NEMZETI KÖZSZOLGÁLATI EGYETEM
Közigazgatás-tudományi Doktori Iskola

Oroszi Eszter Diána

A biztonságtudatossági szint fejlesztése gamifikációs módszerek alkalmazásával

Doktori (PhD) értekezés

Témavezető:

Dr. Leitold Ferenc, főiskolai tanár

……..

Budapest, 2023

TARTALOMJEGYZÉK

1. BEVEZETÉS

Disszertációm témájának a biztonságtudatossági szint mérési és fejlesztési módszereinek vizsgálatát választottam, mivel 2005 óta foglalkozom az emberi tényezőt kihasználó, Social Engineering támadások vizsgálatával, információbiztonsági auditok keretein belül történő szimulálásával, illetve a kapcsolódó biztonságtudatossági fejlesztésekkel. 2008-ban írt szakdolgozatom témája kifejezetten az emberi tényező sebezhetőségeinek és a Social Engineering módszereinek vizsgálata volt (Oroszi, 2008), 2011-ben, az MSc-s tanulmányaim lezárása során pedig szimulációs megoldásokkal, a biztonságtudatossági szint auditokon keresztül történő mérésével foglalkoztam (Oroszi, 2011). 2014-ben kidolgoztam a biztonságtudatossági szabadulószoba alkalmazásának lehetőségeit, melyet több rendezvényen mutattam be, illetve több szervezetnél szolgáltatásként alkalmaztam a felhasználók biztonságtudatossági ismereteinek növelésére, 2022-ben pedig saját fejlesztésű biztonságtudatossági társasjátékom került kiadásra *SILENT SIGNAL – A biztonságtudatossági játék* néven. Mindezek mellett részt vettem a Silent Signal Kft. Awareness Game online biztonságtudatosságot fejlesztő játékának szakmai fejlesztésében, valamint szakértői képzést dolgoztam ki a gamifikációs módszerek információbiztonsági környezetben való alkalmazásának támogatására (Oroszi, 2023).

Jelen disszertációban kifejezetten a felhasználók biztonságtudatossági szintjének a fejlesztésére fókuszálok, és az eddigi ismereteket összegzem, illetve kifejezetten az új megoldások bevezetésének vizsgálatával, a felhasználók hatékony tudatosításával foglalkozom.

1.1. A TÉMAVÁLASZTÁS INDOKOLTSÁGA

Ahogyan a mondás tartja, minden lánc olyan erős, mint a leggyengébb láncszeme, ez pedig az információbiztonságban maga az emberi tényező. A Verizon 2020-as Data Breach Investigation riportja szerint a sikeres támadások 67%-a emberi mulasztás és/vagy felhasználót érintő támadás (például adathalászat) miatt következik be (Verizon Data Breach Investigation Report, 2020), a PurpleSec 2020-as kiberbiztonsági riportjának statisztikái szerint pedig a kibertámadások 98%-a valamilyen Social Engineering technikán alapul (PurpleSec Cyber Security Statistics, 2020). De Pasquale (2023) statisztikái szerint a kibertámadások 2022-ben globálisan 38%-kal nőttek az előző évhez képest, és a szervezetek 83%-a érintett volt valamilyen incidensben. A Verizon 2022-es Data Breach Investigation Report-ja szerint támadásoknak már 82%-a az emberi tényezőre volt visszavezethető, például adathalászatra,

egyéb módon megszerzett azonosító adatokra, nem megfelelő használatra. (Verizon Dta Breach Investigation Report, 2022) Az ENISA Threat Landscape 2022 kiadványa a zsarolóvírusok és kártékony kódok mellett 3. helyen listázza a Social Engineering támadásokat is (ENISA Threat Landscape, 2022). Bár jelen disszertációban a továbbiakban is mutatok be statisztikát a felhasználókat érintő támadásokkal kapcsolatban, az igazság azonban az, hogy vannak valós Social Engineering technikát alkalmazó visszaélések, melyek azonban soha nem derülnek ki, ezért pontos statisztika készítése gyakorlatilag lehetetlen. Ennek egyik oka lehet, hogy nem is tud róla a felhasználó, hogy támadás áldozatává vált (például egy telefonon keresztüli sikeres megtévesztésnél érzékeny információt adott ki, melyet más támadáshoz felhasználtak), másrészt az áldozatul esett munkavállalók gyakran nem vallják be tévedésüket, elhallgatják az őket ért támadásokat - ezek különösen az IT rendszereket mellőző technikák alkalmazása során veszélyesek, melyek esetében nem segítenek riasztások és logbejegyzések az események észlelésében, kivizsgálásában. Tapasztalataim alapján mind a valós, mind a Social Engineering auditok során végrehajtott támadások igen kevés áldozata jelenti be az incidenst (és itt az auditok során most kifejezetten azokra gondolok, akik áldozattá is válnak). Ennek oka egyrészt, hogy lehet, nem is tud róla a felhasználó, hogy incidens áldozata, másrészt aki rákattint valamilyen kártékony kódot tartalmazó oldalra irányító linkre, és gyanús tartalmakat engedélyez, vagy megadja az adatait egy adathalász felületen, netán más furcsa eseménnyel találkozik, jellemzően inkább csak akkor vallja be azt, ha már úgy érzi, az esetnek rá nézve, akár személyes érintettséggel is negatív következményei lehetnek, illetve a történtek kiderülése elkerülhetetlen. Nagyon fontos tehát, hogy igazából sosem tudhatjuk, hogy valójában mennyire ellenállóak a munkatársaink az emberi tényezőt kihasználó fenyegetésekkel szemben, ez azonban nem jelenti azt, hogy nem szükséges tisztában lennünk az emberi tényező jelentette kockázatokkal és a munkatársak biztonságtudatossági ismereteinek aktuális szintjével. Az ezek vizsgálatára irányuló auditok egyfajta pillanatképet adnak, melyek jó kiindulási alapot jelentenek a biztonságtudatosság célirányos fejlesztéséhez. Sőt, napjainkban már maguk az ilyen jellegű tesztek, például adathalász szimulációk is az „oktatás” részét képezik és bevett tudatosító megoldásnak számítanak. A gyakorlatias megközelítés nem csak a biztonságtudatossági szint mérése során hatékony megoldás, hanem a felhasználók képzése, információbiztonsági oktatása esetében is. Ezt támogatják a napjainkban oly népszerű gamifikációs, másnéven játékosítást alkalmazó biztonságtudatosság-fejlesztő megoldások is, melynek 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 adatbázisban. 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. Mindezen okokból kifolyólag jelen értekezésben célul tűztem ki a gamifikációs módszerek biztonságtudatossági képzésekben való alkalmazhatóságának és hatékonyságának vizsgálatát.

1.1.1. KÖZIGAZGATÁSI KAPCSOLÓDÁS

Információbiztonsági kockázatokban minden szervezet érintett – nem képeznek ez alól kivételt a közigazgatási szervek, illetve az állami szféra egyéb szervezetei sem. Ahogyan Beláz (2019) fogalmaz „*az átlagos polgárok – a híroldalak és közösségi média platformok böngészésén túl, – egyre gyakrabban mobilkészülékeiken, okos eszközeiken keresztül intézik közigazgatási hatósági ügyeiket. A közigazgatás modernizációjával, digitalizálódásával azonban együtt kell járnia annak, hogy növeljük az információs rendszerek megbízhatóságát és az információbiztonsági események elleni védekező képességét.*” (Beláz, 2019, p. 92.)

Khando és szerzőtársai (2021) szakirodalom kutatásuk során szintén azt állapították meg, hogy 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.

Irwin (2023) az IT Governance kutatásában kiemeli, hogy a közszféra a harmadik legtöbb kiberbiztonsági incidens által érintett szektor 2022-ben. Legárd (2023) 2019 és 2021 között vizsgálta a hazai állami és önkormányzati szervek incidenseit, melyek – ugyan csökkenő trendet mutatnak, de – 4%-a Social Engineering jellegű támadásra, 6%-a pedig a szorosan kapcsolódó spam-re volt visszavezethető. Legárd (2023) az NKI adatait vizsgálva a pszichológiai manipuláció, a megszemélyesítés és az információgyűjtés összesített arányát a vizsgált időszakban 23%-ra állapította meg.

Fentiek miatt elengedhetetlen a közszféra szervezeteinek információbiztonsági fejlesztése, melynek a munkavállalók biztonságtudatossági oktatása elengedhetetlen része. A későbbiekben bemutatott, információbiztonsági relevanciájú hazai jogszabályok, illetve ajánlások mindegyike előírja a felhasználók információbiztonsági oktatásának szükségességét.

Az információbiztonsági relevanciájú képzésekhez több szervezet is támogatást nyújt: a Közigazgatási Továbbképzési Intézet Pro Bono felületén (https://eib.uni-nke.hu/, utolsó elérés:

2023.06.23.) rendszeresen jelennek meg új, aktuális információbiztonsági képzések, a Szabályozott Tevékenységek Felügyeleti Hatósága pedig 2023. május 31-i, Híd a kibertér biztonságáért nevű konferenciáján elhangzottak szerint ENISA partnerként biztonságtudatossági kampányokkal, például az AR-in-a-Box játékkal támogatja a hozzá forduló szervezeteket.

1.1.2. A TUDOMÁNYOS PROBLÉMA MEGFOGALMAZÁSA

A szervezet elsődleges védvonalát az információbiztonsági támadásokkal szemben annak munkavállalói jelentik. Ahogyan a statisztikák is rávilágítanak, a humán faktor kihasználása gyakori – és sikeres – eszköze a támadóknak. Az emberi tényezőt kihasználó támadásoknak számtalan technikája létezik, ezen módszereket nemzetközi szerzők (például Harl, 1997; Mitnick, 2003; Mann, 2008; Long, 2008; Hadnagy, 2011) mellett több hazai szakértő is részletesen bemutatta tanulmányaiban, és megalapozta, hogy a Social Engineering módszerek valós fenyegetést jelentenek a szervezeteknek (például Bányász és szerzőtársai, 2019; Deák, 2017; Deák, 2019; Kollár és Zakar, 2020; Oroszi, 2008; Oroszi, 2014; Oroszi, 2015; Oroszi, 2018; Oroszi, 2020b). Ezen támadási technikák folyamatosan fejlődnek és egyre újabbak jelennek meg. Sadiq és szerzőtársai (2021) publikációjukban az adathalász támadások típusait mutatják be, kiegészítve az új trendekkel, Alhabri és szerzőtársai (2022) pedig kifejezetten a social médiához kapcsolódó phishing támadásokkal foglalkoznak.

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.

A bevezetésben taglalt, a humán faktort kihasználó támadások statisztikái miatt elmondható, hogy a legfontosabb a munkavállalók biztonságtudatossági szintjének folyamatos fejlesztése és a korábbi ismeretek szinten tartása, mely azonban nem triviális feladat, és jóval túlmutat egy évente egyszer meghirdetett, sok esetben pusztán e-Learning keretein belül megvalósított oktatáson, és néhány, a legfontosabb ismereteket hangsúlyozó plakát kihelyezésén. Tapasztalataim alapján érdekeltté kell tenni a felhasználókat a biztonságtudatos magatartás gyakorlásában mind a munkahelyen, mind a magánéletben, és fel kell hívni a figyelmüket a kihasználható tulajdonságaikra, szituációkra és támadási technikákra, hiszen minden ember kihasználható – kérdés, hogy mennyi idő- és energia-ráfordításra van szüksége ehhez a támadónak. Kifejezetten fontosnak tartom, hogy a különböző képzések célja ne pusztán

szabályok bemagoltatása és a támadási technikák ismertetése legyen (bár tény, hogy ezek is nagyon fontosak), hanem a biztonságtudatos szemléletmód kialakítása, melynek köszönhetően a felhasználó azon gyanús eseményeket is fel tudja ismerni és hatékonyan kezelni tudja, melyek újonnan megjelent ártó szándékú megkeresések, aktualitásokra épülő, eddig nem ismert forgatókönyveket alkalmazó módszerek.

A szemléletmód kialakítását és a gyakorlat elsajátítását kiemelten fontos hangsúlyozni, hiszen az összes megkeresési lehetőségre, minden, a felhasználókat érintő támadási módszerekre nem lehet felkészíteni a munkavállalókat, tekintve, hogy az alkalmazott módszerek, technikák, forgatókönyvek folyamatosan változnak, egyre kifinomultabbak lesznek. A bemagolt „*ha ezt tapasztalod, akkor azt nem szabad tenni*" jellegű szabályok a mai világban már nem elegendőek.

Figyelembe véve pedig, hogy a munkavállalók jelenthetik a szervezet elsődleges védvonalát a különböző támadási technikákkal szemben, nagyon fontos, hogy képzésük, érzékenyítésük megfelelő módszerekkel történjen.

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 vizsgálom 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 (például Khan és szerzőtársai, 2011; Abawajy, 2014; Tschakert és Ngamsuriyaroj, 2019; Legárd, 2020), és eredményeik azt mutatják, érdemes tovább vizsgálni a témát, hiszen ahogyan Abawajy (2014), valamint Tschakert és Ngamsuriyaroj (2019) is bizonyította, a preferált megoldások a gyakorlatban még nem 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.

