. Célzott támadásokat nem észleltünk, azonban sérülékenységvizsgálatok segítségével folyamatosan monitorozzuk a releváns területeket.

DV: *Milyen védekezési stratégiát alkalmaznak?*

OCS: Az adminisztratív védelem keretében kiemelt figyelmet fordítunk a kollégák biztonságtudatosságának növelésére, így például a különféle tudatossági képzésekre, oktatásokra és programokra. Ezen kívül kialakítottuk a politikák és szabályzatok rendszerét, melynek betartását folyamatosan ellenőrizzük, illetve szükség esetén módosítjuk. A fizikai védelem megvalósítására számos intézkedést foganatosítottunk, így például fizikai beléptetésre, az irodák, helyiségek és létesítmények védelmére vagy akár a berendezések védelmére vonatkozó intézkedéseket. A logikai védelem keretében különös jelentőségűek többek között a rosszindulatú szoftverek elleni védelem, operatív szoftverek kontrollja, naplózás és monitorozás, biztonsági mentések, illetve a hozzáférés-vezérlés.

ML: Szervezetünknél részletes szabályozás vonatkozik minden olyan területre, amely a biztonsággal összefügg. Komplex és minden részletre kiterjedő informatikai biztonsági szabályzattal rendelkezünk. Éves szinten kötelező az informatikai biztonsági oktatás és vizsga minden munkavállaló számára. A fizikai védelem

megvalósulását számtalan intézkedés és eszköz biztosítja, például zárt objektumok, elektronikus beléptető rendszer, élőerős és mechanikai védelem, kamerarendszerek. A logikai védelem területén törekszünk a zárt és teljeskörű védelem megvalósítására, a tűzfalaktól a rosszindulatú szoftverek elleni védelmen keresztül a hozzáférés-ellenőrzésig.

DV: Milyen kiberbiztonsággal kapcsolatos képzéseket tartanak az alkalmazottak számára?

OCS: Minden új belépő munkavállaló számára egy általános képzést biztosítunk, majd ezt követően folyamatosan, a felmerülő biztonsági kérdésekhez igazodva további képzéseket tartunk, valamint a képzési rendszer harmadik elemeként munkavállalóink meghatározott időközönként rendszeres oktatásokon vesznek részt.

ML: Kötelező e-learning-es képzést biztosítunk a szervezet minden munkavállalója számára, amelyet minden évben felülvizsgálunk és szükség esetén módosítjuk. Jelenleg éppen az adatvédelmi ismeretekkel (GDPR) kombinált informatikai biztonsági képzés kialakítása zajlik, amely segítségével a szükséges adatvédelmi és informatikai biztonsági ismeretek egy képzés keretében sajátíthatók el.

DV: *Melyiket látja hatékonyabbnak a technológiai védelmet vagy a személyek képességeinek fejlesztését? Miért?*

OCS: Mindkettő rendkívül fontos és szükséges. Amennyiben az emberek nem értik és nem képesek egyetérteni azzal, hogy szükség van a korlátozó intézkedésekre, akkor nem fogják, illetve tudják betartani a technológiai védelem eszközeit. Ez utóbbiak előnye pedig, hogy a nap 24 órájában folyamatosan működnek és biztosítják számunkra a biztonságos működést.

ML: Mindkettő egyformán szükséges. A személyek képességeit azért kell fejleszteni, mert jól képzett személyzet nélkül nem működik a technológia. A technológiára is szükség van, hogy kiegészítse a személyi képességeket. Nem helyettesíthetik, hanem kiegészítik egymást, a kettő együtt biztosítja a hatékony védelmet.

DV: *Financiális szempontból melyiket tartják gazdaságosabbnak, a technológiai védelmet vagy a személyek képességeinek fejlesztését?*

OCS: A személyek képességeinek képzése során nem csak magának a képzésnek a megtartása a költség, hanem annak az ideje, ameddig nem dolgoznak az adott cégben,

ami akár jelentős bevétel kiesést is jelenthet. Azonban technológia szinten is elkölthető hasonló mennyiségű összeg. A fő feladat a kockázatok azonosítása és a kockázatok arányában költeni a képzésekre és a technológiákra. Túlbiztosítani egyik oldalt sem szükséges.

