NEMZETI KÖZSZOLGÁLATI EGYETEM
Közigazgatás-tudományi Doktori Iskola

Oroszi Eszter Diána

A biztonságtudatossági szint fejlesztése gamifikációs módszerek alkalmazásával

Doktori (PhD) értekezés

TÉZISFÜZET

Témavezető:

Dr. Leitold Ferenc, főiskolai tanár

Budapest, 2023

TARTALOMJEGYZÉK

1. A DISSZERTÁCIÓ CÉLJA, A TÉMA AKTUALITÁSA

A szervezet elsődleges védvonalát az információbiztonsági támadásokkal szemben annak munkavállalói jelentik. Ahogyan számos statisztika is rávilágít, a humán faktor kihasználása gyakori – és sikeres – eszköze a támadóknak. Az emberi tényezőt kihasználó támadásoknak számtalan technikája létezik, ezen módszereket nemzetközi szerzők mellett több hazai szakértő is részletesen bemutatta tanulmányaiban, és megalapozta, hogy a Social Engineering módszerek valós fenyegetést jelentenek a szervezeteknek. Ezen támadási technikák folyamatosan fejlődnek és egyre újabbak jelennek meg.

Világszerte számos állami szervezet támaszkodik digitális kormányzati szolgáltatásokra, mely növeli az információbiztonsági kockázatokat ebben a szektorban is. A közigazgatási szervezetek szerepükből és működésükből kifolyólag különösen a szolgáltatásokat elérhetetlenné tevő túlterheléses/DoS támadásoknak, honlaprongálásnak (defacement), adathalászat és kártékony kód jelentette fenyegetéseknek, jogosulatlan hozzáférésnek és adatszivárgásnak, illetve adatlopásnak vannak kitéve. Nemzetközi kutatások is alátámasztják, hogy a közszféra az egyik legtöbb kiberbiztonsági incidens által érintett szektor 2022-ben. Mindezek miatt elengedhetetlen a közszféra szervezeteinek információbiztonsági fejlesztése, melynek a munkavállalók biztonságtudatossági oktatása elengedhetetlen része. A disszertációban bemutatott, információbiztonsági relevanciájú hazai jogszabályok, illetve ajánlások mindegyike előírja a felhasználók információbiztonsági oktatásának szükségességét. Az emberi tényező jelentette kockázatok csökkentése tehát minden szervezet érdeke, ezért elengedhetetlen a felhasználók biztonságtudatossági ismereteinek bővítése, a téma iránti érzékenyítése megfelelő módszerek kidolgozásával és alkalmazásával. Az egyes képzési módszerek eltérő hatékonysággal működhetnek különböző szervezeteknél, illetve felhasználói csoportoknál, ezért fontos azok alkalmazás előtti értékelése, hatékonyságának vizsgálata.

Mind a szakirodalom feltárás alátámasztotta, mind a saját tapasztalataim megerősítették, hogy az általánosan alkalmazott oktatási módszerek önmagukban már nem elegendőek a tudatossági szint hatékony fejlesztésére, ahogyan a támadási technikák, úgy a felhasználók igényei is az elmúlt 10 év során rengeteget változtak.

Ezen okokból kifolyólag tűztem ki célul annak vizsgálatát, hogy milyen, a kor követelményeinek és aktuális trendeknek megfelelő módszerekkel lehet a felhasználók biztonságtudatossági ismereteit hatékonyan fejleszteni, a biztonságtudatos szemléletet elsajátíttatni, a résztvevőket a biztonságtudatos magatartásra ösztönözni. Ennek egy potenciális

megoldásaként a manapság elterjedt gamifikációs módszereket azonosítottam, és ezek alkalmazhatóságát vizsgáltam a biztonságtudatosság fejlesztésének lehetőségére. Kíváncsi voltam arra, hogy mely biztonságtudatosságot fejlesztő megoldások milyen hatékonyan bővítik a munkavállalók biztonságtudatossági ismereteit, melyik módszer mennyire preferált a felhasználók által, milyen felhasználói élményt nyújt a résztvevőknek, illetve a gamifikációs megoldások ténylegesen alkalmazhatóak-e munkahelyi környezetben a biztonságtudatosság fejlesztésére, és ha igen, milyen eredményességgel, valamint kinek és hogyan érdemes ezt a módszert használnia. Mindezen kutatás során ezért arra is hangsúlyt fektettem, hogy a munkahelyi környezet, munkahelyi sajátosságok, kifejezetten a szervezetek jellege hogyan befolyásolja a felhasználók biztonságtudatosságának szintjét, valamint az alkalmazott módszerek sikerességét és hatékonyságát.

A biztonságtudatossági módszerek hatékonyságának vizsgálatához kapcsolódó kutatásokat szintén több nemzetközi és hazai szakértő is publikált, és eredményeik azt mutatják, érdemes tovább vizsgálni a témát, hiszen ahogyan több szerző is bizonyította, a preferált megoldások a gyakorlatban még nem feltétlenül bizonyulnak hatékonynak. Ennek ellenére a gamifikáció biztonságtudatossági képzésekben való alkalmazhatóságát még viszonylag kevés tudományos publikáció vizsgálta: 2023. június 26-i lekérdezés alapján a Scopus-on az „awareness” és „gamification” kifejezésekre keresve 104 darab releváns találat született, a témakört leszűkítve „Computer Science”-re 13 darab publikáció volt azonosítható, az Academia.edu felületén a „security awareness gamification” témára keresve összesen 959 darab publikációt, ezen belül 62 darab folyóirat cikket és 1 darab konferencia közleményt találtam. Mindezek miatt fontosnak találtam a biztonságtudatosság gamifikációs módszerekkel történő fejlesztésének mind szakirodalmi, mind gyakorlati vizsgálatát.