1.1.3. A TÉMA IDŐSZERŰSÉGE, AKTUALITÁSA

Az elmúlt években olyan változások történtek a világban, melyek minden szervezet életére hatással voltak – ezáltal azok információbiztonsági fenyegetettségére is. Az új szituációk nem csak a támadási technikákra, de a védekezési módszerekre is hatással voltak, így a biztonságtudatossági fejlesztésekre, valamint azok hatékonyságára is.

Disszertációm megírásakor, 2023-at írva az emberi tényező biztonságtudatosságának fejlesztése különösen aktuális, hiszen folyamatosan újabb eszközök, alkalmazások, és ezáltal támadási technikák jelennek meg, melyeket a potenciális támadók általában hamarabb lekövetnek, mint a biztonságért felelős munkatársak. Mindezek miatt kifejezetten fontosnak tartom a képzések, kampányok során olyan módszerek alkalmazását, melyek igazodnak a kor követelményeihez és a felhasználók igényeihez, a munkavállalók képességeihez, aktuális biztonságtudatossági ismereteihez, illetve hatékonyan rá tudnak mutatni arra, miért is fontos a biztonságtudatosság és mi az emberi tényező szerepe a biztonságtudatosságban.

Ahogyan a világ, illetve az emberi tényezőt érintő fenyegetések is változnak, elengedhetetlen, hogy az oktatási módszerek is kövessék a legújabb trendeket. Tapasztalataim alapján azonban még mindig az előadások és a különböző e-Learning tananyagok a leginkább elterjedt oktatási megoldások, főleg, hogy ezek az online térben is működőképesek. Az online oktatás és kapcsolattartás, melynek előnyeit és hátrányait szükségszerűen megtapasztaltuk a 2020-as COVID-19 világjárvány alatt, mai napig megosztó a munkavállalók és munkáltatók körében. Vannak, akik üdvözítik a változásokat és preferálják az online térben rejlő lehetőségeket, míg mások egyenesen betiltják, vagy legalábbis kerülik a távoli munkavégzés intézményét. Ezen

változások természetesen a biztonságtudatossági fejlesztésekre is hatással vannak, nem csak tartalmi elemek (például, mely támadási technikák jellemzőek inkább az online munkavégzés során), de megközelítés szempontjából is (például egy biztonságtudatossági szabadulószobát távolról nem, vagy online játékká történő alakítást követően sem lehet olyan hatékonyan megvalósítani). Nem szabad arról sem megfeledkezni, hogy az online térbe való költözésnek sokszor anyagi vonzata van, és ezen beruházások esetében az információbiztonsági képzések általában hátrányba kerülnek az alaptevékenységeket kiszolgáló fejlesztésekkel szemben.
A disszertációban szintén rá kívánok mutatni arra, hogy a hagyományos tudatosítási módszerek a mai világban elavultnak tekinthetők, a felhasználók igénylik a személyes, tapasztalati úton történő tanulást. Ezért sokkal hatékonyabb, ha a célközönség átéli a szituációt, ezáltal jobban rögzülnek a biztonságtudatossági ismeretek, illetve könnyebben elsajátításra kerülhet a biztonságtudatos szemléletmód, ha gyakorlati elemeket csempészünk a képzésekbe, melynek egyik módja a játékosítás alkalmazása. Ahogyan a szakirodalom feltárása során azonosítottam, a különféle gamifikációs módszerek hazánkban is kezdenek egyre népszerűbbé válni munkahelyi környezetben, a világban pedig már bevett gyakorlatnak számítanak, a szervezetek felismerték és kihasználják ezek előnyeit – egyre inkább a biztonság, illetve a biztonságtudatosság fokozása terén is.

1.2. MEGKÖZELÍTÉS ÉS VIZSGÁLT HIPOTÉZISEK

A fent bemutatott problémákból kifolyólag 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 ismeretbővülését (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 hipotézist határoztam meg és mutatom be, valamint vizsgálom részletesen a disszertáció további fejezeteiben.

1.2.1. A BIZTONSÁGTUDATOSSÁG FEJLESZTÉSI MÓDSZEREK HATÉKONYSÁGA A FELHASZNÁLÓI ÉLMÉNY TÜKRÉBEN

1.2.1.1. 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.”

Ezen hipotézis igazolására vagy cáfolására a 3. fejezetben bemutatott kutatást folytattam 5 db Magyarországon elhelyezkedő, privát szektorban működő, illetve 5 db, szintén hazai állami szervezetnél, melynek során hat különböző módszer hatékonyságát vizsgáltam abból a szempontból, hogy melyik milyen mértékben bővíti a résztvevők információbiztonsági ismereteit, ezáltal feltételezhetően fejlesztve a biztonságtudatosságukat. A vizsgálat során értékelési szempont volt a különböző módszerek hatékonyságának összehasonlítása mellett az is, hogy a felhasználók mennyire preferálják az adott programot, valamint mennyire tartják élvezetesnek (*élmény-index*), illetve hasznosnak (*hasznosság-index*) az egyes programokat, és ennek milyen hatása van a biztonságtudatossági ismeretek bővülésére (*átlagos új ismeretszám*), vagy a biztonságtudatos felhasználók számának növelésére (*legalább egy új ismeretet szerző résztvevő felhasználók aránya*). A vizsgálat során azt igazoltam, hogy a felhasználók által értékelt preferencia, felhasználói élmény, valamint a hasznosság-érzet közül legnagyobb hatással a felhasználói élmény van a biztonságtudatossági szint fokozására, valamint a biztonságtudatosabb felhasználók számának növelésére.

1.2.1.2. Kapcsolódó új fejlesztés

A hipotézis igazoláshoz kifejlesztettem egy gyakorlati felmérési módszertant a biztonságtudatosságot fejlesztő módszerek hatékonyságának összehasonlítására, melyet a 3. fejezetben mutatok be.

1.2.1.3. Elérni kívánt tudományos eredmény

A vizsgálattal célom annak bizonyítása, 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.

1.2.2. A GAMIFIKÁCIÓ ALKALMAZHATÓSÁGA A FELHASZNÁLÓK BIZTONSÁGTUDATOSSÁGI ISMERETEINEK BŐVÍTÉSÉRE

1.2.2.1. 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 igazolására vagy cáfolására az előző pontban alkalmazott kutatás eredményeit használatam fel, melynek során hat különböző, köztük két gamifikációs módszer élvezetességét és hatékonyságát vizsgáltam abból a szempontból, hogy melyiknek milyen hatása van a biztonságtudatossági ismeretek bővülésére (*átlagos új ismeretszám*), vagy a biztonságtudatos felhasználók számának növelésére (*legalább egy új ismeretet szerző résztvevő felhasználók aránya*). Az eredményeket a disszertáció 4. fejezete mutatja be.

1.2.2.2. Kapcsolódó új fejlesztés

A hipotézis igazoláshoz kifejlesztettem egy gyakorlati felmérési módszertant a biztonságtudatosságot fejlesztő módszerek hatékonyságának összehasonlítására, melyet a 3. fejezetben mutatok be.

1.2.2.3. Elérni kívánt tudományos eredmény

A vizsgálattal célom annak bizonyítása, hogy a gamifikációs módszerek képesek a biztonságtudatossági szint fejlesztésére mind az ismeretek bővítése, mind a biztonságtudatosabb felhasználók számának növelése szempontjából.

1.2.3. A BIZTONSÁGTUDATOSSÁGI SZABADULÓSZOBA ALKALMAZHATÓSÁGA A FELHASZNÁLÓK BIZTONSÁGTUDATOSSÁGI ISMERETEINEK BŐVÍTÉSÉRE

1.2.3.1. 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 hipotézis igazolására vagy cáfolására szintén az első hipotézishez készített kutatást használtam fel, melynek során hat különböző, biztonságtudatosságot fejlesztő módszert, köztük az általam 2014-ben fejlesztett biztonságtudatossági szabadulószoba hatékonyságát vizsgáltam abból a szempontból, hogy melyiknek milyen hatása van a biztonságtudatossági ismeretek bővülésére (*átlagos új ismeretszám*), vagy a biztonságtudatos felhasználók számának növelésére (*legalább egy új ismeretet szerző résztvevő felhasználók aránya*). Az általam fejlesztett biztonságtudatossági szabadulószobát, valamint a vizsgálat eredményeit a disszertáció 5. fejezete mutatja be.

1.2.3.2. Kapcsolódó új fejlesztés

A saját fejlesztésű biztonságtudatossági szabadulószoba módszertanának kialakítása 2014-ben.

1.2.3.3. Elérni kívánt tudományos eredmény

A vizsgálat során célom annak bizonyítása, hogy az általam 2014-ben fejlesztett biztonságtudatossági szabadulószoba képes a biztonságtudatossági szint fejlesztésére mind az ismeretek bővítése, mind a biztonságtudatosabb felhasználók számának növelése szempontjából.

1.2.4. A BIZTONSÁGTUDATOSSÁGI TÁRSASJÁTÉK ALKALMAZHATÓSÁGA A FELHASZNÁLÓK BIZTONSÁGTUDATOSSÁGI ISMERETEINEK BŐVÍTÉSÉRE

1.2.4.1. 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 hipotézis igazolására vagy cáfolására szintén az első hipotézishez készített kutatást használtam fel, melynek során hat különböző biztonságtudatosságot fejlesztő módszert, köztük az általam 2021-2022-ben fejlesztett biztonságtudatossági társasjáték hatékonyságát vizsgáltam abból a szempontból, hogy melyiknek milyen hatása van a biztonságtudatossági ismeretek bővülésére (*átlagos új ismeretszám*), vagy a biztonságtudatos felhasználók számának növelésére (*legalább egy új ismeretet szerző résztvevő felhasználók aránya*). Az általam fejlesztett biztonságtudatossági társasjátékot, valamint a vizsgálat eredményeit a disszertáció 6. fejezete mutatja be.

1.2.4.2. Kapcsolódó új fejlesztés

„*SILENT SIGNAL – A biztonságtudatossági játék*" című, a felhasználók biztonságtudatossági ismereteit fejlesztő kooperációs-stratégiai társasjáték megalkotása 2021-ben és kiadása 2022-ben.

1.2.4.3. Elérni kívánt tudományos eredmény

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.

1.3. ALKALMAZOTT MÓDSZEREK ÉS MEGKÖZELÍTÉS

Ahhoz, hogy a fent bemutatott hipotéziseket igazoljam, vagy cáfoljam, 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. Az alábbi alpontokban ezeket mutatom be röviden.

1.3.1. SZAKIRODALOM FELTÁRÁS

A disszertáció elkészítésének első lépéseként szakirodalom feltárást folytattam, melynek során a rendelkezésemre álló nemzetközi és hazai publikációk tanulmányozása mellett egyaránt kitértem a felhasználók biztonságtudatosságának fejlesztését előíró nemzetközi és hazai szabályozás vizsgálatára is.

A szakirodalom feltárás fő fókuszában a kutatásomhoz illeszkedően a biztonságtudatosság fejlesztés lehetséges módszerei, az ezekkel kapcsolatos külső és szervezeti (belső) követelmények, valamint a gamifikációs megoldások és azok alkalmazhatóságának vizsgálata álltak. A szakirodalom feltárás eredményeit saját kutatási célom meghatározásában, valamint annak összeállításában használtam fel.

A szakirodalom feltárás eredményeit jelen disszertáció 2. fejezetében mutatom be.

1.3.2. SAJÁT FELMÉRÉSEK

Az elérhető szakirodalmak és szabályozások vizsgálatán túl nagy hangsúlyt fektettem a saját felmérések végrehajtására is. Első körben kifejezetten a biztonságtudatossági szabadulószobában 2016 és 2019 között résztvevő felhasználókkal töltettem ki kérdőívet a játékkal kapcsolatban. A kérdőíves felmérés eredményeit 2019-ben publikáltam az Oxfordban rendezett Cyber Science konferencián. (Oroszi, 2019) Ezt követően kifejezetten ezen disszertációhoz készült, a biztonságtudatosságot fejlesztő módszerek hatékonyságát vizsgáló kutatást folytattam le 2021. augusztus 31. és 2023. április 6. között, mely rövid és hosszútávon egyaránt mérte a felhasználók biztonságtudatossági ismereteinek bővítését a kutatás során alkalmazott programokon való részvételt követően.

Disszertációmban az első, kifejezetten a biztonságtudatossági szabadulószobára vonatkozó felmérés az 5., a második, az egyes módszerek összehasonlítását célzó vizsgálatot pedig a 3. fejezetben mutatom be. A részletes eredményeket a vonatkozó fejezetekben ismertetem.

Ezek mellett, ahol rendelkezésemre állt, saját kiegészítő felmérések eredményeit is bemutatom.

1.3.3. SZEMÉLYES TAPASZTALATGYŰJTÉS

Tekintve, hogy a munkám során az alkalmazott biztonságtudatosság fejlesztési módszerek mindegyikét aktívan használom, elengedhetetlennek tartom, hogy mind az ezekből, mind a kutatás során végrehajtott gyakorlati programelemekből származó tapasztalatokat és azokból levont következeteseket is megosszam jelen disszertációban, melyeket – ahol lehet – a felmérésből származó statisztikai adatokkal is alátámasztok.