ML: Pénzügyi, gazdaságossági szempontból a személyek képzése költséghatékonyabbnak tekinthető, tulajdonképpen relatíve kis költséggel kiképzett személyzet hatékony védelemre képes. Azonban a személyes képesség megléte nem képes kiváltani a technológiai védelem eszközeit (pl. tűzfal, vírusírtó). A megfelelően képzett személyzet segítségével valamelyest csökkenthetők a költségek, de egyik sem válthatja ki a másik tényezőt.

DV: *Milyen kibervédelmi képességek szükségesek a munkavállalók mindennapi feladatainak ellátáshoz?*

OCS: A korábban említett biztonságtudatosság nélkülözhetetlen a mindennapi feladatok ellátása során, ennek keretében, hogy a munkavállalók ismerjék a kockázatokat, a következményeket, illetve a szabályzatokat. Ezen túlmenően kulcsfontosságú, hogy az ismeretek megszerzését követően megértsék és egyet is értsenek a különféle védelmi eszközökkel, intézkedésekkel, hiszen azok eredményes és hatékony gyakorlati alkalmazása csak így valósítható meg.

ML: A munkavállalóknál rendkívül fontos a minden részletre kiterjedő figyelem készsége, például ide sorolható amennyiben beérkezik egy gyanús üzenet, amely esetben a munkavállalónak figyelnie és döntenie kell arra vonatkozóan, hogyan reagál erre a helyzetre, rákattint-e a csatolmányra, válaszol-e az e-mailre, kell-e értesíteni valakit a gyanúsnak tűnő üzenetről, illetve van-e bármilyen teendője az üzenettel kapcsolatban.

DV: *Lát-e különbséget a közszolgálat és a magánszféra kiberbiztonsági kockázatait illetően?*

OCS: A szervezetek típusától és profiljától függően eltérő kockázatok jellemzőek, ennek következtében pedig eltérő intézkedések szükségesek. Kritikus infrastruktúra esetében, így például egy energia- vagy vízhálózat megtámadása egészen más nagyságrendű problémákat okozhat, így egészen más nagyságrendű intézkedéseket is igényelnek. A súlyossági és az érintetti tényező eltérő lehet a közszférában, ennek

következtében a kockázatok és az ezek reagálására foganatosított intézkedések is különbözhetnek.

ML: Megfigyelhető valamilyen különbség, azonban a magán- és a közszféra szoros kapcsolatban áll egymással, átfedések figyelhető meg ezen területek között. A különbséget abban látom elsődlegesen, hogy az adott szervezet feladatai mennyire tekinthetők létfontosságúnak a nemzet szempontjából.

F2. GYAKORLATI ÉS VIZSGAKÉRDÉSEK

Adathalászat Gyakorlat

A teszt általános leírása

Az adathalászat (*phishing*) lényege abban rejlik, hogy az adathalászok a felhasználókat valamilyen elektronikus csatornán keresztül, - például e-mailben, azonnali üzenetben vagy éppen szalagcím hirdetésekben - egy látszólag teljesen eredeti, valójában pedig egy hamis weboldalra irányítják, ahol arra kérik, hogy adják meg bizalmas adataikat. Az adathalászatnak számos válfaja van aszerint, hogy milyen módon, milyen elektronikus csatornán keresztül invitálják a felhasználót a hamis weboldalra.

Előkészítés

A teszt elkezdéséhez indítsa el az alábbi virtuális gépeket a VirtualBox alkalmazás segítségével és válassza ki az alattuk található "Phishing" nevű pillanatfelvételt a meghatározott sorrendben:

1. Áldozat (Ubuntu Phishing)
2. Támadó (Kali Phishing)

Végül lépjen be az Áldozathoz kapcsolódó virtuális gép felületére.

Ubuntu és Chromium

Ez a gyakorlat az Ubuntu (Linux alapú) operációs rendszeren zajlik. A támadás során az operációs rendszer kisegítő szerepet tölt be, ezért hasznos lehet megismerkedni a Windows-on kívül más operációs rendszerekkel is, hiszen a Linux/Unix alapú rendszereket rendkívül sok helyen használják (pl.: az Android és a Mac is erre épül).

A Windows operációs rendszerben már jól ismert *Google Chrome* alkalmazás megfelelője Ubuntun a *Chromium*, amely funkcionalitása szempontjából teljes mértékben megegyezik Windows-os párjával.

Kérem, hogy nyissa meg a *Chromium* alkalmazást (a bal oldali kedvencek menü legfelső eleme). Sikerült elindítani?