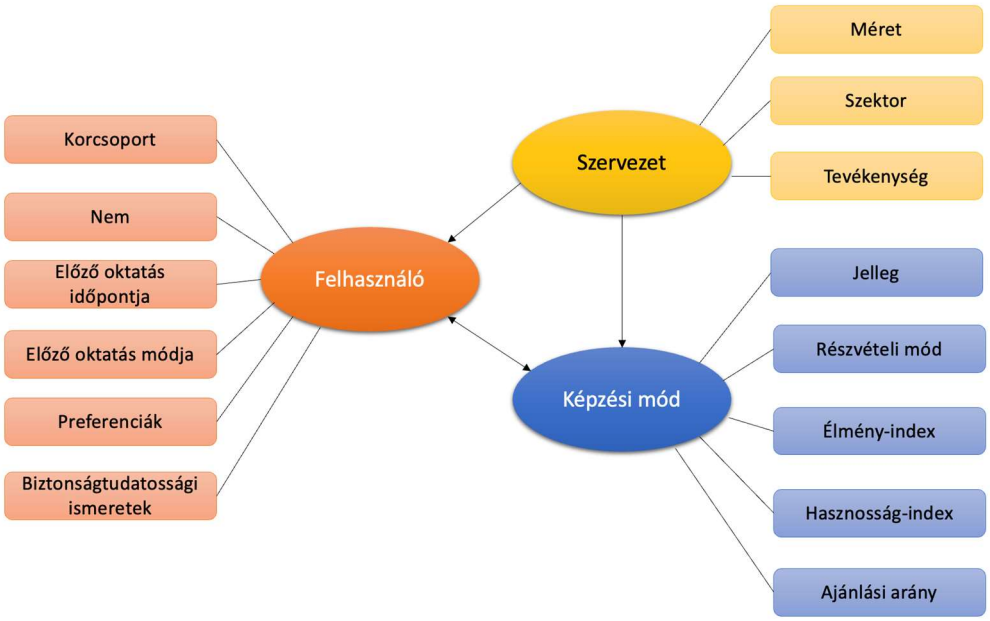
2. A KAPCSOLÓDÓ KUTATÁS BEMUTATÁSA ÉS A DISSZERTÁCIÓ FELÉPÍTÉSE

A disszertáció elkészítéséhez mind szakirodalom feltárást, mind saját kutatásokat végeztem. A vizsgálatok és felmérések során számtalan esetben támaszkodtam egyrészt saját gyakorlati tapasztalataimra, másrészt más forrásokból származó felmérések eredményeire, valamint a tudatosító programok visszajelzéseire és kifejezetten a biztonságtudatossági szabadulószobában és a társasjáték programok lebonyolítása során tett megfigyelésekre is.

A kutatás első lépése a releváns nemzetközi és hazai szakirodalom feltárása volt Social Engineering, biztonságtudatosság, illetve a kapcsolódó oktatások, képzések, fejlesztési lehetőségek, azon belül is kifejezetten a gamifikáció vonatkozásában.

A szakirodalom feltárás eredményei alapján négy hipotézist állítottam fel, és ezeket külön fejezetekben vizsgáltam. A hipotézisek igazolására legalkalmasabb adatgyűjtési módszernek a gyakorlati elemekkel kiegészített kérdőíves felmérést választottam, melyet az első hipotézis vizsgálata során mutatok be részletesen. Emellett figyelembe vettem a témában releváns korábbi felméréseimet, valamint gyakorlati tapasztalataimat is.

A kérdőíves felmérés során gyűjtött adatokat az egyes hipotézisek vizsgálata során mutatom be és elemzem, az egyes fejezetek bemutatják a kutatás felhasznált adatait az adott témához illeszkedően. Összességében az 1. ábrán jelölt adatokkal dolgoztam.



1. ábra: A kutatás során gyűjtött és felhasznált adatok (forrás: saját szerkesztés)

Az ábrán a színek jelölik az egyes összetartozó csoportokat, így a szervezeti, felhasználói, valamit a képzés típusokhoz kapcsolódó jellemzőket. A csoportok közötti nyilak azok egymásra hatását mutatják be.

Az adatok elemzése során általános, leíró statisztikai módszereket, valamint klaszterelemzést hajtottam végre.

Disszertációmat az alábbi fejezetekre bontottam, melyek során a következőket mutatom be:

- **2. fejezet**: *Szakirodalom áttekintés*, melyben a kutatás első fázisának módszerét és eredményeit mutatom be részletesen, és ismertetem a kutatásban is megjelenő biztonságtudatosság fejlesztési módszereket, illetve feltárom az ezekhez kapcsolódó követelményeket, azonosított legjobb gyakorlatokat.
- **3. fejezet**: *A biztonságtudatossági fejlesztési módszerek hatékonyságának vizsgálata a felhasználói élmény tükrében*, melyben bemutatom a választott adatgyűjtési módszert és a disszertációhoz készített gyakorlati kutatást, és annak eredményeit, mint például az egyes vizsgált módszerek hatékonyságát, illetve vizsgálom ennek felhasználói preferenciával élménnyel, valamint hasznossággal való kapcsolatát.
- **4. fejezet**: *A gamifikáció alkalmazhatósága munkahelyi környezetben a felhasználók biztonságtudatossági ismereteinek bővítésére* címet viseli, melyben kifejezetten azon kutatási eredményeket taglalom, melyek azt bizonyítják, a játékosított megoldásoknak van-e létjogosultsága az információbiztonsági fejlesztésekben.
- **5. fejezet**: *A biztonságtudatossági szabadulószoba alkalmazhatósága munkahelyi környezetben a felhasználók biztonságtudatossági ismereteinek bővítésére* című részben a 4. fejezet egy speciális megoldását emelem ki, melyhez egy korábbi kutatás eredményeit is felhasználom, annak vizsgálatára, hogy a hivatkozott megoldás alkalmazható-e munkahelyi környezetben a biztonságtudatosság fejlesztésére.
- **6. fejezet**: *A biztonságtudatossági társasjáték alkalmazhatósága munkahelyi környezetben a felhasználók biztonságtudatossági ismereteinek bővítésére* című részben a 4. fejezet egy speciális megoldását emelem ki, bemutatva egy ilyen megoldás fejlesztésének lépéseit is, egyúttal megvizsgálva, hogy a hivatkozott megoldás alkalmazható-e munkahelyi környezetben a biztonságtudatosság fejlesztésére.
- **7. fejezet**: *Összegzés*, melyben összefoglalom a kapcsolódó kutatás eredményeit és következtetéseit, valamint a készített módszertanok és eszközök további felhasználási és bővítési lehetőségeit.

3. VIZSGÁLT HIPOTÉZISEK

Disszertációmban azt tűztem ki célul, hogy összehasonlítsam a különböző biztonságtudatosságot fejlesztő módszerek hatékonyságát, következtetést vonjak le, hogy melyik módszer milyen jellegű fejlesztésekre, illetve mely témakörökben és munkahelyi környezetekben alkalmazható leginkább, segítve ezzel a szervezetek információbiztonsági-tudatosság fejlesztő akcióinak tervezését, azok hatékonyságának növelését. A vizsgált módszereken belül kifejezetten kíváncsi voltam a gamifikációs megoldások alkalmazhatóságára hazai környezetben, eltérő szektorban működő, különböző méretű szervezetek körében, azon belül is két általam fejlesztett gamifikációs program, a biztonságtudatossági szabadulószoba és a biztonságtudatossági társasjáték vonatkozásában.
A disszertáció készítése során olyan kérdésekre kerestem a választ, mint

- melyik biztonságtudatosságot fejlesztő módszer a leghatékonyabb, ezen belül is hogyan szerepelnek a gamifikációs megoldások,
- milyen módszer adja át a legtöbb tudást a különböző fejlesztési akciók résztvevőinek,
- mely módszerrel lehet elérni a legtöbb felhasználó legalább minimális szintű ismeret-bővülését (azaz növeli azon felhasználók számát, akik a programot követően legalább egy új ismerettel gazdagodnak),
- hosszútávon (például egy hónappal később) melyik oktatási módszeren tanult ismeretek maradnak meg leginkább a felhasználókban, milyen képzések adnak tartós tudást,
- milyen módszereket preferálnak a felhasználók, ha képzéseken való részvételről kell dönteniük és ennek van-e befolyása a tanultakra,
- hogyan értékelik a felhasználók az egyes biztonságtudatossági programokat felhasználói élmény, élvezetesség szempontjából, és ez milyen hatással van a biztonságtudatossági szint fejlődésére,
- hogyan értékelik a felhasználók az egyes biztonságtudatossági programokat hasznosság szempontjából, és ez milyen hatással van a biztonságtudatossági szint fejlődésére,
- tehát van-e összefüggés a megszerzett tudás, illetve a felhasználói preferencia, valamint a program által nyújtott felhasználói élmény mértéke között,
- melyek a leginkább meglévő biztonságtudatossági ismeretek, és
- melyek azok, amelyek legtöbbet fejlődtek a biztonságtudatossági programon való részvételt követően,

- van-e létjogosultsága a gamifikációs módszereknek, azon belül a biztonságtudatossági szabadulószoba és a biztonságtudatossági társasjáték alkalmazásának munkahelyi környezetben,
- hogyan és milyen módszert válasszunk a következő biztonságtudatosságot fejlesztő kezdeményezésünk tervezése során?

Ezen kérdések alapján az alábbiakban bemutatott négy, részben egymásra épülő hipotézist határoztam meg és mutattam be, valamint vizsgáltam részletesen a disszertáció fejezeteiben.

H1 hipotézis: „A Magyarországon elhelyezkedő, mind privát, illetve állami szektorban működő szervezetek esetében azon biztonságtudatosságot fejlesztő programok, melyeket a felhasználók élveznek, nagyobb mértékben növelik a biztonságtudatossági ismeretek számát, illetve több munkavállaló biztonságtudatossági ismereteit növelik, mint azok a megoldások, melyeket a felhasználók preferálnak, vagy hasznosnak vélnek."

A hipotézis igazoláshoz kifejlesztettem egy gyakorlati felmérési módszertant a biztonságtudatosságot fejlesztő módszerek hatékonyságának összehasonlítására, melyet a disszertáció 3. fejezetében mutatok be. A vizsgálattal célom annak bizonyítása volt, hogy azok a biztonságtudatosságot fejlesztő módszerek, melyek élvezetesek a felhasználók számára, nagyobb mértékben növelik a felhasználók biztonságtudatossági ismereteinek számát, valamint több felhasználó ismereteit képesek bővíteni, mint azon módszerek, melyeket a felhasználók preferálnak, vagy hasznosnak tartanak.