1.3.4. A DISSZERTÁCIÓHOZ KÉSZÜLT KUTATÁS HATÓKÖRE, LIMITÁCIÓI

A disszertációhoz kapcsolódó kutatás során a célom kifejezetten annak vizsgálata volt, hogy a különböző, általam kiválasztott hat biztonságtudatosság fejlesztési módszer hogyan bővíti a munkavállalók biztonságtudatossági ismereteit a szintén általam előzetesen kiválasztott 10 ismeret-kategóriában, ezáltal feltételezhetően fejlesztve a biztonságtudatosságukat. Mindezekből kifolyólag az alábbi limitációkkal élek.

1.3.4.1. A kapcsolódó kutatás célcsoportja

Jelen kutatásba kizárólag Magyarországon, azon belül is Budapesten vagy megyeszékhelyen elhelyezkedő szervezeteket vontam be, melyek legalább 30 fő munkavállalóval rendelkeznek (ez nem zárja ki a vizsgált módszerek kisebb méretű szervezeteknél való alkalmazhatóságát, viszont az összehasonlíthatóság érdekében csak olyan szervezeteket vonhattam be, melyeknél a létszám meghaladta a kutatáshoz minimálisan szükséges 30 főt).

A kutatásban résztvevő munkavállalókkal kapcsolatban nem alkalmaztam olyan megkötéseket, mint

- nemre, korra, pozícióra vonatkozó elvárások,
- önkéntes jelentkezés vagy delegálás elvárása,
- előző biztonságtudatossági oktatáson való részvétellel, vagy annak hiányával kapcsolatos elvárások.

Egyedül a következő, nem kötelezően kikényszerített preferenciákat támasztottam a szervezetekkel és résztvevőkkel szemben:

- a szervezet elsőlegesen ne a biztonsági terület munkavállalóit delegálja a felmérésbe,
- a résztvevők ne közvetlenül a kutatási program előtt részesüljenek más jellegű biztonságtudatossági oktatásban.

1.3.4.2. Kizárólag a biztonságtudatossági ismeretek számának bővülését veszem figyelembe, a tényleges magatartást nem vizsgálom

Jelen vizsgálat nem terjedt ki arra, hogy a felhasználók tényleges biztonságtudatossági szintjét vizsgáljam az egyes programokon való részvétel előtt, illetve után, például szimulációs módszerek, gyakorlati vizsgálatok vagy Social Engineering audit keretein belül. A minta nagyságát tekintve (300 fő) kizárólag a kérdőív keretein belül adott válaszok alapján mérhettem fel jelenlegi ismereteket, azok tényleges és helyes alkalmazását nem teszteltem.

A kérdőíves felmérés során az ismeretekre vonatkozóan viszont szabadszöveges válaszadást kértem, mellyel csökkentettem annak kockázatát, hogy egy listából választva olyan ismereteket is bejelöljenek a válaszadók egy potenciálisan jobbnak vélt eredmény elérése érdekében, melyet ténylegesen nem, vagy nem olyan mélységben ismernek. Ezáltal olyan tudáselemeket sikerült azonosítanom, melyeket a felhasználók nagyobb valószínűséggel ténylegesen alkalmaznak a mindennapokban. Annak kockázatát, hogy az előzetes kérdőíven bizonyos ismeretek nem jutnak eszébe a kitöltőnek, elhanyagolhatónak ítéltem, hiszen ezeket a második kérdőíven, felelevenítést követően rögzíteni tudják, kontrollként pedig az utolsó, egy hónappal későbbi kérdőívben szintén megjelenhetnek.

1.3.4.3. Kifejezetten csak az előzetesen kiválasztott hat módszer hatékonyságát vizsgálom

Jelen kutatás kifejezetten csak hat, általam választott biztonságtudatossági fejlesztési módszerre korlátozódott, melyek kiválasztása az alábbi szempontok szerint történt:

- a kiválasztott módszerek fele igényeljen mindenképpen személyes jelenlétet,
- a kiválasztott módszerek harmada tisztán gamifikációs elem legyen,
- a kiválasztott módszerek minden szervezetnél megvalósíthatóak legyenek, speciális tudás és a szervezet részéről igényelt erőforrás, külön beruházás ne legyen szükséges az alkalmazhatósághoz (ezáltal az online játékot és a mobilapplikációt kizártam),
- a kiválasztott módszerek mindegyike limitálható, de értelmesen végrehajtható legyen egy fél órás időkeretben (ezáltal a különböző pontgyűjtő akciókat, versenyeket kizártam).

Ezen korlátozásokkal biztosítottam, hogy a végrehajtott kutatás minden szervezetre értelmezhető legyen, ugyanakkor bármilyen más szervezetnél, eltérő módszerek bevonásával megismételhető legyen.

1.3.4.4. Kifejezetten csak az előzetesen kiválasztott tíz biztonságtudatossági ismeret meglétét értékelem

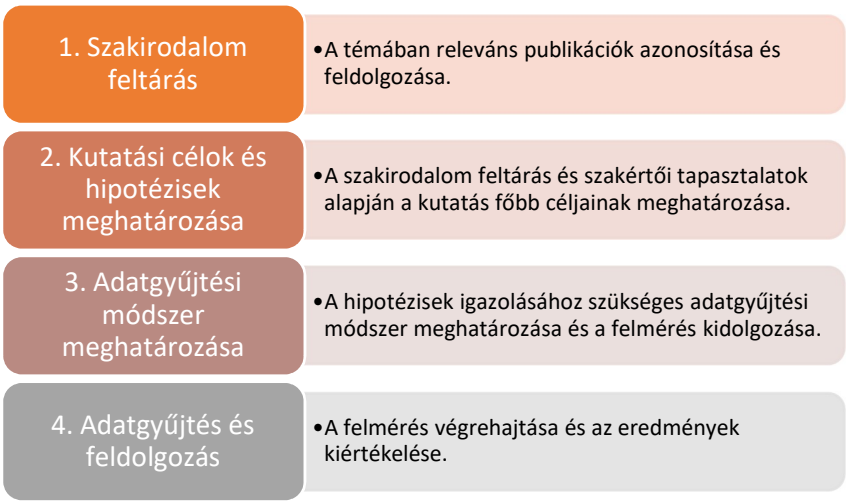
Jelen kutatás során azt tűztem ki célul, hogy olyan tíz darab biztonságtudatossági ismeretek meglétét vagy hiányát azonosítsam, melyek általánosságban megjelennek a biztonságtudatossági oktatások alkalmával. Mindezek érdekében az alábbi szempontok alapján választottam ki a vizsgált ismereteket:

- a vizsgált ismeretek fele számítógépen keresztüli, másik fele számítógépet mellőző támadási technikák megelőzésére szolgáljon,
- egy ismeret csak egyszer szerepeljen, egyik se kerüljön alsóbb rendű kategóriákra bontásra (például jelszavak esetében),
- egyik ismeret se tartozzon szándékosan a kutatásban résztvevő szervezetek célirányos fejlesztési igényeihez,
- mindegyik ismeret megjeleníthető legyen minden, a kutatásba bevont fejlesztési módszer során.

Ezen korlátozásokkal biztosítottam, hogy a végrehajtott kutatás minden szervezetre értelmezhető legyen, ugyanakkor bármilyen más szervezetnél, eltérő biztonságtudatossági ismeretek bevonásával megismételhető legyen.

1.3.5. A KUTATÁSI MÓDSZERTAN BEMUTATÁSA ÉS A DISSZERTÁCIÓ FELÉPÍTÉSE

A disszertációhoz készített kutatást az 1. ábrán bemutatott lépések szerint hajtottam végre:



1. ábra: A kutatási folyamat lépései (forrás: saját szerkesztés)

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

Disszertációmat a fent rögzített kutatási lépések, illetve hipotézisek mentén 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. (Kapcsolódó kutatási szakasz: 1. Szakirodalom feltárás és 2. Kutatási célok és hipotézisek meghatározása.)
- **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. (Kapcsolódó kutatási szakasz: 3. Adatgyűjtési módszer meghatározása és 4. Adatgyűjtés és feldolgozás.)
- **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. (Kapcsolódó kutatási szakasz: 4. Adatgyűjtés és feldolgozás.)
- **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. (Kapcsolódó kutatási szakasz: 4. Adatgyűjtés és feldolgozás.)

- **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. (Kapcsolódó kutatási szakasz: 4. Adatgyűjtés és feldolgozás.)
- **7. fejezet**: *Összegzés*, melyben összefoglalom a kapcsolódó kutatás eredményeit és következtetéseit, valamint a készített módszertanok és eszközök további felhasználási és bővítési lehetőségeit.

Az értékezés végén a kötelező mellékleteket és hivatkozásokat listáztam.

2. SZAKIRODALOM ÁTTEKINTÉS

2.1. A SZAKIRODALOM FELTÁRÁS MÓDSZERTANA

A disszertáció elkészítésének első lépéseként feltártam a biztonságtudatosság fejlesztéséhez kapcsolódó szakirodalmat, melynek során a következőket vizsgáltam:

- A biztonságtudatosság fejlesztésének szükségessége, követelményei a Magyarországon működő szervezetek vonatkozásában.
- A biztonságtudatosság fejlesztésének lehetőségei, hagyományos módszerei, azok alkalmazása és korlátjai.
- A jelenleg elérhető gamifikációs módszerek és azok alkalmazhatósága, kiemelten a biztonságtudatossági szabadulószoba és a biztonságtudatossági társasjátékok terén.
- A fentiekhez kapcsolódó, jelenleg rendelkezésre álló értékelések a felhasználói élmény és hatékonyság szempontjából.

A szakirodalom feltárást a következő lépések mentén hajtottam végre:

1. Összegyűjtöttem a lehetséges dokumentum típusokat, forrásanyag-típusokat.
2. Azonosítottam a potenciális forrásokat, publikációs oldalakat.
3. Feltártam a kulcs-szakirodalmat, jelentősebb szerzőket.
4. Felhasználtam a feltárt kulcs-szakirodalmak hivatkozás-jegyzékét további források azonosítására.
5. Felhasználtam a feltárt kulcs-szakirodalmakra való hivatkozásokat.

A szakirodalom áttekintéséhez az alábbi jellegű dokumentumokat, forrásanyagokat tártam fel és használtam a későbbiek során:

- Jogszabályok
- Szabványok
- Ajánlások
- Szakcikkek
- Tudományos publikációk
- Tudományos és szakmai konferencia kiadványok
- A piacon elérhető, kapcsolódó szolgáltatások és termékek leírásai

Ezek feltárására elsődleges, de nem kizárólagos forrásként olyan oldalakat használtam fel, mint

- academia.edu,
- cisa.gov,

- elsevier.com
- enisa.europa.eu,
- isaca.org,
- iso.org,
- ludovika.hu
- net.jogtar.hu,
- nist.gov,
- nki.gov.hu,
- mtmt.hu
- researchgate.net,
- sans.org,
- scholar.google.com,
- scopus.com
- sztfh.hu,

Fentiek között tudományos folyóiratok feltárására az MTMT Journal Search funkcióját használtam a következő területekre vonatkozóan:

- Computer Science
- Control and System Engineering
- Education
- Information Systems and Management
- Safety, Risk, Reliability and Quality

Hazai tudományos publikációk és szakmai folyóiratok terén pedig elsődlegesen, de nem kizárólagosan a következőket vettem figyelembe (ezek utolsó elérése: 2023.03.26):

- AARMS – Academic and Applied Research in Military and Public Management Science (https://folyoirat.ludovika.hu/index.php/aarms)
- Biztonságtudományi Szemle (https://biztonsagtudomanyi.szemle.uni-obuda.hu)
- Hadmérnök (https://folyoirat.ludovika.hu/index.php/hadmernok)
- Nemzetbiztonsági Szemle (https://folyoirat.ludovika.hu/index.php/nbsz)
- Nemzet és Biztonság – Biztonságpolitikai Szemle (https://folyoirat.ludovika.hu/index.php/neb)
- Pro Publico Bono – Public Administration (https://folyoirat.ludovika.hu/index.php/ppbmk)

Nemzetközi tudományos publikációk és szakmai folyóiratok terén pedig elsődlegesen, de nem kizárólagosan a következőket vettem figyelembe (ezek utolsó elérése: 2023.06.23.):

- IEEE kiadványok (https://www.ieee.org/)
- IGI Global kiadványok (https://www.igi-global.com/)
- ISACA Journal (https://www.isaca.org/resources/isaca-journal)

A tudományos és szakmai publikációk feltárásához használt főbb kereső kifejezéseim, kulcsszavaim elsődlegesen, de nem kizárólagosan a következők voltak mind magyar, mind angol nyelven (csak az angol feltüntetésével):

- information security, IT security, cybersecurity
- awarness, security awareness, information security awareness
- Social Engineering, human factor, user, end-user, employee
- improvement, education, training, methods, actions
- campaign, program
- gamification, serious game, GBL
- escape room, exit room, boardgame, card game, online game, video game
- measuring security awareness level, simulated attack

2.2. FOGALMI KERETEK, LEGFONTOSABB ALAPFOGALMAK

A feltárt szakirodalom elemzésének bemutatása előtt a disszertáció témájához kapcsolódó legfontosabb négy fogalmat gyűjtöttem össze és határozom meg az alábbiakban.

2.2.1. EMBERI TÉNYEZŐ (HUMAN FACTOR)

Az emberi tényezőt, vagy más néven humán faktort sokszor a biztonság leggyengébb láncszemeként aposztrofálják (Schneier, 2000; Oroszi, 2008; Jain 2016). Kobis (2021) úgy határozza meg az emberi tényezőt, mint a viselkedés, tudás, tapasztalat és kompetenciák, valamint szándékok összessége.