☒ Igaz ☐ Hamis

Belépés freemail-es accountra

A gyakorlat végrehajtásához be kell lépnünk a tárgy freemail-es fiókjába. Kérem, hogy navigáljon el a https://freemail.hu oldalra és lépjen be a tárgy fiókjába az alábbi felhasználónév, jelszó párossal:

- Felhasználónév: **sajat.infokomm**@freemail.hu
- Jelszó: **Sajat.infokomm1**

Sikerült belépnie? (Ha nem sikerült, bátran válassza a nem opciót.)

☐ Igen ☒ Nem

Adathalászat támadás

Észrevette, hogy átesett egy adathalász támadáson? Ennek igazolására kérem váltson át a támadó gép felületére és az ott található konzolon azonnal látható a https://freemail.hu oldalon beírt felhasználónév és jelszó páros. A támadás tesztelhető más adatokkal is: lépjen a https://freemail.hu oldalra és írjon be egy tetszőleges felhasználónév és jelszó párost. Az eredmény a támadógép konzolján látható.

☒ Igen ☒ Nem

Hogyan azonosítsunk egy ilyen támadást?

Az általános alapvetések, amelyekre fel szokták hívni az áldozatok figyelmét, itt most nem állják meg a helyüket:

- A böngésző nem adott semmilyen figyelmeztető jelzést, hogy bármi miatt is aggódni kellene vagy esetleg nem megbízható oldalra navigáltunk.
- Az url cím nincs elgépelve (pl. sokszor szokták alkalmazni a faceb00k.com, vagy facebo0k.com címeket, mert a 0 karakter nagyon hasonlít az o karakterre).
- A kommunikációs csatorna titkosítva van (kis lakat a címsor elején).

Ez azt jelentheti, hogy valaki hozzáfért a számítógépünkhöz (ezért nagyon fontos, hogy mindig zároljuk a gépünket, ha felügyelet nélkül hagyjuk, illetve mindig komplex jelszavakat válasszunk). Egy ilyen támadás esetén az áldozat gépén rendkívül

rövid idő alatt végrehajtható a támadó tevékenység. Amennyiben a támadó egy rutinos hacker, akkor szinte lehetetlen észrevenni, hogy valami nincs rendben.

Segítségünkre lehet azonban a weboldal tanúsítványa. Ha a támadó felületes munkát végzett az sok esetben a tanúsítványból ez észrevehető. Navigáljunk a https://freemail.hu oldalra és kattintsunk a lakat gombra, majd a certificate elemre. A felugró ablakban láthatjuk a tanúsítvány részleteit.

Milyen cég bocsátotta ki a tanúsítványt?

Internet Widgits Pty Ltd.

Melyik állam?

Melyik államban található a kibocsátó cég?

☒ Some-State ☐ New York ☐ Texas

IP cím azonosítása

Már a tanúsítványból is következtethetünk arra, hogy itt valami nincs rendben. De érdemes megvizsgálni az IP címeket is. Indítsunk egy terminált (bal oldalon a kedvenc listából a legalsó elem).

Először vizsgáljuk meg a saját IP címünket az *ifconfig* parancssal.

10.0.2.4

Majd vizsgáljuk meg a weboldalhoz tartozó IP címet a *ping freemail.hu* parancssal. (A freemail.hu egy olyan domain név, amihez egy IP cím tartozik. A számítógépek igazából az IP címeket használják az eléréshez, míg a domain név az emberek segítségéül szolgál, hogy könnyen megjegyezhessék egy-egy szerver elérési címét.)

10.0.2.6

Mit kell tennünk ezek után?

Jelezzük a böngészőnknek, hogy ebben a tanúsítványban nem bízunk meg.

1. A Chromium felületén a jobb felső sarokban található egy ... ikon függőleges helyzetben.
2. A lenyíló menüben keressük meg a *Settings* (Beállítások) pontot.
3. Az így megnyílt oldalon a keresési mezőbe beírva keressünk rá a *"certificates"* (tanúsítványok) kulcsszóra.
4. Security → Manage Certificates → Authorities tab
    - az itt található Tab-on keressünk rá az Internet Widgets Pty Ltd tanúsítvánra és töröljük a "*delete*" (törlés) gombbal.
5. Indítsuk újra a Chromium alkalmazást.