Az eredmények alapján megállapítottam, hogy a felhasználói preferencia nem befolyásolja a képzések hatékonyságát, vagyis attól, hogy a felhasználó általa nem preferált képzési módban részesül, még nem jelenti azt, hogy nem tanul belőle, és ugyanez fordítva is igaz: egy preferált képzési módszer még nem feltétlenül lesz hatékony is. A felhasználó által vélt hasznosság értékelése és a hatékonyság között gyenge pozitív kapcsolatot azonosítottam, mely alapján elmondható, hogy azok az oktatási módszerek, melyeket a felhasználók hasznosnak tartanak, kis mértékben hatékonyabbak mind a biztonságtudatossági ismeretek számának, mind a biztonságtudatosabb felhasználók számának növelésében. Ugyanígy egy gyenge pozitív kapcsolatot mutatott annak vizsgálata is, hogy a felhasználói élmény hogyan befolyásolja az új biztonságtudatossági ismeretek számát egy képzésen való részvételt követően, szoros kapcsolatot azonosítottam azonban a biztonságtudatosabb felhasználók számának növelésében. Ezáltal elmondható, hogy a felhasználói élmény befolyásolni tudja egy biztonságtudatossági program hatékonyságát. Tehát akik olyan programon vesznek részt, melyet élveznek, nagyobb

valószínűséggel tanulnak is a képzés során, mint akik kevésbé élvezetes oktatásban részesülnek.

H2 hipotézis: „A játékosítást alkalmazó megoldások, gamifikációs módszerek alkalmazhatóak a Magyarországon elhelyezkedő, mind privát, illetve állami szektorban működő szervezeteknél tartott információbiztonsági képzések során, valamint képesek a munkavállalók biztonságtudatossági ismereteinek bővítésére és az új biztonságtudatossági ismeretekkel gazdagodott felhasználók számának növelésére."

A hipotézis igazoláshoz a H1-nél alkalmazott felmérés eredményeit használtam fel. A vizsgálattal célom egyrészt annak bizonyítása volt, hogy a felhasználók tényleg a játékosított programokat tartják a legélvezetesebbnek a biztonságtudatossági fejlesztések terén is, másrészt a gamifikációs módszerek képesek a biztonságtudatossági szint fejlesztésére mind az ismeretek bővítése, mind a biztonságtudatosabb felhasználók számának növelése szempontjából.

Az eredmények alátámasztották, hogy a gamifikációs módszereket minden szervezetnél, annak jellegétől, méretétől függetlenül alkalmazhatjuk, mint legélvezetesebb megoldást, illetve a munkavállalók korosztálya és neme szerinti bontásban is bármely felhasználói réteg számára alkalmazható lehet a felhasználói élmény alapján. Ezáltal ki lehet zárni azon tévhiteket, miszerint ezek a módszerek szűkebb felhasználói réteg elérésére lehetnek alkalmasak. Kutatásom azt is igazolta, hogy összességében a gamifikációs módszerek rövid távon legalább olyan hatékonyan képesek fejleszteni a biztonságtudatossági szintet, mint a hagyományos megoldások, hosszútávon viszont alulmaradnak az előadás jellegű oktatásokkal szemben, érdemes ezért vegyes progamelemeket alkalmazni.

H3 hipotézis: „Egy újszerű, általam fejlesztett biztonságtudatossági szabadulószoba képes a Magyarországon elhelyezkedő, mind privát, illetve állami szektorban működő szervezetek munkavállalóinak biztonságtudatossági ismereteinek bővítésére és az új biztonságtudatossági ismeretekkel gazdagodott felhasználók számának növelésére."

A vizsgálat során célom annak bizonyítása volt, hogy az általam 2014-ben fejlesztett biztonságtudatossági szabadulószoba képes a biztonságtudatossági szint fejlesztésére mind az ismeretek bővítése, mind a biztonságtudatosabb felhasználók számának növelése szempontjából. Ehhez a H1-es hipotézishez kidolgozott kutatást alkalmaztam, és annak eredményeit vizsgáltam kifejezetten a szabadulószoba, mint abban is alkalmazott elem vonatkozásában. Az eredmények alapján elmondható, hogy a legalább egy új biztonságtudatossági ismeretet szerző felhasználók aránya szerint a biztonságtudatossági

szabadulószoba a vizsgált 6 módszer közül a 3. legjobb biztonságtudatosságot fejlesztő megoldás, ezáltal képes a biztonságtudatosság fejlesztésére, és érzékenyítés céljából elsősorban az 50-59 éves korosztály, illetve a 30 év alattiak körében a leghatékonyabb. Az eredmények a biztonságtudatossági ismeretek számának növelése szempontjából a biztonságtudatossági szabadulószobának nagyon megosztó az értékelése szektoronként: állami szférában ezen vizsgálati pont alapján kevésbé hatékony az alkalmazása, míg privát szektorban a leghatékonyabb megoldás a tudatossági ismeretek számának növelésére. Mindezek alapján elmondható, hogy a szabadulószoba programot követően nagymértékben fejlődnek a korábban általános hiányosságként azonosított ismeretek (iratmegsemmisítés, közösségi média, telefon és okos eszközök biztonságtudatos használata), illetve a módszer kifejezetten alkalmazható a könnyű testreszabhatóság révén célzott ismeretek átadására.

H4 hipotézis: „Egy újszerű, általam létrehozott biztonságtudatossági társasjáték képes a Magyarországon elhelyezkedő, mind privát, illetve állami szektorban működő szervezetek munkavállalóinak biztonságtudatossági ismereteinek bővítésére és az új biztonságtudatossági ismeretekkel gazdagodott felhasználók számának növelésére."