Korábbi szakdolgozatomban emberi tényezőként azonosítottam a

- szervezetek külső és belső munkavállalóit,
- partnereinek, beszállítónak alkalmazottjait,
- ügyfeleit, illetve
- bármilyen más, a szervezettel kapcsolatba kerülő személyt, látogatót. (Oroszi, 2008)

Szintén az előbb jelölt forrásban mutattam be azt is, hogy az emberi tényező jelentős szerepet tölt be az információbiztonságban, hiszen a szervezet védendő értékeihez közvetlenül hozzáfér, ezáltal egyben vonzó célpontot is jelent a támadóknak. (Oroszi, 2008)

Az emberi tényező kihasználható tulajdonságait és kapcsolódó szituációit szintén több publikációban vizsgáltam, illetve határoztam meg aszerint, hogy mikor és milyen körülmények között lehetnek jellemzőek az egyénekre (Oroszi, 2008; Oroszi, 2014; Oroszi, 2021).

Összességében a humán faktort vagy emberi tényezőt úgy határozom meg, mint a szervezettel bármilyen kapcsolatba kerülő személyek összességét, akiknek tulajdonságai, viselkedése, kompetenciája, tapasztalata, szándéka, motivációja hatással van a szervezet biztonságára.

2.2.2. SOCIAL ENGINEERING

A Social Engineering egy, jellemzően magyarra nem-fordított fogalom, lényegében az emberi tényezőn alapuló támadási technikák gyűjteménye.

Harl (1997) úgy határozta meg, mint annak művészete és tudománya, hogy a támadó rávegye az embereket céljai megvalósítására, kívánságainak, kéréseinek teljesítésére.

Granger (2001) több meghatározás vizsgálata után úgy értelmezte, mint a hackerek azon támadási módszerei, melyek az emberi bizalom kihasználásán, illetve manipulálásán alapulnak, abból a célból, hogy a támadó hozzáférést szerezzen rendszerekhez és információkhoz.

Mitnick és Simon (2003) definíciója szerint „*a social engineering a befolyásolás és rábeszélés eszközével megtéveszti az embereket, manipulálja, vagy meggyőzi őket, hogy a social engineer tényleg az, akinek mondja magát. Ennek eredményeként a social engineer – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni*”. (Mitnick és Simon, 2003, borító)

Mann (2008) úgy határozza meg a Social Engineering-et, mint az emberi tényező manipulálására, annak megtévesztésére, információ kiadására vagy egyéb cselekedet végrehajtására ösztönző támadási technika.

Jain és szerzőtársai (2016) Huber és szerzőtársai (2009) alapján úgy határozzák meg a fogalmat, mint az információbiztonság leggyengébb láncszemének, vagyis a rendszereket használó felhasználók kihasználási módszereit.

Deák (2017) megfogalmazása szerint „a social engineering a bizalmas információk megszerzésére irányuló támadási forma, amely a technológiai sérülékenységeket és az emberi tényező gyengeségeit együttesen használja ki”. (Deák, 2017, p. 2.)

Chapple és társai (2021) a CISSP tananyagában úgy határozzák meg a fogalmat, mint egy olyan támadási forma, mely az emberi tényező természetét és viselkedését használja ki.

Publikációk (például Guenther, 2001; Mitnick és Simon, 2003; Oroszi, 2008; Oroszi, 2014) által általánosan elfogadott, hogy a Social Engineering módszerek két nagy csoportba sorolhatóak: a humán alapú, illetve a számítógép alapú támadások kategóriáiba.

Fentiek alapján a Social Engineering-et úgy határozom meg, mint olyan támadási technikák gyűjteménye, melyek az emberi tényező kihasználható tulajdonságain alapulva, annak személyes vagy számítógépen keresztüli megtévesztésével, befolyásolásával segítik a támadót céljainak elérésében, legyen az információszerzés, jogosulatlan hozzáférés, vagy bármilyen más károkozás.

2.2.3. BIZTONSÁGTUDATOSSÁG (SECURITY AWARENESS)

A Social Engineering jellegű támadások elleni leghatékonyabb védekezés az emberi tényező biztonságtudatosságának fokozása, ezért következő legfontosabb fogalomnak ezt választottam. Siponen (2000) a biztonságtudatosságot egy állapotnak tekinti, melyben a munkavállalók tisztában vannak a szervezet biztonsági küldetésével.

Tsohou (2010) a biztonságtudatosságot olyan folyamatként definiálja, melynek célja az egyének viselkedésének, normáinak, munkavégzési szokásainak, valamint a szervezeti kultúra megváltoztatása az információbiztonsági szemlélet tükrében.

Haeussinger és Kranz (2013) a biztonságtudatosság megfogalmazására három különböző perspektívát azonosított: a folyamat, viselkedés, valamint kognitív szemléletű megközelítéseket. Szakirodalom feltárásuk eredményei alapján a biztonságtudatosságot úgy azonosították, mint a felhasználók információbiztonsági ismereteit, a biztonság fontosságának szemléletét, valamint a felhasználók felelősségét, érdekeltségét a biztonságban.

Maquosi és szerzőtársai (2013) a biztonsághoz hasonlóan a biztonságtudatosságot is egy folyamatnak tekintik, melynek során a felhasználók folyamatosan tanulnak és viselkedésük változik, melyből a szervezet profitál.

Nemeslaki és Sasvári (2015) definíciója a munkavállalók általános információbiztonsági tudásaként, valamint az információbiztonsági szabályok ismereteként határozza meg a biztonságtudatosságot.

Tarján (2020) megfogalmazása szerint „*az információbiztonsági tudatosság a szervezet érdekelt feleinek tudása és attitűdje a szervezet tulajdonában vagy kezelésében lévő információs javak védelmével kapcsolatban*”. (Tarján, 2020, p. 28.)

Jasenszky és szerzőtársai (2021) a biztonságtudatosságot általánosságban úgy határozták meg, mint egy állapot, mely a biztonságtudatosságot fejlesztő akciók, oktatások következtében érhető el, és a szabályok ismeretén túl azok betartására is hatással van.

Fentiek alapján az általam alkalmazott definíció a biztonságtudatosság fogalmára a következő: azt információbiztonsági szabályok, valamint a felhasználókat érintő támadási technikák és azok jellemzőinek ismerete, a tanultak és ismeretek alkalmazása a kockázatok bekövetkezésének megelőzése, a támadások felismerése, észlelése, valamint kezelése során.

2.2.4. GAMIFIKÁCIÓ (GAMIFICATION)

A gamifikáció, vagy játékosítás meghatározására már szintén rengeteg definíció született az évek során.

Zichermann és Linder (2013) Magyarországon is megjelent könyvének megfogalmazása alapján „*a gamifikáció az a folyamat, amelyben a közönség elköteleződik a hűségprogramok, a játéktervezés és a viselkedési közgazdaságtan legjobb eszközeinek felhasználása révén.*" (Zichermann és Linder, 2013, p. 14.)

Findlay (2016) szerint a gamifikáció úgy értelmezhető, mint a játékmechanika alkalmazása nem játék-kontextusban, a kívánt viselkedés, illetve eredmények elérése érdekében.

Van den Boer (2019) definíciója alapján a gamifikáció a játékelemek és a játékos gondolkodás alkalmazása nem játék-környezetben a célzott viselkedés és elkötelezettség növelése érdekében.

Karagiannis és szerzőtársai (2020) szerint a gamifikáció általános elfogadott definíciója a játékgondolkodás és játékmechanika folyamata a felhasználók bevonásába a problémák megoldás érdekében.

Pacsi és Szabó (2017) szakirodalom feltárásuk során úgy határozták meg a gamifikáció definícióját, mint „*az átadni kívánt információk játékos formában történő tálalása az élet játékon kívüli területein a fogyasztók felé. A játék ösztönös magatartás, mely segíti az információk feldolgozását, s az átélt élményen keresztül azok tartós tárolását.*" (Pacsi és Szabó, 2017, p. 63.) Szintén a szerzőpáros világított rá, hogy a gamifikációt gyakran összekeverik az „edutainment" fogalmával, mely az angol „education" és „entertainment" szóból származik és gyakorlatilag „szórakozva tanulásként" értelmezhető. Ettől a gamifikációt elsősorban az különbözteti meg, hogy az edutainmenttel szemben nem csak az oktatásban, hanem az oktatáson kívüli területeken is használják. (Pacsi és Szabó, 2017)

Mindezek alapján a gamifikációt úgy határozom meg, mint játék elemeket alkalmazó, élmény-alapú, ösztönző jellegű, elkötelezettséget növelő, pozitív kimenetelű, visszajelzést adó nem játék-környezetben alkalmazott motivációs megoldások, melyek akár munkahelyi problémák megoldására, illetve kifejezetten a biztonságtudatosság fejlesztésére is alkalmazhatóak.

A kapcsolódó alsóbb-rendű fogalmakat a disszertáció vonatkozó fejezeteiben definiálom.

2.3. A BIZTONSÁGTUDATOSSÁG FEJLESZTÉSÉNEK INDOKOLTSÁGA ÉS KÖVETELMÉNYEI

A Verizon 2020-as Data Breach Investigation riportja szerint a sikeres támadások 67%-a emberi mulasztás és/vagy felhasználót érintő támadás (például adathalászat) miatt következik be (Verizon Data Breach Investigation Report, 2020), a PurpleSec 2020-as kiberbiztonsági riportjának statisztikái szerint pedig a kibertámadások 98%-a valamilyen Social Engineering technikán alapul (PurpleSec Cyber Security Statistics, 2020). De Pasquale (2023) statisztikái szerint a kibertámadások 2022-ben globálisan 38%-kal nőttek az előző évhez képest és a szervezetek 83%-a érintett volt valamilyen incidensben. A Verizon 2022-es Data Breach Investigation Report-ja szerint pedig a támadásoknak már 82%-a az emberi tényezőre volt visszavezethető, például adathalászatra, egyéb módon megszerzett azonosító adatokra, nem megfelelő használatra. (Verizon Data Breach Investigation Report, 2022) Az ENISA Threat Landscape 2022 kiadványa a zsarolóvírusok és kártékony kódok mellett 3. helyen listázza a Social Engineering támadásokat is. (ENISA Threat Landscape, 2022) Ezek az adatok alátámasztják, hogy az emberi tényező kihasználása segíti a támadókat a célzott rendszerekhez való hozzáférés megszerzésében, rosszindulatú programok terjesztésében, az IT rendszerek egyéb sebezhetőségeinek kihasználásában és a Social Engineering módszerek alkalmazásában. Ahogy Fandi (2019) is megfogalmazta, a kiberbiztonság nem csak biteket és bájtokat jelent, hanem embereket és folyamatokat is. Az alkalmazottak könnyen kihasználható erőforrást jelentenek a támadók számára, mivel közvetlen hozzáféréssel rendelkeznek mindazokhoz az eszközökhöz és adatokhoz, amelyeket egy szervezet védeni kíván. Például az alkalmazottak használnak és szállítanak (vagy hagynak el) hardvereszközöket, telepítenek és frissítenek (vagy mulasztanak el frissíteni) szoftvereket, hozzáférnek belső és bizalmas minősítésű fájlokhoz, rendszerekhez és adatokhoz, emellett hasznos belső információk és tudás birtokában vannak, valamint kommunikálnak nem csak egymással, hanem ügyfelekkel és partnerekkel. Mindezek mellett olyan kihasználható tulajdonságokkal rendelkeznek, amelyek vonzó célpontjaivá teszik őket a Social Engineering támadásoknak – és melyeket megfelelő képzés nélkül a támadók sikeresen ki is használhatnak. (Oroszi, 2021)

Az emberi tényezőt kihasználó támadásoknak számtalan technikája létezik, ezen módszereket nemzetközi szerzők (például Harl, 1997; Mitnick, 2003; Mann, 2008; Long, 2008; Hadnagy, 2011) mellett több hazai szakértő is részletesen bemutatta tanulmányaiban, és megalapozta, hogy a Social Engineering módszerek valós fenyegetést jelentenek a szervezeteknek (például Bányász és szerzőtársai, 2019; Deák, 2017; Deák, 2019; Kollár és Zakar, 2020; Oroszi, 2008;

Oroszi, 2014; Oroszi, 2015; Oroszi, 2018; Oroszi, 2020b). Ezen támadási technikák folyamatosan fejlődnek és egyre újabbak jelennek meg. Sadiq és szerzőtársai (2021) publikációjukban az adathalász támadások típusait mutatják be, kiegészítve az új trendekkel, Alhabri és szerzőtársai (2022) pedig kifejezetten a social médiához kapcsolódó phishing támadásokkal foglalkoznak.

Ahogyan Mitnick és Simon (2003) is megfogalmazta, a technológiai védelmi intézkedések nem elegendőek ezen típusú támadásokkal szemben. Bevezethetünk bármilyen technológiai intézkedést, a teljeskörű védelem érdekében elengedhetetlen a munkavállalók biztonságtudatossági ismereteinek fejlesztése, érzékenyítése a téma iránt. (Oroszi, 2008)

A biztonságtudatossági módszerek hatékonyságának vizsgálatához kapcsolódó kutatásokat szintén több nemzetközi és hazai szakértő is publikált (például Khan és szerzőtársai, 2011; Abawajy, 2014; Tschakert és Ngamsuriyaroj, 2019; Legárd, 2020), és eredményeik azt mutatják, érdemes tovább vizsgálni a témát, hiszen ahogyan Abawajy (2014), valamint Tschakert és Ngamsuriyaroj (2019) is bizonyította, a preferált megoldások a gyakorlatban még nem 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.