Ezzel azt értük el, hogy most már a böngészőnk nem bízik meg ebben az oldalban (illetve tanúsítványban). De érdekes kérdés, hogy miért a támadó IP címéhez próbálunk csatlakozni, ha a freemail.hu oldalt szeretnénk elérni. Erre az a válasz, hogy az úgynevezett DNS kiszolgálót írta felül a támadó (DNS kiszolgálótól kérdezi meg a számítógépünk, hogy egy domain névhez milyen IP cím tartozik). Ezt értelmes keretek között csak akkor tudja megtenni a támadó, ha kicsi a hálózat (pl. otthoni WiFi).

- Tehát érdemes hálózatot váltani, illetve megkérni a rendszeradminisztrátort, hogy vizsgálja meg történt-e behatolás a rendszerbe.

Sajnos ebben az esetben rosszabb a helyzet. Hiába váltanánk hálózatot, a domainhez továbbra is a támadó IP címe lenne rendelve. De hogyan lehetséges ez?

A DNS kiszolgálók hierarchikusan működnek. Van egy első DNS kiszolgáló, amit a számítógépünk megkérdez egy domain feloldásáról. Ha ez a kiszolgáló nem tudja a választ, mert benne nincs ilyen információ, akkor az továbbküldi a kérést egy másik DNS kiszolgálónak és így megy tovább a folyamat, amíg meg nem találjuk a kérdéses domain címhez tartozó IP címet. (Ennél a gyakorlatban azért sokkal komplexebb működésről van szó, de a lényeget jól leírja.) Viszont érdemes tudni, hogy minden számítógép esetén a 0. ilyen kiszolgáló maga a számítógép. Ehhez egy "*hosts*" nevű fájlt használ, amibe felvehetünk domain és IP cím párosokat. Linux alapú rendszerek esetén ez a fájl az "*/etc/hosts*" Windows alapú rendszerek esetében a "*C:\Windows\System32\drivers\etc\hosts*", míg Mac OS X esetében a "*/private/etc/hosts*" elérési úton található.

1. Nyissuk meg az "*/etc/hosts*" fájlt egy szerkesztővel. Ennek módosításához szükséges lesz a felhasználó jelszavára is (tehát egy ilyen támadás esetén a támadó ismeri a gépünk jelszavát).
    - a terminálba írjuk be, hogy "*sudo gedit /etc/hosts*", majd a jelszavunkat, ami **Ubuntu11.**
    - meglepő lehet, hogy jelszó írásakor nem jelenik meg semmilyen karakter a terminálban, de ettől ne ijedjünk meg.
2. Keressük meg és töröljük a freemail.hu oldalhoz kapcsolódó sort.
3. Mentsük a fájlt és indítsuk újra a Chromium alkalmazásunkat.

Ha minden jól sikerült, most már nyugodtan tudunk böngészni.

Adathalászat vizsga

Leírás és előkészület

Az adathalászat (*phishing*) lényege abban rejlik, hogy az adathalászok a felhasználókat valamilyen elektronikus csatornán keresztül, - például e-mailben, azonnali üzenetben vagy éppen szalagcím hirdetésekben - egy látszólag teljesen eredeti, valójában pedig egy hamis weboldalra irányítják, ahol arra kérik, hogy adják meg bizalmas adatait. Az adathalászatnak számos válfaja van aszerint, hogy milyen módon, milyen elektronikus csatornán keresztül invitálják a felhasználót a hamis weboldalra.

A teszt elkezdéséhez indítsa el az alábbi virtuális gépeket a VirtualBox alkalmazás segítségével és válaszd ki az alattuk található "Phishing" nevű pillanatfelvételt a meghatározott sorrendben:

1. Áldozat (Ubuntu Phishing Vizsga)
2. Támadó (Kali Phishing)

Végül lépjen be az Áldozathoz kapcsolódó virtuális gép felületére.

Biztonságosak-e?

Biztonságosak-e a következő oldalak? (Az oldalak kipróbálásához kérem használja a Chromium Web Browser alkalmazást)

Kérdés 0

facebook.com ☒ Igen ☐ Nem

Kérdés 1

freemail.hu ☐ Igen ☒ Nem

Kérdés 2

index.hu ☒ Igen ☐ Nem

Kérdés 3

gmail.com ☒ Igen ☐ Nem

Kérdés 4

Mi a támadó IP címe?

10.0.2.6

Kérdés 5

Hány elfogadott tanúsítvány található, ami "e" betűvel kezdődik? (Az "*org-*" résztől tekintsünk el.)