A vizsgálat során célom annak bizonyítása, hogy az általam 2021-2022-ben fejlesztett biztonságtudatossági társasjáték képes a biztonságtudatossági szint fejlesztésére mind az ismeretek bővítése, mind a biztonságtudatosabb felhasználók számának növelése szempontjából. Ehhez a H1-es hipotézishez kidolgozott kutatást alkalmaztam, és annak eredményeit vizsgáltam kifejezetten a társasjáték, mint abban is alkalmazott elem vonatkozásában. Az eredmények alapján elmondható, hogy a legalább egy új biztonságtudatossági ismeretet szerző felhasználók aránya alapján a biztonságtudatossági társasjáték a vizsgált módszerek között a 2. legjobb biztonságtudatosságot fejlesztő megoldás, ezáltal képes a biztonságtudatosság fejlesztésére, mely érzékenyítés céljából a 30 év alattiak, illetve a 30-39 éves korosztály számára a leghatékonyabb. Állami szférában a biztonságtudatossági ismeretek számának növelése szerint a leghatékonyabb oktatási módszer, míg privát szektorban a legkevésbé hatékony megoldás a tudatossági ismeretek számának növelésére. Általánosságban elmondható, hogy a társasjáték programot követően kis mértékben, de fejlődnek a korábban általánosságban hiányosságként azonosított ismeretek is (iratmegsemmisítés, közösségi média, telefon és okos eszközök biztonságtudatos használata), ezen a téren a játék testreszabhatóságának fejlesztése lehet indokolt, például a lapok speciális jelölésével előválogatás céljából.

4. ÚJ TUDOMÁNYOS EREDMÉNYEK

A disszertációm célja annak bizonyítása volt, hogy az élmény alapú képzési megoldások, gamifikációs biztonságtudatossági módszerek képesek a biztonságtudatosság fejlesztésére mind a biztonságtudatossági ismeretek számának bővítésében, mind pedig a biztonságtudatosabb felhasználók számának (tehát, akik legalább 1 db új ismerettel gazdagodnak az oktatást követően) növelésében. Mindezek mellett kifejlesztettem két, játékosított oktatási lehetőséget, a biztonságtudatossági szabadószobát és egy biztonságtudatossági társasjátékot, melyek biztonságtudatosság-fejlesztésben való hatékony alkalmazhatóságát ezúton is igazoltam.

Fentiek alapján az alábbi tudományos eredmények állapíthatóak meg:

I. Az általam kifejlesztett felmérési módszerrel nem pusztán hagyományos kérdőívek, hanem a különböző programokon való gyakorlati részvétel alapján is tudtam mérni a felhasználók egyes programokra adott értékeléseit, úgy mint preferencia, hasznosság, és az élvezetesség. Ezekhez hozzá tudtam kapcsolni a biztonságtudatossági ismereteik változásának eredményeit és azonosítani tudtam a felhasználói értékelések és a program hatékonysága közötti kapcsolatot. **Mindezekkel bizonyítottam azt a tézist, hogy a Magyarországon elhelyezkedő, mind privát, illetve állami szektorban működő szervezetek esetében azon biztonságtudatosságot fejlesztő programok, melyeket a felhasználók élveznek, nagyobb mértékben növelik a biztonságtudatossági ismeretek számát, illetve több munkavállaló biztonságtudatossági ismereteit növelik, mint a preferált vagy hasznosnak vélt módszerek.**

II. A felhasználói élmény szempontjából egyértelműen a gamifikációs módszerek kerültek ki legjobb megoldásként a kutatásom alapján. Ennek megfelelően egyrészt a felhasználók játékosításra való nyitottságát, másrészt ezen módszerek hatékonyságát mértem szintén az első pontban alkalmazott felméréssel. **Vizsgálatom bizonyította azt a tézist, hogy a játékosítást alkalmazó megoldások, gamifikációs módszerek alkalmazhatóak a Magyarországon elhelyezkedő, mind privát, illetve állami szektorban működő szervezeteknél tartott információbiztonsági képzések során, valamint képesek a munkavállalók biztonságtudatossági ismereteinek bővítésére és az új**

biztonságtudatossági ismeretekkel gazdagodott felhasználók számának növelésére.

III. A biztonságtudatosság fejlesztésére még 2014-ben kifejlesztettem egy **szabadulószoba** módszertant, melyet azóta is aktívan alkalmazok a felhasználók információbiztonsági képzése során. Ezen megoldásra számos pozitív visszajelzés érkezett, azonban a hatékonyságának egyéb módon történő mérése még nem történt meg, így az alkalmazhatósága nem is volt igazolt. **A kutatással és az általam 2014-ben fejlesztett biztonságtudatossági szabadulószobával igazoltam azt a tézist, hogy a biztonságtudatossági szabadulószoba, mint újszerű biztonságtudatosság fejlesztési megoldás, képes a biztonságtudatossági szint fejlesztésére mind az ismeretek bővítése, mind a biztonságtudatosabb felhasználók számának növelése szempontjából.**

IV. A biztonságtudatosság fejlesztésére 2021-2022 között egy biztonságtudatosságot fejlesztő **társasjátékot** is kialakítottam, mely kiadásra került, és mind szervezetek, mind magánszemélyek számára elérhető edukációs megoldás. Ezen megoldásra számos pozitív visszajelzés érkezett, azonban a hatékonyságának egyéb módon történő mérése még nem történt meg, így az alkalmazhatósága nem is volt igazolt. **A kutatással és az általam 2021-2022-ben fejlesztett biztonságtudatossági társasjátékkal igazoltam azt a tézist, hogy biztonságtudatossági társasjáték, mint újszerű biztonságtudatosság fejlesztési megoldás, képes a biztonságtudatossági szint fejlesztésére mind az ismeretek bővítése, mind a biztonságtudatosabb felhasználók számának növelése szempontjából.**