Napjainkban elmondható, hogy minden szervezet szembenézett már valamilyen szinten az információbiztonság fontosságával: a tapasztalatom alapján a felhasználók legalább a GDPR-nak (Az Európai Parlament és a Tanács (EU) 2016/679 rendelete, (2016. április 27.), a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (GDPR) való megfelelés biztosítása kapcsán találkoztak már a fogalommal, illetve a kapcsolódó információbiztonsági követelményekkel is, például a 3. fejezetben bemutatott kutatásom válaszadóinak 14%-a írta fel az *adatvédelem* vagy *GDPR* szavakat, mint „biztonságtudatossági ismeret”. Ugyanezt igazolja az ISACA Budapest Chapter által készített 2019-es Információbiztonsági helyzetkép, melynek egyik fókusza és a tárgyév legfontosabb információbiztonsági célkitűzése a GDPR megfelelés volt. (ISACA Budapest Chapter Információbiztonsági Helyzetkép 2019)

Nem csak az adatvédelmi kötelezettségek, hanem ezek mellett a szervezetek jelentős részére vonatkozik valamilyen közvetett vagy közvetlen, külső információbiztonsági szabályozás, mely egyrészt előírja a felhasználók biztonságtudatosságának fejlesztését, másrészt az információbiztonsági kockázatok elemzését és kezelését, melynek az emberi tényező egyértelműen része. (Oroszi, 2011) Első lépésként azt vizsgáltam meg ennek okán, hogy a különböző jogszabályi előírások és egyéb külső követelmények milyen kötelezettséget rónak a szervezetekre a munkavállalók biztonságtudatossági fejlesztésének vonatkozásában, illetve milyen követelményeket támasztanak az információbiztonsági képzésekkel szemben.

2.3.1. A HAZAI SZERVEZETEKRE VONATKOZÓ KÜLSŐ KÖVETELMÉNYEK A BIZTONSÁGTUDATOSSÁG FEJLESZTÉSÉRE VONATKOZÓAN

A felhasználók biztonságtudatosságának fejlesztését több nemzetközi és hazai szabályozás is előírja a szervezetek számára, kötelezővé téve ezáltal legalább egy minimális, rendszeres biztonságtudatossági oktatás megvalósítását. A nem kötelező érvényű információbiztonsági ajánlások szintén segítik ezek alkalmazását, illetve a szabályozás előírásán túl a megvalósítást is támogatják. Ezeket a szabályozásokat és ajánlásokat az alábbiakban szedtem össze és vizsgáltam meg felhasználhatóság szempontjából. A lent hivatkozott dokumentumok mindegyike a 2023. március 26-án hatályos, illetve elérhető állapotában került vizsgálatra.

2.3.1.1. Magyarországi jogszabályok, rendeletek és ajánlások

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról és végrehajtási rendeletei

Az információbiztonság egyik legjelentősebb hazai szabályozója az állami szférában a *2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról*, illetve a *41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről végrehajtási rendelet*, mely a hatálya alá tartozó szervezetekre határoz meg információbiztonsági előírásokat, köztük az információbiztonsági képzések megvalósítását is.

Az előírásokat tartalmazó OVI tábla a következőt rögzíti a felhasználók biztonságtudatossági képzésével kapcsolatban:

- minden besorolási szint szerint elvárt, hogy az informatikai biztonsági szabályzatban szabályozni kell az informatikai biztonság tudatosítására irányuló tevékenységet és képzést az érintett szervezet összes közszolgálati, vagy munkavégzésre irányuló egyéb

jogviszonyban álló alkalmazottainak, munkavállalóinak, megbízottjainak tekintetében (3.1.1.1.3.7),

- minden besorolási szinten elvárt a képzési eljárásrend készítése (3.1.7.2),
- minden besorolási szinten elvárt a munkavállalók biztonságtudatossági képzésben való részesítése, mind új belépők esetén, mind a rendszerben bekövetkezett jelentősebb változásokat követően, mind pedig a szervezet által előre meghatározott gyakoriság szerint (3.1.7.3),
- 3-as és magasabb besorolási szinten a szervezetnek szerepkör vagy feladat alapú biztonságtudatossági képzésben kell részesítenie a munkavállalóit, szintén a fenti feltételek teljesülése esetén (3.1.7.5), valamint a képzéseket dokumentálnia kell (3.1.7.6),
- 4-es és magasabb besorolási szinten a biztonságtudatossági képzésnek ki kell terjednie a belső fenyegetéssel szembeni védelemre is (3.1.7.4)

Az informatikai rendszer zártsági követelményeit előíró jogszabályok

A különböző szervezetek, szolgáltatók érintett informatikai rendszereinek zártságát több jogszabály is megköveteli és tanúsíttatja. Például a *2003. évi C. törvény az elektronikus hírközlésről*, a *2007. évi LXXXVI. törvény a villamos energiáról*, *2008. évi XL. törvény a földgázellátásról*, a *2011. évi CCIX. törvény a víziközmű-szolgáltatásról* a számlázási rendszer zártságát követeli meg. A *2007. évi CXXXVIII. törvény a befektetési vállalkozásokról és az árutőzsdei szolgáltatókról, valamint az általuk végezhető tevékenységek szabályairól,* a *2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról*, valamint a *2014. évi LXXXVIII. törvény a biztosítási tevékenységről* a hatálya alá tartozó szervezetek esetében szintén előírja, hogy a tevékenységük végzésére csak olyan informatikai rendszer felhasználásával kerülhet sor, amely biztosítja a rendszerelemek zártságát.

Ezen érintett rendszereknek meg kell felelniük az általános információbiztonsági zártsági követelményeknek, melyek szintén az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényre hivatkoznak vissza, vagy pénzügyi szervezetek esetében a *42/2015. (III. 12.) kormányrendelet* alapján kerültek meghatározásra. Mindezek alapján pedig a biztonságtudatossági képzés – legalább az érintett rendszerek vonatkozásában azonosítható felhasználói körre – kötelezően elvárt.

A Magyar Nemzeti Bank 8/2020. (VI.22.) számú ajánlása az informatikai rendszer védelméről

Az MNB ezen ajánlásának a célja, hogy gyakorlati útmutatást adjon az érintett szervezeteknek az informatikai rendszerük kockázatarányos védelmének megvalósításában. Az ajánlás 12. *Személyi biztonság* fejezetének 12.2 alpontja a biztonságtudatossági oktatás követelményeit rögzíti, melyek az alábbiak:

- Az intézmény az informatikai biztonsági szabályozási rendszerében meghatározza az informatikai biztonságtudatossági oktatás szabályait, eljárásrendjét.
- Az intézmény gondoskodik az üzleti folyamatai támogatására szolgáló élesüzemi informatikai rendszerekhez és az azokban tárolt adatokhoz hozzáférő felhasználók rendszeres, az új belépők esetén a belépéstől számított 3. hónapig bezárólag, a többi felhasználó esetében legkésőbb éves szinten történő dokumentált biztonságtudatossági oktatásáról.
- Az intézmény folyamatosan gondoskodik az élesüzemi rendszerek üzemeltetésében részt vevő személyek megfelelő szakmai színvonalon történő biztonságtudatossági képzéséről.
- Az intézmény a képzésekhez éves képzési tervet készít, a külső képzéseken történő részvételét a költségvetése tervezésekor figyelembe veszi.

Előremutató gyakorlatként pedig meghatározza, hogy az üzemeltetők és fejlesztők biztonsági oktatásának tervezésekor figyelembe veheti az üzemeltetők és fejlesztők speciális részterületeire, valamint a tervezés során esetlegesen bevezetésre kerülő új rendszerekre vonatkozó biztonsági képzéseket annak érdekében, hogy releváns információk birtokába kerüljenek.

A Magyar Nemzeti Bank 12/2020. (XI.6.) számú ajánlása a távmunka és távoli hozzáférés informatikai biztonsági követelményeiről

A COVID-19 következtében bevezetett otthoni munkavégzés kockázataira reagálva az MNB a hivatkozott ajánlásban már specializáltabb követelményeket rögzít a biztonságtudatosság fokozásával kapcsolatban, és elvárja, hogy az intézmény készítsen informatikai biztonsági oktatási anyagot a távmunka használatának feltételeiről, kockázatairól, melynek keretén belül az intézmény hívja fel a távoli felhasználó figyelmét legalább az általa definiált 11 információbiztonsági előírásra (eszközök felügyelete, képernyő zárolása, betekintésvédelem, hitelesítéshez használt eszközök biztonsága, jelszavak biztonságával kapcsolatos követelmények, otthoni WiFi biztonsága, utazás - adathordozók szállítása, incidensek észlelése

és jelentése), tehát ebben az ajánlásban már konkrét ismeretek is megjelennek, mint követelmény.

2.3.1.2. Nemzetközi, Magyarországot érintő rendeletek, szabványok és ajánlások

AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE a pénzügyi ágazat digitális működési rezilienciájáról és az 1060/2009/EK rendelet, a 648/2012/EU rendelet, a 600/2014/EU rendelet, valamint a 909/2014/EU rendelet módosításáról

Az úgynevezett „DORA" rendelet 12. cikkének (Tanulás és alkalmazkodás) (6) bekezdése szerint a pénzügyi szervezetek IKT-biztonsági tudatosságot elősegítő programokat és a digitális működési rezilienciával kapcsolatos képzéseket dolgoznak ki személyi állományuk képzési rendszerének kötelező moduljaként, melyeket minden munkavállalónak és a felsővezetés minden tagjának el kell végeznie. Tehát ezen előírás is kötelezettséget ró az érintett szervezetekre a biztonságtudatosság fejlesztése terén.

AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2555 IRÁNYELVE az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv)

A NIS 2 irányelv II. fejezetének 7. cikkében meghatározott nemzeti kiberbiztonsági stratégiának tartalmaznia kell a kiberbiztonsággal kapcsolatos tudatosság általános szintjének a polgárok körében történő fokozását célzó tervet, ideértve a szükséges intézkedéseket is. Emellett a rendelet előírja, hogy a kiberbiztonsággal kapcsolatos tudatosság és a kiberhigiénia elengedhetetlen az Unión belüli kiberbiztonság szintjének növeléséhez, különös tekintettel a kibertámadások során egyre gyakrabban használt csatlakoztatott eszközök növekvő számára, ezért törekedni kell az ilyen eszközökkel kapcsolatos kockázatokra vonatkozó általános tudatosság növelésére, míg az uniós szintű értékelések segíthetnek biztosítani az ilyen kockázatok egységes értelmezését a belső piacon.

A rendelet szintén megköveteli, hogy az alapvető és fontos szervezeteknek az alapvető kiberhigiéniai gyakorlatok széles skáláját kell alkalmazniuk, például a zéró bizalom alapelveit, a szoftverfrissítéseket, az eszközkonfigurációt, a hálózatszegmentálást, a személyazonosság- és hozzáférés-kezelést, vagy a felhasználói tudatosságot, továbbá képzéseket kell szervezniük alkalmazottjaik számára és fel kell hívniuk a figyelmet a kiberfenyegetésekre, illetve az adathalászatra és más Social Engineering technikákra.

ISO/IEC 27001:2013, valamint ISO 27001:2022 szabvány

Az *ISO/IEC 27001:2013 Information technology. Security techniques. Information security management systems. Requirements* szabvány „A" mellékletének 7.2.2 pontja szerint követeli meg a felhasználók biztonságtudatossági képzését, miszerint „*A szervezet minden alkalmazottjának, és ahol alkalmazható, a szerződéses munkatársaknak, megfelelő tudatosító képzésben és tréningben, illetve munkakörükhöz tartozó szervezeti szabályzatok és eljárások rendszeres frissítéseiben kell részesülniük*". (ISO 27001:2013)

Ugyan a szabvány részleteibe menően nem szabályozza túl a biztonságtudatossági képzések megvalósítását, ennek ellenére fontos kikényszerítő azon szervezetek számára is, melyek nem tartoznak az előző alpontban felsorolt jogszabályok egyikének hatálya alá sem, viszont rendelkeznek ISO 27001 tanúsítvánnyal, vagy tervezik annak megszerzését és fenntartását.

A szabvány új verziója 2022. októberében került kiadásra (ISO 27001:2022), melyben az információbiztonság-tudatosság fejlesztésekre vonatkozó lényeges változás nem történt.

NIST 800-53 Revision 5. Security and Privacy Controls for Information Systems and Organizations

A NIST (National Institute of Standards and Technology) 800-53 ajánlása általános információbiztonsági megfeleléssel foglalkozó követelményjegyzék, mely azonban kellő részletességgel foglalkozik a felhasználók információbiztonsági képzésével kapcsolatos elvárásokkal, és jóval részletesebben taglalja azokat, mint például az ISO 27001. Az ajánlás kitér az információbiztonsági oktatások követelményeire, előírja azok szabályozottságát, előírásokat fogalmaz meg a biztonságtudatossági képzések célcsoportjaira, a szerepkör alapú oktatások indokoltságára, szimulációs tesztekre és a tudatosság gyakorlati ellenőrzésére és fejlesztésére, a különböző fenyegetések azonosítására és jelentésére, úgy, mint a Social Engineering, illetve a belső fenyegetések is.