3

Kérdés 6

A támadás elhárítása után állapítsa meg, hogy mi az eredeti oldal tanúsítványának kibocsátó cége. (Issued By rész Organization Name értéke)

DigiCert Inc

DoS gyakorlat

A teszt általános leírása

A DoS (Denial of Service) egy olyan általános támadási metodológia, amely elsősorban szolgáltatások ellehetetlenítését célozza. Azonban mi magunk is áldozatául eshetünk a DoS támadásnak saját eszközünkön. Emiatt fontos megtapasztalni milyen az, amikor DoS támadás éri eszközünket.

Előkészítés

A teszt elkezdéséhez indítsa el az alábbi virtuális gépeket a VirtualBox alkalmazás segítségével és válassza ki az alattuk található "DoS" nevű pillanatfelvételt a meghatározott sorrendben:

1. Áldozat (Windows DoS)
2. Támadó (Kali DoS)

Végül lépjen be az Áldozathoz kapcsolódó virtuális gép felületére.

Gép leválasztása a hálózatról

A Windows-os asztali számítógépünk éppen támadás alatt van. Méghozzá olyan mértékben, hogy a gépen szinte semmit se lehet tenni. Ilyenkor érdemes azonnal lecsatlakoznunk a hálózatról.

Hogyan tudjuk kihúzni az internetkábelt a virtuális gépen?

☒ Gép → Konfigurálás → Hálózat → Haladó → Kábel bedugva

☐ Gép → Reset

☒ Eszközök → Hálózat → Hálózati Adapter Csatlakoztatása

ICMP Flood

A DoS támadásoknak sok fajtája van attól függően, hogy a rendszer mely hálózati komponensének/szolgáltatásának gyengeségeit próbálják meg kihasználni. Jelen esetben egy úgynevezett ICMP Flood támadással állunk szemben. Az ICMP Flood azon az egyszerű parancson alapul, amit "ping"-nek nevezünk, és eredeti célja

megkérdezni egy hálózaton található számítógéptől, hogy elérhető-e. Amire az adott számítógép természetesen automatikusan válaszolhat, illetve amennyiben nagyon sokszor kell egy ilyen kérdésre nagyon rövid időn belül válaszolni, akkor az ellehetetleníti más programok futtatását.

Melyik alkalmazásban tilthatjuk le bejövő kérésekre történő reagálást?

☐ Feladatkezelő ☒ Fokozott biztonságú Windows Defender tűzfal

☒ Csoportházirend ☐ Beállításszerkesztő

Tűzfal beállítások

Indítsunk egy "Fokozott biztonságú Windows Defender tűzfal" alkalmazást. Az alkalmazáson belül válasszuk ki a "Bejövő szabályok" részt, hiszen azt szeretnénk megvizsgálni, hogy milyen szabályok vonatkoznak a távolról érkező kérdésekkel kapcsolatban. A táblázatban pedig vizsgáljuk meg, hogy van-e olyan szabály, amely az ICMP protokollhoz kapcsolódik és engedélyezi a kapcsolatfelvételt.

A "Kimenő szabályok" természetesen ennek az ellentét szabályozzák, tehát itt a számítógépen futó alkalmazások kimenő kommunikációjára vonatkozó szabályok találhatóak meg.

Mi a szabály neve, amely engedélyezi a ping üzenetek fogadását?

Ping engedélyezés

Szabály letiltása és csatlakoztatás

Az így megtalált szabályt tiltsuk le (jobb klikk → szabály tiltása). Ezek után engedélyezzük újra a hálózati kapcsolatot (Eszközök → Hálózat → Hálózati adapter csatlakozása). Ha minden jól sikerült, akkor a csatlakozás után is sikerül hozzáférni a gép felületéhez. Ennek ellenőrzése érdekében kérem adja meg a számítógép IP címét.

(Indítsuk el a "Gépház" alkalmazást, majd válasszuk ki a "Hálózat és Internet" menüpontot. Ezután kattintsunk a "Tulajdonságok" gombra, végül tekerjünk az oldal aljára és keressük meg az "IP-v4 cím" bejegyzést.)

10.0.2.5

DoS vizsga

Leírás és előkészület

A DoS (Denial of Service) egy olyan általános támadási metodológia, amely elsősorban szolgáltatások ellehetetlenítését célozza. Azonban mi magunk is áldozatául eshetünk a DoS támadásnak saját eszközünkön. Emiatt fontos megtapasztalni milyen az, amikor DoS támadás éri eszközünket.