5. GYAKORLATI FELHASZNÁLHATÓSÁG

Disszertációmban bebizonyítottam azt, hogy a gamifikációs módszerek, közük a szabadulószoba és a társasjáték is képes a biztonságtudatossági ismeretek fejlesztésére, mind az új ismeretek bővítése, mind a biztonságtudatosabb felhasználók (azaz olyan résztvevők, akik legalább 1 db új ismerettel bővültek a programot követően) számának növelése céljából. A két vizsgált gamifikációs megoldás (biztonságtudatossági szabadulószoba, illetve biztonságtudatossági társasjáték) a kutatásom eredményei szerint rövid távon kiemelkedően hatékonynak bizonyult, hosszabb távon azonban, bár hatékonyan fejlesztették ugyan a résztvevők tudását, a ranglista alján végeztek. Megjegyzendő azonban, hogy mindkét bemutatott gamifikációs módszerem elsősorban a rendszeres használatot támogatja, a társasjátékkal például kifejezetten cél a gyakori oktatási lehetőség biztosítása, vagy akár társasjáték-klub jellegű felhasználás is. A bemutatott kutatási eredmények, illetve az értekezésben részletesen leírt tapasztalatok hasznos segítséget nyújthatnak az információbiztonság-tudatosító programokat tervező szervezeteknek a számukra legmegfelelőbb módszerek összeválogatásában – hiszen nagyon fontos, hogy nem létezik mindenkinek megfelelő, egyetlen legjobb megoldás.

Az új megoldások, aktuális trendeket követő módszerek, mint jelenleg a gamifikáció, nagy valószínűséggel mindig is népszerűek lesznek, érdemes ezért lépést tartani a korral és nyitni az új lehetőségek felé, fontos azonban, hogy értékeljük, szervezetünknek, munkavállalóinknak mely megoldások a legélvezetesebbek, és leghatékonyabbak. Ahogy a kutatásom több ízben is meglepő módon rávilágított, óriási különbségek lehetnek még a gamifikációs módszerek hatékonysága között is, pusztán a működési szektor vonatkozásában is. Ami az állami szférában a leghatékonyabb megoldásnak bizonyult, az a piaci vállalatok körében az utolsó helyen végzett – és fordítva. Nagyon fontos ezért az előzetes értékelés, preferáltan kulcsfelhasználókkal való tesztelés, melyben akár az általam használt, a disszertációban bemutatott felmérés módszere is nagy segítséget nyújthat.

6. JÖVŐBELI KUTATÁSI IRÁNYOK, TOVÁBBFEJLESZTÉSI LEHETŐSÉGEK

A disszertációhoz készített kutatás számomra is nagyon érdekes és tanulságos eredményekkel szolgált, melyek mentén a következő továbbfejlesztéseket tervezem, mind a további felmérési lehetőségek, mind a kialakított gamifikációs eszközök esetében:

- Célom tovább vizsgálni azt, hogy a rövid távon hatékonyabb gamifikációs módszereknek milyen pozitív hatása lehet más hagyományos képzésekre, az érdeklődés játékosított módszerekkel való felkeltése hatással van-e a hagyományos módszerek sikerességére.
- Jelen kutatásban elsődlegesen a minta-nagyság miatt nem volt rá lehetőség, de érdekes lehet annak vizsgálata is, hogy a gyakorlatban (például egy Social Engineering audit során) ténylegesen hogyan alkalmazzák a tanultakat a felhasználók, az elméleti tudás hosszútávú felidézése és a gyakorlati alkalmazás között milyen összefüggés figyelhető meg.
- Kifejezetten a társasjáték vonatkozásában, annak pozitív fogadtatása és biztonságtudatossági fejlesztésekben való hatékonysága megerősítette, hogy van létjogosultsága a disszertációban részletesen bemutatott továbbfejlesztési lehetőségeknek, a meglevő játék tökéletesítésének, illetve kiegészítőkkel való ellátásának, valamint specializáltabb (otthoni, illetve menedzsmentnek szóló) változatok kialakításának.

7. KAPCSOLÓDÓ SAJÁT PUBLIKÁCIÓK

OROSZI, Eszter Diána, *Információbiztonsági stratégia és vezetés*, EIV képzés tananyag (egyetemi jegyzet), 2014

OROSZI, Eszter, *A humán erőforrás védelme – védelem a humán erőforrás ellen* In. MUHA, Lajos – LEITOLD, Ferenc – SZÁDECZKY, Tamás – OROSZI, Eszter – SOM, Zoltán – LEITOLD, Ferenc (szerk.) Információ és adatvédelem a közigazgatásban, 2014, p. 27-37.

OROSZI, Eszter, *A biztonságtudatossági szint mérésének lehetőségei* In. GULYÁS, Éva – MARÓTI, Dávid – MÁTHÉ, Réka Zsuzsánna – SOMOGYI, Renáta – SŐREG, Krisztina – SZINAY, Ildikó (szerk.) Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Doktori Iskola 2014/15-ös Kutatói Fórumának tanulmánykötete, 2015, p. 169-183.

OROSZI, Eszter, LEITOLD, Ferenc, *Social Engineering methodologies – Identifying and analysing human risks* In. CEE eGov Days 2014 eGovernment: Driver or Stumbling Block for European Integration, 2014 Alexander Balthasar, Handrik Hansen, Balázs König, Robert Müller-Török, Johannes Pichler (Eds.) ISBN: 978-3-85403-300-4, p. 127-138.