NIST SP 800-50 Building an Information Technology Security Awareness and Training Program

Az előző pontban bemutatott ajánlás mellett a NIST már 2003. októberében publikálta a NIST SP-800-50 Building an Information Technology Security Awareness and Training Program című ajánlást, melynek kifejezett célja az IT biztonsági oktatási programok támogatása, lehetséges módszerek bemutatása, tehát ez inkább azon szervezetek számára segédlet, melyek felismerték az információbiztonsági tudatosítás fontosságát, vagy követelményét. Az ajánlás kitér az oktatások céljára, gyakoriságára, célcsoportjaira, az alkalmazandó lehetséges

módszerek rövid bemutatására, a biztonságtudatossági programok tervezésére és megvalósítására, a tananyagok fejlesztésére, valamint a képzések értékelésére, utókövetésére is. (Wilson és Hash, 2003) Az ajánlás aktualizálása folyamatban van, a honlapon szereplő információk alapján a SP 800-50 Rev. 1. (Draft) kiadása 2023. közepén várható.

NIST SP 800-16 Rev. 1. (Draft) A Role-Based Model for Federal Information Technology/Cybersecurity Training (3rd Draft)

A NIST 800-16 ajánlásának kifejezett célja az információbiztonsági/kiberbiztonsági képzésekkel kapcsolatos követelmények meghatározása, mindez szerepkör alapú tréningek megvalósításával. Ezáltal a dokumentum jóval túlmutat a minden felhasználó számára ajánlott, általános biztonságtudatossági fejlesztéseken, melyek azonban fontos alapját képezik a további releváns oktatásoknak.

SANS – Leveraging the SANS Security Awareness Maturity Model to Effectively Manage Human Risk (e-book)

A SANS több publikációja, illetve megoldása a felhasználók biztonságtudatosságának fokozását támogatja, nem tekinthető biztonságtudatosság fejlesztését előíró szabványnak, viszont szintén segítséget nyújt azon szervezeteknek, melyek saját, vagy külső elvárás miatt foglalkoznak a munkavállalóik biztonságtudatossági ismereteinek fokozásával.

SANS – Útmutató a biztonságtudatossági intézkedések bevezetéséhez – A biztonságos otthoni munkavégzés

A SANS a COVID-19 világjárvány hatására bevezetett otthoni munkavégzés kapcsán adta ki fenti, magyar nyelven is elérhető útmutatóját, mely a legfontosabb általános ismereteket mutatja be, melyek a felhasználók edukálása során kiemelten fontosak, valamint a dokumentum egy linkgyűjteményt is tartalmaz az egyes támadási technikák és ellenük való védekezés bemutatására. Az útmutató 33 nyelven elérhető, bizonyos hivatkozásai azonban kizárólag angol nyelvű források.

CISA – Cybersecurity Awareness Month Publications

A CISA (Cybersecurity and Infrastructure Security Agency) szintén támogatja a szervezeteket térítésmentesen elérhető ajánlásokkal, útmutatókkal. A 2021-es kiberbiztonsági hónapra készült csomagjuk több felhasználható mintát, példát tartalmaz, illetve segítséget nyújt a programok tervezésében, megvalósításában.

Ez a publikációcsomag elsősorban azon szervezetek számára hasznos, amelyeknél a biztonságtudatosság fejlesztése már valamilyen más elvárás szerint kikényszerített, és valamilyen „belépő” szintű biztonságtudatossági kampány megvalósítását tervezik.

A fenti szabályozások és ajánlások áttekintésével megállapítottam, hogy a kötelező érvényű, előíró szabályozások minimális mértékben támasztanak követelményeket az érintett szervezetekkel szemben a biztonságtudatosság fejlesztése terén. Az oktatások dokumentálásának, gyakoriságának, illetve célközönségének meghatározásán túl általában csak a kockázatarányosság elvének megfelelő tartalmi elemeket követelik meg. Jellemzően nem írnak elő speciális követelményt az oktatási módszerekre vonatkozóan, vagy kötelező tartalmi elemek vonatkozásában, illetve ami fontos, hogy nem is tiltanak meg speciális oktatási módszereket és alternatív képzési lehetőségeket, így például nem írják elő, de nem is zárják ki a gamifikációs lehetőségek alkalmazását.
Az oktatási módszerekben és tartalmi elemek meghatározásában a bemutatott, opcionálisan alkalmazható ajánlások nyújthatnak segítséget, de kifejezetten biztonságtudatosságot fejlesztő gamifikációs lehetőségekre a jelenleg vizsgált, elérhető verziók még nem terjednek ki.

2.4. A BIZTONSÁGTUDATOSSÁG FEJLESZTÉSÉNEK ESZKÖZEI

A biztonságtudatossággal kapcsolatos külső előírások, illetve követelmények feltárását követően megvizsgáltam, hogy milyen képzési módszerek, tudatosítási lehetőségek érhetőek el, ezeknek mi a funkciója, erőssége.
A biztonságtudatossági képzések általános célja, hogy tájékoztassák a munkavállalókat és elmagyarázzák a dolgozóknak a szervezet biztonsági irányelveit és szabályait, valamint a biztonságtudatos viselkedés szükségességét, fejlesszék a felhasználók készségeit és kompetenciáit a biztonságos munkavégzéshez, és növeljék a biztonságtudatosság szintjét a teljes szervezetben. (Wilson és Hash, 2003) Nagyon fontos, hogy az ilyen jellegű képzéseken minden alkalmazott részt vegyen beosztástól függetlenül. (Gragg, 2003) Mitnick és Simon (2003) szerint a biztonságtudatossági programok központi célja az emberek viselkedésének és hozzáállásának megváltoztatása, a munkavállalók motiválása is. A képzési anyagok általában általános szabályokat, az adatok osztályozására és kezelésére vonatkozó irányelveket, az emberi tényező kihasználásán alapuló támadások típusainak és az alkalmazottak kihasználható szokásainak bemutatását tartalmazzák, illetve kitérnek arra, hogy hogyan lehet csökkenteni az

ilyen jellegű fenyegetések bekövetkezési valószínűségét vagy hatását. Figyelembe kell azonban venni azt az alapvető irányelvet is, hogy az ilyen jellegű programok fő célja annak tudatosítása is legyen, hogy a szervezet, illetve bárki lehet ilyen jellegű támadások célpontja. (Mitnick és Simon, 2003) Már Mitnick és Simon (2003) is felhívják arra a figyelmet, hogy a biztonságtudatossági képzésnek célja kell, hogy legyen a lebilincselő, interaktív élmény, ezért érdekes lehet a Social Engineering technikák szerepjátékon keresztül történő bemutatása.

A biztonságtudatossági képzéseknek számos különböző formája azonosítható. Wilson és Hash (2003) három, egymásra épülő szintet (oktatás, tréning, képzés) és négy kategóriát különböztet meg: interaktív video tréning (egyfajta e-Learning), web-alapú tréning, nem web-alapú számítógép-alapú tréning, személyes, instruktor által vezetett tréning. Abawajy (2014) a képzési módszereket hat kategóriába sorolja: konvencionális, instruktor által vezetett, online, játék-alapú, videó-alapú és szimulációs módszerekre. Aldawood és Skinner (2019) aszerint különböztetik meg a képzési módszereket, hogy hagyományosnak vagy modernnek számítanak. Előbbibe sorolják a klasszikus személyes oktatásokat, a biztonságtudatossági kampányokat, képernyővédőket, plakátokat, emlékeztetőket és az online kurzusokat, míg modernnek tekintik a komoly játékokat, virtuális laborokat, tematikus videókat és modulokat. Tschakert és Ngamsuriyaroj (2019) a tréningeket és anyagokat aszerint bontja meg és értékeli, hogy videó-alapúak, játék-alapúak, szöveg-alapúak, vagy tantermi képzések.

Legárd (2020) a belső PR eszközök alkalmazási lehetőségeit vizsgálta a biztonságtudatossági programokban és a személyes-, csoportos-, illetve a tömegkommunikáció eszközeinek csoportosításában vizsgálta a különböző kommunikációs és oktatási lehetőségeket (például előadás, e-mail-ek, hírlevelek, cikkek, faliújságok, stb.).

A jelen disszertációhoz készített kutatásomnak ugyan nem volt elsődlegesen célja annak vizsgálata, hogy a különböző szervezetek milyen oktatási módszereket alkalmaznak, kérdőívemben megkérdeztem azonban a felhasználókat, hogy ilyen módon történt az utolsó biztonságtudatossági képzésük lebonyolításra. A releváns válaszadók (tehát, akik már vettek részt biztonságtudatossági képzésen, azaz a minta 64%-a) 48,4%-a az e-Learning-et, 33,5%-a a tantermi oktatást, 22,5%-a az online előadást, 13,7%-a az e-mail-es tájékoztatókat, hírleveleket, 10%-a pedig a biztonságtudatossági kampányokat jelölte meg. Gamifikációs megoldással saját bevallása szerint a válaszadók csupán 7%-a találkozott.

Megbontva a fenti értékeket állami, illetve privát szférára, a következőképpen alakulnak a számok (1. táblázat):

	Állami (%)	*Privát (%)*
E-Learning	33,76	59,04
Tantermi oktatás	28,57	37,14
Online oktatás	27,27	19,04
Kampány	11,68	8,57
Hírlevél, tájékoztató	11,68	15,23
Gamifikációs elem	**6,49**	**7,61**

1. táblázat: Biztonságtudatossági képzések jellege az állami és privát szektorban, a kutatásban résztvevő felhasználók válaszai alapján (forrás: saját szerkesztés)

Az értékek alapján elmondható, hogy a gamifikációs lehetőségek nagyon hasonló mértékben alkalmazottak az állami és privát szektorban, egyedüli kimagasló értéket az egyébként is domináló e-Learning módszerek alkalmazása jelenti a privát szférában.

2.4.1. A BIZTONSÁGTUDATOSSÁG FEJLESZTÉSÉNEK HAGYOMÁNYOS LEHETŐSÉGEI

Bár a disszertációban kifejezetten a gamifikációs lehetőségekre helyezem a hangsúlyt, ennek ellenére az egységes értelmezéshez elengedhetetlennek tartom a hagyományos módszerek rövid bemutatását és annak definiálását, hogy a továbbiakban mit értek ezek alatt. Különösen fontosnak vélem ezt abból kifolyólag is, hogy a kutatásomban ezen képzési módok szintén megjelennek és vizsgálat tárgyát képezik. A feldolgozott szakirodalom értelmezése alapján a következő öt képzési módot különböztetem meg: a tantermi oktatást, az online oktatást és videófelvételeket, a tréningeket és workshopokat, az e-Learning megoldásokat, illetve a kampányelemeket.

2.4.1.1. Tantermi oktatás

Az egyik legrégebbi, klasszikus biztonságtudatosság-fejlesztési módszer a hagyományos biztonságtudatossági oktatás, azaz a személyes, tantermi előadás. (Oroszi, 2008) Ez lehet átfogó, általános tartalmú, vagy célzott, felfrissítésre vagy új tartalmakra, aktualitásokra fókuszáló prezentáció. Emellett megkülönböztethetünk moduláris felépítésű, egymásra épülő előadásokat is. Ez utóbbi esetben a különböző biztonságtudatossági témákat konkrét modulokra oszthatjuk, melynek előnye, hogy a résztvevők a már meglevő biztonságtudatossági ismereteik alapján kiválaszthatják a legérdekesebbeket, vagy esetleges előzetes felmérést követően a problémás vagy hiányosabb területekre irányíthatják őket. A biztonságtudatossági mérést célzó

akciók eredményei nagyon hasznosak lehetnek ezen képzési anyagok specializálásában és színesítésében is. (Oroszi, 2011)

Saját tapasztalataim alapján a felhasználók az ilyen jellegű előadásokon általában évente 1-1,5 órában vesznek részt, csoporttól vagy témától függően, amennyiben a szervezet nem moduláris oktatásokat szervez. Kivételt képez a menedzsment információbiztonsági képzése, amely általában 0,5-1 órát vesz igénybe, és főképp a vezetőket érintő veszélyekre, valamint a kapcsolódó információbiztonsági feladatikra és a példamutató magatartásra helyezi a hangsúlyt. (Oroszi, 2008)

A tantermi oktatás legfontosabb előnye az egyszerűség és a viszonylag alacsony költség lehet, de emellett komoly hátrányt jelenthet a többnyire általános tartalom és az időigényesség, nem is beszélve a 2020-ban kirobbant COVID-19 világjárvány hatásairól, melyek az online megoldások irányába vitték el a fókuszt. (Oroszi, 2020b)

A tantermi oktatások hatékonyságát Khan és társai (2011) is vizsgálták. Kutatásuk szerint ez jobb módszer, mint az e-mail-ben küldött tájékoztatók, hírlevelek, plakátok vagy az e-Learning alkalmazása, de nem olyan hasznos, mint az interaktív, csoportos megközelítésű oktatási módok.