A teszt elkezdéséhez indítsa el az alábbi virtuális gépeket a VirtualBox alkalmazás segítségével és válassza ki az alattuk található "DoS" nevű pillanatfelvételt a meghatározott sorrendben:

1. Áldozat (Windows DoS Vizsga)
2. Támadó (Kali DoS)

Végül lépjen be az Áldozathoz kapcsolódó virtuális gép felületére.

Kérdés 0

Hány fájl található a letöltések mappában?

0

Kérdés 1

Melyik szabály okozta a DoS támadást?

Windows ICMP protokoll engedélyezése

Kérdés 2

Csatlakozás után mi a gép IP címe?

10.0.2.5

Backdoor gyakorlat

A teszt általános leírása

A hátsóajtó alkalmazások (Backdoor) olyan általános támadási programok csoportját alkotják, melyek működése során a felhasználók tudtukon kívül hozzáférést biztosítanak a saját eszközükhöz a hálózaton keresztül. Ezáltal a támadók bármikor át tudják venni az eszköz irányítását, manipulálhatják az eszközön lévő adatokat, illetve el is tulajdoníthatják ezeket az adatokat.

Előkészítés

A teszt elkezdéséhez indítsa el az alábbi virtuális gépeket a VirtualBox alkalmazás segítségével és válassza ki az alattuk található "Backdoor" nevű pillanatfelvételt a meghatározott sorrendben:

1. Áldozat (Android Backdoor)
2. Támadó (Kali Backdoor)

Végül lépjen be az Áldozathoz kapcsolódó virtuális gép felületére.

Fake-email

Amint beléptünk az Android platformra, indítsuk el a Gmail alkalmazást, amelyben egy új e-mailt találhatunk egy bizonyos Teszt Elek felhasználótól. Nyissuk meg az emailt és olvassuk el a tartalmát.

A megtévesztő email a social engineering technikák egyik alapvető eszköze, melynek célja, hogy a gyanútlan felhasználó valamilyen programot telepítsen a saját eszközére. Fontos kiemelni azonban két dolgot:

- az ilyen álhírek elsődleges célja valamilyen hatás, érzelem kiváltása a felhasználóból:
    - kedvenc foci csapatunk videója,
    - csalások a kedvenc telefonos játékunkhoz (végtelen élet, végtelen érme stb.),

    - ingyenes kuponkódok generálása a legnépszerűbb divatáruházak oldalára.
- az ilyen álhírek mindig tartalmaznak valamilyen linket, vagy csatolmányt
    - amin keresztül regisztrálhatunk valahova,
    - amin keresztül letölthetünk valamit.

Mi az alkalmazás neve, amit Teszt Elek barátunk szeretne letöltetni velünk?

SmartWallet

Alkalmazás letöltése

Bár már a megtévesztő e-mail gyanús lehet számunkra, de a gyakorlat kedvéért sétáljuk bele a csapdába. Kattintsunk a megadott linkre.

Mi a fájl neve, amit le szeretnénk tölteni?

☒ smartWallet.v1.2.x86_64.apk ☐ mainActivity.v1.5.x86.apk

☐ readme.txt ☐ installer.apk

Alkalmazás telepítése

A Google Chrome Webbrowser természetesen azért jelzi, hogy óvatosan kezeljük ezeket a .apk kiterjesztéssel rendelkező fájlokat, de ezeket legtöbbször észre se vesszük, automatikusan figyelmen kívül hagyjuk. Ugyanilyen üzenetet kapunk, ha Windows-on .exe vagy .jar kiterjesztésű fájlokat szeretnénk letölteni. Ezek a fájltípusok legyenek gyanúsak.

Mindenesetre, ha letöltöttük a fájlt, akkor az értesítési területen (az egerünket a kijelző telejéről húzzuk le, míg a bal egérgombot nyomva tartjuk - így szimulálva egérrel a mutatóujjal történő lehúzásos érintést). Az értesítési területen pedig kattintsunk a fájlra, aminek hatására elindul a telepítés.

Milyen hozzáféréseket kér az alkalmazás a működéséhez?

☒ Mindenhez. ☐ Üzenetek, névjegyek. ☐ SD kártya és belső tárhely.