OROSZI, Eszter Diána, *Kártékony programok terjedése social engineer szemmel* In. Dunakavics, 2015 III. Évfolyam VIII. szám, felelős szerkesztő: Dr. András István, ISSN: 2064-5007, p. 5-14.

LEITOLD, Ferenc, HADARICS, Kálmán, OROSZI, Eszter, GYŐRFFY, Krisztina, *Measuring the information security risk in an infrastructure* In. 2015 10th International Conference on Malicious and Unwanted Software (MALWARE), 2015, p. 93-100.

OROSZI, Eszter, GYŐRFFY, Krisztina, *Information Security for e-government social media marketing and citizen interaction* In. CEE eDem and eGov Days 2016, Multi-Level (e)Governance: Is ICT a means to enhance transparency and democracy, 2016, p. 225-236.

LEITOLD, Ferenc, ARROTT, Anthony, HADARCSI, Kálmán, OROSZI, Eszter, *Automating visibility into user behaviour vulnerabilities to malware attack* In. Virus Bulletin 2016, Proceedings of the 26th Virus Bulletin International Conference, VB 2016 Denver 5-7 October 2016 Martjin, Grooten (szerk.) p. 1-8.

OROSZI, Eszter Diána, *Social Engineering technikák* In. BODÓ, Attila Pál - OROSZI, Eszter Diána - SÁGI, Gábor János - SZAPPANOS, Gábor -SZARVÁK, Anikó - ZÁMBÓ,

Nóra - DEÁK, Veronika (szerk.) Célzott kibertámadások. Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában résztvevő személy számára, 2018, ISBN: 978-615-5870-52-1 p. 76-118.

OROSZI, Eszter Diána, *Security awareness escape room – a possible new method in improving security awareness of users* In. Cyber Science Cyber Situational Awareness for Predictive Insight and Deep Learning, C-MRiC.ORG, 2019 Onwubiko C., Bellekens X., Erola A., Jaatun M.G., Nogueira C. (Eds.) ISBN: 978-0-9932338-4-5"

OROSZI, Eszter Diána, *Biztonságtudatossági szabadulószoba, mint új programelem az információbiztonsági képzésekben* In. Dunakavics, 2020. VIII. Évfolyam III. szám, felelős szerkesztő: Dr. András István, ISSN: 2064-5007, p. 51-62.

OROSZI, Eszter Diána, *Social Engineering a koronavírus tükrében, avagy a rendkívüli helyzetet kihasználó támadási technikák és megelőzésük* In. Dunakavics, 2020. VIII. Évfolyam V. szám, felelős szerkesztő: Dr. András István, ISSN: 2064-5007, p. 51-62.

OROSZI, Eszter Diána, *Using gamification to improve security awareness level of users - Security awareness escape room as an effective and unique element of trainings* In. ISACA Journal Volume 4, 2020 (2020. July), Jannifer Hajigeorgiou (szerk.), ISSN 1944-1967

OROSZI, Eszter Diána, *Make Security Awareness an Experience,* ISACA Now Blog, 2020.09.25 (https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/make-security-awareness-an-experience, utolsó elérés: 2023.04.09)

OROSZI, Eszter Diána, *Exploitable Traits as Vulnerabilities: The Human Element in Security,* In. ISACA Journal Volume 5, 2021, Jannifer Hajigeorgiou (szerk.), ISSN 1944-1967, p.16-21

OROSZI, Eszter Diána, *Boardgames as Security Awareness Improvement Tools* In. HOF, Hans-Joachim – POPESCU, Manuela – FONGEN, Anders (szerk.) SECURWARE 2021 : The Fifteenth International Conference on Emerging Security Information, Systems and Technologies, 2021, p. 19-23.

OROSZI, Eszter Diána, *Patching Security Awareness: Human Traits as Vulnerabilities,* ISACA Now Blog, 2021.10.15 (https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/patching-security-awareness-human-traits-as-vulnerabilities, utolsó elérés: 2023.04.09)

LACZKÓ, Anikó, OROSZI, Eszter Diána, *Vigyázz – Kész - Rajt! Hamarosan indul a kibervédelmi hónap!* (tanulmány) https://silentsignal.hu/docs/S2_kibervedelmi_honap_kampanyelemek_tanulmany_20220805.pdf, utolsó elérés: 2023.03.26), 2022

OROSZI, Eszter Diána, *Taking a Risk-Based Approach to Pen Testing*, ISACA Industry News, 2022.10.24 (https://www.isaca.org/resources/news-and-trends/industry-news/2022/taking-a-risk-based-approach-to-pen-testing, utolsó elérés: 2023.04.09)

BARNA, Bianka Rita; KOLLÁR, Csaba; **OROSZI, Eszter Diána**: *A social engineering helye az információbiztonsági auditban.* In. Biztonságtudományi Szemle, 5. évfolyam, 1. szám (2023), ISSN 2676-9042, p. 25-41.