2.4.1.2. Online oktatás és videófelvételek

A speciális oktatási lehetőségek közül kiemelném az online vagy virtuális előadások lehetőségét, amelynek legfontosabb előnye, hogy ebben az esetben a távoli telephelyeken vagy otthonról dolgozó kollégák is bekapcsolódhatnak a képzésekbe, vagy később, amennyiben az előadás jellege lehetővé teszi, felvételről is megnézhetik a tartalmat. A COVID-19 következtében az ilyen platformokon tartott megbeszélések és oktatási események nem csak szükséges megoldásként terjedtek el Magyarországon, hanem azt követően is egyre népszerűbbek és elfogadottabbak lettek, valamint nemcsak a munkahelyeken, hanem a felsőoktatásban is alkalmazható módszerré váltak.

Szintén előny, hogy az online oktatás tananyaga akár teljesen megegyezhet a hagyományos tantermi előadáséval, a különbség annyi, hogy itt egy virtuális tanteremben ülve hallgatják a résztvevők az előadást. Sőt, a két oktatás típus akár egy alkalommal is megtartható, személyes és online részvétellel egyaránt. Az online oktatási események megtartásához speciális eszközök nem szükségesek, platformjai lehetnek például a Microsoft Teams, a Google Meet, a Zoom vagy akár a Skype, így költséghatékonyság szempontjából is előnyös módszernek tekinthetőek. Az online képzés nagy előnye továbbá, hogy a moduláris felépítésű tananyagok leadása könnyebben megvalósítható. Moduláris előadások esetén egy-egy képzési alkalom általában

30-45 percet vesz igénybe, és legtöbbször kampányszerűen, vagy bizonyos gyakorisággal (például hetente, kéthetente, havonta) kerülhet rájuk sor.
Személy szerint ezeket a módszereket kevésbé tartom hatékonynak, mert a tapasztalatom az, hogy a részvevők gyakran elveszítik a fókuszt, és néhány bekapcsolt kameraképet látva előfordul, hogy mással foglalkoznak az oktatás közben.
Abawajy (2014) szerint az ilyen oktatásokról készített videófelvételek viszont olyan szempontból nagyon előnyösek, hogy a felhasználók bármikor meg tudják tekinteni, sőt újra tudják nézni ezeket a tartalmakat, valamint saját ütemezésük szerint nézhetik meg az egyes videókat.

2.4.1.3. Tréningek és workshopok

Az előző pontokban bemutatott általános biztonságtudatossági oktatáshoz képest a biztonságtudatossági tréning és workshop kategóriája abban különbözik, hogy legtöbbször egy korábban már megtartott oktatásra épül, így ezek célja elsősorban a meglévő tudás elmélyítése, a kockázatok megértése és a biztonságtudatos viselkedés begyakoroltatása. (Wilson és Hash, 2003) A hagyományos oktatáshoz hasonlóan ez is tantermi vagy online oktatás keretében zajlik, de ebben a megközelítésben a módszer interaktívabb, és különösen fontos a résztvevők tapasztalatainak egymással való megosztása, ezért a résztvevők száma alacsonyabb, mint az általános oktatás esetében. Ezen képzések is lehetnek átfogóak vagy moduláris felépítésűek, mint a biztonságtudatossági előadások, ugyanazokkal a témákkal, mint az előző részben bemutatottak, azonban itt a hangsúly a felhasználók aktív részvételén van. A feladatok összeállításával az oktatónak biztosítania kell, hogy a képzés sikerélményt jelentsen a felhasználó számára, és ne teremtsen kellemetlen helyzetet vagy felelősségre vonást.
Mivel a képzést kisebb csoportokban lehet a leghatékonyabban megvalósítani, egy tréningen vagy workshopon legfeljebb 5-10 fő vehet részt. Egy több száz alkalmazottat foglalkoztató szervezet esetében az összes felhasználó számára nehéz megvalósítani ezt a fajta képzést, ezért tapasztalataim szerint általában az alábbi feltételek valamelyikének megfelelő csoportok részvételét célszerű kötelezővé tenni:

- olyan felhasználók, akik nagy mennyiségű vagy érzékeny adatokkal dolgoznak,
- azok felhasználók, akik olyan környezetben dolgoznak, vagy munkakörükből adódóan olyan tevékenységet végeznek, amely növeli a különböző támadások kockázatát (például az ügyfélszolgálat, a Help Desk, az asszisztensek nagyobb mértékben vannak kitéve a Social Engineering jellegű támadásoknak),

- olyan felhasználók, akik a biztonságtudatossági tesztek, auditok eredményei alapján kevésbé ellenállóak a Social Engineering támadásokkal szemben (amennyiben a felmérés/teszt lehetővé teszi a személyes azonosítást),
- olyan felhasználók esetében, akik a biztonsági szabályokat vagy irányelveket megsértették (például a belépőkártyával való visszaélés, incidens okozása),
- azok a felhasználók, akik információbiztonsági incidens áldozatává váltak (például sikeres adathalász támadás, eszközlopás vagy elvesztés stb.).

A résztvevők számától, a témáktól és a gyakorlati feladatoktól, gyakorlatoktól függően egy tréning vagy workshop jellemzően 1-4 órás időráfordítást igényel, mely akár moduláris felépítésű is lehet. Ennek az oktatási módszernek a legfontosabb előnye, hogy a problémás területekre és a felhasználók tapasztalati tanulására összpontosít.

Khan és szerzőtársainak (2011) kutatása szerint a csoportos, interaktív beszélgetések bizonyulnak a leghatékonyabb oktatási módszernek, mely gyakorlatilag ebben a megközelítésben a tréning, illetve workshop kategóriájának felel meg.

2.4.1.4. E-Learning

A biztonságtudatossági képzések hatékonyságának növelése érdekében sok vállalat választja az e-Learning tanfolyam alkalmazását, ahogyan a kutatásom korábban feltüntetett eredményeiből is látszódik, a legtöbb szervezet ezt a megoldást preferálja szektorbeli elhelyezkedésétől függetlenül.

Chitra és Raj (2018) az e-Learning különböző módjait és területeit különbözteti meg, így az online tanulást, a virtuális tanulást, az elosztott tanulást, a hálózat- és web-alapú tanulást. Fontos különbséget tesznek azonban az m-learning, vagyis mobil tanulás között, mely kifejezetten a hordozható eszközökhöz igazodik.

Az ilyen típusú oktatás előnye, hogy az alkalmazottak szinte bárhol, bármikor elvégezhetik az egy vagy több modulból álló elektronikus tanfolyamot, bármikor megszakíthatják és folytathatják a tanulást, valamint a tanfolyam alatt vagy végén tesztelhetik tudásukat és interaktív feladatokat oldhatnak meg. Patel (2016) szerint az e-Learning alkalmazásának további előnye lehet a költségek csökkentése, a gyorsabb megvalósítás, a hatékonyabb tanulás, az önálló problémamegoldás lehetővé tétele.

Tapasztalataim alapján hátrány lehet azonban, hogy sok munkavállaló nem olvassa el az így megosztott tananyag tartalmát, a legtöbben általában azonnal tovább lépnek a vizsgára, hogy teljesítsék a kötelező képzést, és nem egyedi eset, hogy a felhasználók egymás között megosztják a zárótesztek helyes megoldásait, hogy gyorsan túl legyenek a feladaton. A csalás

lehetőségét, egyszerűségét Patel (2016) is hátrányként emelte ki, valamint az azonnali visszajelzés hiányát is negatívumként értékelte. Súlyos hiányossága a módszernek a konzultációs lehetőség, kérdés-válasz szekció elmaradása, az információbiztonsági csapat tagjaival való közvetlen kapcsolat hiánya. Emellett megemlíthetünk olyan hátrányokat is, mint az önkifejezés hiánya, a negatív egészségügyi hatások, illetve az technológiai esetleges technológiai korlátok, akadályok. (Chitra és Raj, 2018)

Az e-Learning képzések általában modulonként 0,5-1 órás időráfordítással végezhetőek el. Ennek ellenére a tanfolyam elvégzésének ideje egyénenként eltérő lehet, vannak olyan felhasználók, akik 15 perc alatt végig futják ugyanazt az anyagot, mellyel mások akár 2 órát is eltöltenek.

Khan és szerzőtársai (2011) szerint ezen oktatási eszköz hatékonysági szintje alacsony, mivel a módszer nem képes megváltoztatni a résztvevők normáit, szándékait vagy viselkedését. Általánosságban, nem információbiztonsági fókusszal az online tréningek hatékonyságát Singley és Hurst (2011) is vizsgálták, melybe az e-Learning megoldásokat is beleértették. Kutatásuk során ők azt állapították meg, hogy ezen módszerek a személyes képzéseknek életképes alternatívái lehetnek, Sitzmann és szerzőtársai (2006) pedig kimutatták, hogy az online tanulás hatékonyabb a tantermi képzésnél a deklaratív tudás tekintetében.

2.4.1.5. Kampányelemek

A rendszeres képzések és oktatási események mellett a biztonságtudatossági kampányok és programok segíthetnek a felhasználóknak abban, hogy emlékezzenek az információbiztonsági képzések legfontosabb üzeneteire és az emberi tényezőn alapuló kockázatokra. Ennek érdekében az ilyen jellegű, figyelemfenntartó kezdeményezéseknek nagyon kreatívnak kell lennie és minden csatornát fel kell használnia a kommunikációra. (Mitnick és Simon, 2003) A legfontosabb különbség a biztonságtudatossági program és a kampány között, hogy a kampányok általában rövidebb események az egyes időszakokban, a programok pedig általában hosszabb, akár egész éves akciók. (Oroszi, 2017) Mindkettő nagyjából ugyanazokkal az elemekkel valósítható melyek általában a következők Mitnick és Simon (2003), valamint Wilson és Hash (2003) alapján:

- plakátok, matricák, kihelyezett molinók/roll-upok
- képregények
- hírlevelek, emlékeztetők (e-mail)
- intranetes cikkek, blogbejegyzések
- képernyővédők

- ajándékok, ajándéktárgyak, hasznos dolgok
- rejtvények
- díjak, például „a hónap biztonsági alkalmazottja”

Megjegyzendő, hogy a biztonságtudatossági kampány, például „biztonságtudatossági hónap” kibővíthető más, hagyományos vagy gamifikációs képzésekkel, programokkal, de azokat nem sorolom a klasszikus kampányelemek közé.

Khan és szerzőtársainak (2011) kutatása szerint a plakátok és hasonló módszerek alacsony hatékonysággal bírnak a biztonságtudatossági szint fokozásában, ugyanis ezek bár bővítik az ismereteket, de nincs hatásuk a felhasználói viselkedésre. Ráadásul a tartalom elolvasása nem jelenti azt, hogy a felhasználó meg is értette, vagy helyesen értelmezte azt.

A disszertációm során folytatott kutatás során a kampányelemek tekintetében kíváncsi voltam arra, hogy melyik kampányelemhez hogyan viszonyulnak a felhasználók, így ennél a módszernél egy kiegészítő kérdőívet is alkalmaztam, melyből egy későbbi, a szervezeteket segítő publikáció készült. A kérdőíven a kutatás során kapott kampánycsomag egyes elemeit 4 pontos Likert-skálán kellett értékelniük a résztvevőknek, aszerint, hogy mennyire tetszett az adott kampányeszköz. Ezen felmérés alapján a leginkább az ajándékokat preferálták a résztvevők, és a válaszadók 85%-a értékelte pozitívan a kapott kameratakarót, 75%-a a memóriajátékot, 70%-a pedig a jelszókódolót. A „*Nagyon tetszett*” kategória győztesei a kameratakaró (72%), poszterek (44%) és a jelszókódoló (39%) voltak. A válaszadók legkevésbé a rejtvényt és a hírlevelet preferálták (8-8%-nak egyáltalán nem tetszett, 39-39% pedig csak elfogadhatónak értékelte azokat). (Laczkó és Oroszi, 2022)

Összességében a válaszadók a „*Mi tetszett a leginkább a kampányelemek közül?*” kérdésre kedvenc elemnek jelölték meg a posztereket (33%), a kameratakarót (26%) és a jelszókódolót (17%). Igaz a kutatás során a poszterek esetében szokatlan megközelítést, macskákkal való illusztrációt alkalmaztam, mely a visszajelzések alapján tovább növelte a figyelem felkeltését – és nem mellesleg azóta is több szervezetnél viszontlátom őket. (Laczkó és Oroszi, 2022)

2.4.2. ÚJ LEHETŐSÉGEK ÉS IGÉNYEK A BIZTONSÁGTUDATOSSÁG FEJLESZTÉSÉBEN

Az előbbiekben bemutatott, hagyományos biztonságtudatosság fejlesztő programok elemei legtöbbször a felhasználók információbiztonsági tudását bővítik és a legfontosabb szabályokra emlékeztetnek, kevésbé képesek azonban az attitűd és a viselkedés befolyásolására, illetve a felhasználók ösztönzésére a biztonságtudatos magatartás gyakorlására.