☐ Kamera és GPS. ☐ Telefonhívás alkalmazáshoz. ☐ SMS küldéshez.

Alkalmazás elindítása

A telepítés utolsó fázisa az alkalmazás elindítása. Ehhez a képernyő jobb alsó sarkában lévő Open gombra kell kattintani.

Támadó korlátlan eszközei

Miután elindítottuk az alkalmazást a támadó korlátlan hozzáférést szerzett az eszközünkhöz. Próbáljuk is ki. Váltsunk át a Támadó gép felületére, amin egy terminál látható, ahol az alábbi parancsokat próbálhatjuk meg beírni:

- dump_contacts: az összes névjegy letöltése
- dump_sms: az összes sms letöltése
- webcam_stream -i [azonosító]: az azonosító helyére beírva egy számot, az adott azonosítóval rendelkező kamera képét kapja meg a támadó
- geolocate: az eszköz helyadatait küldi el.
- ?: az összes elérhető parancs

Ezen adatok támadó általi felhasználásának lehetőségei sokrétűek.

Alkalmazás törlése

Térjünk vissza az áldozat gépére és próbáljuk meg törölni az alkalmazást. De mi volt a telepített alkalmazás neve?

☐ SmartWallet ☒ MainActivity

Rejtőzködés

Az ilyen Backdoor alkalmazások rendkívül ügyesen rejtőzködnek:

- nem jött létre indító ikon,
- nem az a neve az alkalmazásnak, mint aminek álcázták eredetileg.

Menjünk a Beállítások (Settings) menübe és keressük meg az Alkalmazások és Értesítések (Apps & Notifications) menüpontot. Itt találhatóak a telepített alkalmazások, melyek között keressük meg a "MainActivity" nevű alkalmazást, majd kattintsunk rá és töröljük.

Ismeretlen Szoftver telepítésének letiltása

Az Android platformon külön beállítható, hogy milyen forrásból származó ismeretlen aklalmazásokat lehet telepíteni. Ha minden ilyen opciót letiltunk, akkor csak a Play Áruházból lehet majd telepíteni hitelesített alkalmazásokat.

Lépjünk a Beállítások alkalmazásba (Settings) és az Alkalmazások és Értesítések menüpontra (App & Notifications). Ezen belül keressük meg a Speciális alkalmazáshozzáférések menüpontot (Special app access), ahol kattintsunk az Ismeretlen Alkalmazások Telepítésére (Install unknown apps). Mint látható a Google böngészőből való telepítés engedélyezve van. Ezt tiltsuk le.

Play Protect

Az alkalmazásokhoz kapcsolódóan az Android bevezette a Play Protect alkalmazást, amely egy vírusírtóként funkcionál és képes értesítést küldeni a felhasználónak, ha gyanús program telepítését észleli. Ezt is kapcsoljuk be, amelyhez indítsuk el a Play Áruházat (Play Store), majd a bal felső sarokban kattintsunk a három vonalra (beállítások/settings), ahol válasszuk ki a Play Protect menüpontot és kapcsoljuk be (turn on).

Backdoor vizsga

Leírás és előkészület

A hátsóajtó alkalmazások (Backdoor) olyan általános támadási programok csoportját alkotják, melyek működése során a felhasználók tudtukon kívül hozzáférést biztosítanak a saját eszközükhöz a hálózaton keresztül. Ezáltal a támadók bármikor át tudják venni az eszköz irányítását, manipulálhatják az eszközön lévő adatokat, illetve el is tulajdoníthatják ezeket az adatokat.

A teszt elkezdéséhez indítsa el az alábbi virtuális gépeket a VirtualBox alkalmazás segítségével és válassza ki az alattuk található "Backdoor" nevű pillanatfelvételt a meghatározott sorrendben:

1. Áldozat (Android Backdoor Vizsga)
2. Támadó (Kali Backdoor)

Végül lépjen be az Áldozathoz kapcsolódó virtuális gép felületére és indítsa el a Gmail alkalmazást a megtévesztő e-mail megtekintéséhez.

Kérdés 0

Mi a weboldal IP címe, ahonnan szeretnénk letölteni az alkalmazást?

10.0.2.9

Kérdés 1

Melyik alkalmazás esetén van engedélyezve az ismeretlen alkalmazások telepítése?

☒ Chrome ☐ Gmail

Kérdés 2

Be van kapcsolva a Play Protect?

☐ Igen ☒ Nem