Előadások:

- *Social Engineering – amikor fellebben a fátyol*, Hacktivity 2011, Budapest, 2011.09.18
- *„Social Media Engineering", avagy játék határok nélkül?,* Ethical Hacking konferencia2014, Budapest, 2014.05.22
- *Magánélet és biztonság – avagy biztonságtudatosság a munkahelyen innen és túl...,* ITBN konferencia 2014, Budapest, 2014.09.24
- *Kibertámadások a kibertéren kívül – avagy a pokolba vezető út is jószándékkal van kikövezve*, HISEC konferencia 2014, Budapest, 2014.11.18
- *„Hacking with human" – avagy a pokolba vezető út is jószándékkal van kikövezve,* Ethical Hacking konferencia 2015, Budapest, 2015.05.08
- *Beléptető rendszerek biztonsága – Valós védelem vagy hamis biztonságérzet?,* Ethical Hacking 2016, Budapest, 2016.05.12
- *Kibertámadások a kibertéren kívül - A biztonságtudatosság szerepe és jelentősége a technológiai informatikai rendszerek elleni támadások kezelésében,* Védelem és irányítástechnikai fórum 2016, Velence, 2016.06.01
- *Biztonságtudatossági szabaduló szoba, mint a felhasználók biztonságtudatosságának új fejlesztési eszköze*, ISACA második szerdai előadás, Budapest, 2017.05.10
- *A „humán hackelés" művészete, avagy az emberi tényező, mint a biztonság leggyengébb láncszeme*, BM OKF konferencia 2017, Budapest, 2017.10.26
- *Kibertámadások a kibertéren túl, avagy az információbiztonság humán oldala*, Kihívások a nemzetbiztonságban konferencia 2017, Budapest, 2017.10.27

- *A biztonságtudatosság fejlesztésének új lehetőségei*, BM OKF konferencia 2018, Budapest, 2018.10.11
- *Social Engineering támadások megelőzése, avagy a tudatosítás lehetőségei munkahelyi környezetben*, Alkotmányvédelmi Hivatal, Awareness konferencia 2019, Budapest, 2019.03.06
- *Az információbiztonság humán faktora*, Nemzetközi Katonai Információbiztonsági Konferencia, 2019, Balatonkenese, 2019.05.23
- *A biztonság humán faktora, avagy az emberi tényező kihasználható tulajdonságai*, Alkotmányvédelmi Hivatal, Awareness konferencia 2020, Budapest, 2020.03.04
- *Biztonságtudatossági játékok, avagy a felhasználók információbiztonsági ismereteit fejlesztő módszerek hatékonyságának értékelése*, ISACA Második Szerda, 2022.01.12
- *A biztonság nem játék... de játszva fejleszthető!,* Hétpecsét Információvédelem Menedzselése CI. Szakmai Fórum, Budapest, 2022.05.18
- *Időutazás a Social Engineering auditok korában, avagy mi változott az elmúlt 10 év alatt?,* ISACA Konferencia 2022, Budapest, 2022.06.16.
- *Szirének hálójában – avagy hívószavak a szervezetet érintő információbiztonsági kockázatok (költség)hatékony kezeléséhez*, MLBKT Kongresszus 2022, Siófok, 2022.10.19
- *Szirének szigete - avagy tévutak és csábító lehetőségek a kockázatmenedzsmentben,* WITSEC Konferencia 2022, Budapest, 2022.10.26
- *Szirének hálójában - avagy a szervezetünket érintő információbiztonsági kockázatok teljeskörű feltérképezésének fontossága*, EIVOK-30 Tudományos – Szakmai Konferencia, Debrecen, 2022.11.03
- *Kárral szemben – Úton a SIREN fedélzetén,* Silent Signal Szakmai Nap, Budapest, 2023.03.28
- *Adataink őrzői – és a végtelen kockázatok,* ISACA Konferencia 2023, Budapest, 2023.06.01.

8. SZAKMAI ÖNÉLETRAJZ

Oroszi Eszter Diána 2009-ben végzett a Budapesti Corvinus Egyetem Gazdaságinformatikus BSc szakán, majd 2011-ben ugyanezen egyetem Gazdaságinformatikus MSc képzésén. Tanulmányai mellett 2008-ban először gyakornokként, majd információbiztonsági tanácsadóként csatlakozott a Kancellár.hu Zrt. csapatához. Már ekkor is kifejezetten érdekelte az emberi tényező biztonságtudatosságának mérése és fejlesztése, 2008-ban írt szakdolgozata a Social Engineering technikákat gyűjti össze és mutatja be részletesen, MSc-s diplomamunkája pedig a Social Engineering auditok módszertanát írja le.

Eszter 2014-ben nyert felvételt a Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Doktori Iskolába, ahol a korábban írt szakdolgozatokhoz illeszkedően a biztonságtudatosság fejlesztési lehetőségeinek kutatását tűzte ki célul. Kifejezett kutatási területe a biztonságtudatosság fejlesztése terén a gamifikáció alkalmazási lehetőségeinek vizsgálata, olyan módszerek feltárása és megalkotása, melyekkel a biztonságtudatossági szint hatékonyan, és a felhasználók számára élvezhető módon fejleszthető. 2014-ben Magyarországon először ő mutatta be az első, saját biztonságtudatossági szabadulószobát, melyet módszertanná alakított és azóta is folyamatosan fejleszt, 2022-ben pedig jelenlegi munkahelye, a Silent Signal Kft. támogatásával kiadásra került biztonságtudatossági társasjátéka, valamint szintén a nevéhez köthető a cég online biztonságtudatossági játékának megalkotása is.

Eszter a tanácsadói tevékenységen túl 6 éven keresztül belső információbiztonsági szakértőként is dolgozott mind állami, mind privát szférában működő nagyvállalatoknál, mely tapasztalatok a kutatói munkájához szintén nagymértékű segítséget nyújtottak. Emellett 2014 óta oktatója a Nemzeti Közszolgálati Egyetem Elektronikus információbiztonsági vezető szakirányú továbbképzésnek.

Jelenleg a Silent Signal Kft. információbiztonsági tanácsadás üzletágának vezetője.

Rendszeres előadója hazai szakmai konferenciáknak, valamint rendszeresen publikál nemzetközi szakmai kiadványokban is.