Rocha Flores és Ekstedt (2016) szerint az információbiztonsági képzésekben a személyre szabás és speciális tartalmak használata az oktatási anyagokban a résztvevők számára relevánsabbá és érthetőbbé teheti a biztonságtudatosságot fejlesztő programot, a hagyományos képzési módszerek és a gyakorlati elemek kombinálása pedig nagyobb valószínűséggel vezet a biztonságtudatosság fokozásához. Saját tapasztalataim is alátámasztják, hogy a felhasználók egyre unalmasabbnak tartják a meglevő képzési és figyelemfelkeltési módokat, és nagy igényük van az újdonságokra. (Oroszi, 2019)

Mindezek miatt javasolt átalakítani a biztonságtudatossági programokat, és olyan egyedi és szervezetre szabott eszközök alkalmazását kell megfontolni, amelyek bevonják a munkavállalókat, és segítenek az információbiztonsági ismeretek megértésében, elsajátításában. Ilyen akciók lehetnek a játékosítás irányába mutató aktív programok, melyek során a résztvevők elgondolkodhatnak az információbiztonságról és az abban betöltött szerepükről. Emellett dönthetünk úgy, hogy játék-alapú, aktív közreműködést igénylő programelemeket használunk, mint például egy biztonságtudatossági szabadulószoba vagy társasjáték.

2.5. GAMIFIKÁCIÓS MEGOLDÁSOK ALKALMAZÁSA A BIZTONSÁGTUDATOSSÁG FEJLESZTÉSÉBEN

Az előző pontban foglalt problémák és igények miatt megvizsgáltam a gamifikáció alkalmazásának lehetőségét, mely egyre népszerűbb módszer nem csak az oktatásban, hanem a vállalatoknál is a munkavállalók motiválására, a teljesítmény javítására, a képzések élményének fokozására.

Gamifikációs megoldásokkal akár a mindennapi életben is találkozhatunk, egy gamifikációs lehetőségekről szóló oktatási anyagomhoz összeállítottam, hogy akár csak a saját okostelefonomról tudom mondani a következő példákat:

- áruházak mobilapplikációi tesznek lehetővé pontgyűjtést különböző kedvezményekért,
- GPS alkalmazások jutalmaznak a balesetek, lezárások, egyéb események vagy térképhibák javításáért,
- nyelvtanuló alkalmazások ösztönöznek az egyre magasabb szintek elérésére és a mindennapi tanulásra,
- sport alkalmazások állítanak kihívások elé, melyek teljesítéséért badge-eket kaphatok, sőt versenyezhetek az applikációban felvett ismerőseimmel. (Oroszi, 2023)

A fentiekből is látszódik, hogy ezek mind-mind észrevétlenül motiválnak a megfelelő cél elérése érdekében, legyen az fejlesztésben való közreműködés, tanulás vagy éppen sport. Ugyanezt erősíti meg Pacsi és Szabó (2017) is, akik a Nike+ futó applikáció példáján mutatták be a gamifikáció alkalmazását és elterjedését, és a szerzőpáros kiemelte azt is, hogy nem csak a szórakozás, hanem a felhasználók fejlődésének követésében is komoly előrelépés volt az eszköz megjelenése.

A gamifikáció fogalmát általánosságban a 2.2 pontban, az alapfogalmak bevezetése során bemutattam. Burke (2014) szerint a gamifikáció legfontosabb célja a motiváció növelése, az elkötelezettség és az eredmények javítása. Az előbbit Krause (2015) is megerősíti, aki a gamifikáció lehetőségeit vizsgálta a felsőoktatásban, és megállapította, hogy a hallgatók jobban elsajátították a tananyagot, ha játékos elemeket építettek bele.

A játékosítás módszerének egyik kulcseleme, hogy alkalmazásával azt akarjuk, hogy „mindenki nyerjen”, de természetesen ennek lehet kollaboratív-versengő megközelítése is, ebben az esetben a résztvevők nem egyénileg, hanem csapatként versenyeznek. (Burke, 2014)

Gjertsen és szerzőtársai (2017) szerint gamifikáció egyik legfontosabb eleme a pozitív visszajelzés, mely növelheti a résztvevők adott témával kapcsolatos pozitív érzelmeit is. Emellett fontos azt is megjegyezni, hogy a játékosítással elérhetjük, hogy a képzés inkább szórakoztató, és ne csak kötelező feladat legyen. Klimmt (2009) szerint pedig a játék élvezete növeli a figyelmet és fenntartja az érdeklődést. Denning és szerzőtársai (2013) alapján a játékok alkalmazásának szintén az az előnye, hogy szórakoztatóak, és ezáltal jobban lekötik az embereket, növelik az elköteleződést, mely ráadásul ahhoz is vezethet, hogy a felhasználók önként alkalmazzák azokat, emellett lehetővé teszik kérdések felmerülését és új ötletek születését. Fromann és Damsa (2016) tanulmányukban megállapították, hogy a külső motivációnál jóval hatékonyabb a belső motivációs mechanizmus, melynek aktiválására kifejezetten alkalmas a gamifikáció. Véleményük szerint az ember ösztönösen szereti a játékos közegben meghatározó motivációs elemeket, melynek része lehet a felfedezés, a flow-élmény és a tevékenység öröme. Leaning (2015) pedig arra világított rá, hogy a felhasználók jobban elkötelezettek és motiváltak a játékos tanulás során.

McGonigal (2011) munkássága során azt emelte ki, hogy az emberek elégedettséget és pozitív érzelmeket szereznek egy játékos környezetben.

Mindezek alapján összefoglalóan elmondhatom, hogy a gamifikáció

- játék elemeket alkalmazó
- ösztönző jellegű
- elkötelezettséget növelő

- pozitív kimenetelű
- visszajelzést adó
- élmény alapú
- nem játék-környezetben alkalmazott

megoldás, mely akár munkahelyi problémák megoldására, illetve kifejezetten a biztonságtudatosság fokozására is alkalmazható.

2.5.1.1. A gamifikáció alkalmazása munkahelyi környezetben

Fromann és Damsa (2016) szerint a gamifikáció kiválóan alkalmazható az oktatásban, az egészségügyben, a kulturális területeken és munkahelyi környezetben is, alkalmazása pedig minőségi javulást eredményezhet.

Bár a gamifikációval kapcsolatban munkahelyi környezetben tapasztalhatunk ellenállást (például a menedzsment nem támogatja, mert véleménye szerint csökken a produktív munkavégzés, ha a munkavállalók „csak játszanak", illetve kockázatosnak látják az idősebb korosztály játékosított képzésben való részvételének hajlandóságát), De Freitas és Liarokapis (2011) a játékosítás pozitív munkahelyi légkör megteremtésében való közreműködését is azonosította.

Hamari és szerzőtársainak (2014) kutatása 24 empirikus tanulmányt tekintett át, és azt vizsgálta, hogy a gamifikáció hatásai hogyan függenek a felhasználóktól és a kontextustól, amelyben a technikát alkalmazták. Khan és szerzőtársainak (2011) már többször hivatkozott kutatási eredményei szerint, melynek során hét biztonságtudatosság fejlesztő módszert (oktatás, e-mail üzenetek, csoportos interaktív beszélgetések, hírlevelek, videojátékok, e-Learning anyagok és plakátok) hasonlítottak össze, a videojáték, mint gamifikációs módszer nem végzett az élen, a leghatékonyabb technikának a csoportos, interaktív beszélgetések (gyakorlatilag tréningek, workshopok) alkalmazása bizonyult, mert ez a megközelítés pozitív hatással bírt a tudásra, az attitűdre, a normákra, a felhasználói szándékra és a viselkedésre is. Ez az eredmény azt is megerősíti, hogy a személyes interaktív programok hatékonyabbak, mint a passzív és személytelen megközelítésű képzések.

Bármilyen játékosított megoldást válasszunk, a visszajelzés nagyon fontos eleme minden gamifikációs akciónak. Ciampa (2013) szerint még a jelszóerősség-mérők visszajelzései is elérik céljukat, és erősebb jelszavak választásához vezetnek – tehát bármilyen visszajelzési mechanizmus befolyásolhatja a felhasználókat, hogy a biztonságosabb irányt válasszák.

A játékosítást nem csak információbiztonsági oktatások során alkalmazzák a munkahelyen, hanem számos más képzés támogatására, sőt a munkavégzés hatékonyságának fokozására is.

A TalentLMS 2019-es „Gamification at Work” című felmérése (TalentLMS, 2019) alapján a megkérdezett munkavállalók 89%-a érzi magát produktívabbnak és 88%-uk boldogabbnak a munkahelyén a gamifikációs módszerek alkalmazásának köszönhetően. A megkérdezettek 33%-a mondta, hogy több játékosítást szeretne a képzésekben. A kutatásból az is kiderül, hogy az eredmények alapján a gamifikációs képzésben részesülők 83%-a érzi magát motiváltnak, míg a hagyományos módszereket a megkérdezettek mindössze 28%-a értékelte így. A klasszikus képzésben részesülők 49%-a unatkozott az oktatások alatt, 12%-uk pedig nem volt produktív, ezzel szemben a gamifikációs programok résztvevőinek csak 10%-a unatkozott, és csupán 3%-uk mondta, hogy nem produktív a képzés után. Az eLearning Industry 2020-ban folytatott kutatása alapján (Finances Online, 2021) a munkavállalók 71%-a vélte úgy, hogy a gamifikáció az energiaszint növeléséhez vezet, és a megkérdezettek 66%-a érezte azt, hogy a munkahelyi gamifikációs módszerek csökkentették a stressz szintjét.

A fent bemutatott eredmények alapján elmondható, hogy a gamifikáció segíthet a felhasználók elkötelezettségének, motivációjának és termelékenységének javításában, a játékalapú módszerek pedig pozitív hatással vannak a teljesítményre és javítják a tudásmegosztás hatékonyságát is. Djaouti és szerzőtársai (2011) szerint a gamifikációs módszerek a legkülönbözőbb területeken jelennek meg, nemcsak az oktatásban, hanem például az egészségügyben, a védelemben, sőt a politikában is. A játékosítás elemeit a szervezetek számos területen alkalmazzák, mint például az új termékek, ügyfélmegoldások bevezetése, a fejlesztés, de akár a HR és projektmenedzsment folyamatok hatékonyságának növelésében is – sőt akár a felhasználók biztonságtudatosságának fokozásában is alkalmazhatóak.

2.5.1.2. A gamifikációs lehetőségek tipizálása

A gamifikációs megoldások között megkülönböztethetőek a játékosítást alkalmazó elemek, illetve a játék-alapú tanulás, illetve az úgynevezett „serious game”-ek, vagy komoly játékok lehetőségei. Ezek sokszor a szakirodalomban is nagyon nehezen különböztethetőek meg, sőt az egyes besorolások is vitatottak, így a következőkben bemutatom ezek meghatározását és főbb lehetőségeit.

Az előzőleg bemutatott, klasszikus gamifikációs eszközök leginkább a képzések vagy más programok teljesítésének „jutalmaként” szolgálnak. Ezzel szemben a játék-alapú tanulás (Game-Based Learning, vagy röviden GBL) olyan módszer, amely a játékokat oktatási eszközként használja, így a gamifikáció és a játékalapú tanulás közötti fő különbség a játékmechanika integrálása a képzési tartalomba. (Findlay, 2016) Patrício és szerzőtársai (2018) ennek mentén négyféle játék-alapú megközelítést különböztetnek meg: a tisztán játékokat, a

játékos tervezést, a komoly játékokat és a gamifikációt. Kutatásom során nem találtam olyan egyértelmű szabványt vagy szabályozást, mely pontos definícióval szolgálna ezek behatárolásáról, így a feldolgozott szakirodalmakból vonom le a következtetéseket a lehetséges típusokkal kapcsolatban.

De Freitas és Liarokapnis (2011) a komoly játékokat úgy határozzák meg, mint olyan számítógépes játékok, amelyeknek oktatási és tanulási aspektusa van, és nem csupán szórakoztatási célokat szolgálnak. Chen és Michael (2005) meghatározása szerint ezek olyan játékok, amelyeknek nem a szórakoztatás, az élvezet vagy a kikapcsolódás az elsődleges célja. Ami ezen típusok alkalmazhatóságát illeti, Kato és szerzőtársai (2008) kutatásaik során megállapították, hogy a komoly játékok alkalmazásával korosztálytól függetlenül lehet motiválni a résztvevőket és pozitív eredményeket lehet elérni a fejlődésben.

A komoly játékok célközönsége nagyon különböző lehet: diákok, egyetemisták vagy végzős hallgatók, szakemberek, szervezeti környezetben pedig az általános felhasználóktól kezdve egészen a vezetőség tagjaiig bárki, vagy akár speciális felhasználói csoportok is. Ezeknek a játékoknak a legfontosabb előnye, hogy lehetővé teszik a felhasználók számára a lehetőségek kipróbálását, olyan környezetet teremtenek, ahol következmények nélkül játszhatnak el különböző szcenáriókat, forgatókönyveket, és próbálhatnak ki különböző megoldásokat egy játékon belüli környezetben. (Hill és szerzőtársai, 2020)

2.5.2. ÁLTALÁNOS JÁTÉKOSÍTÁST ALKALMAZÓ GAMIFIKÁCIÓS MÓDSZEREK

A disszertációhoz készített, 3. fejezetben bemutatott kutatásom is megerősítette, hogy a felhasználók általában szeretik a rejtvényeket, találós kérdéseket és kvízeket, ezért jó ötlet ezeket a biztonságtudatosságot fejlesztő megoldásokként alkalmazni, akár a biztonságtudatossági képzéssel, akár más jellegű program vagy kampányelemekkel együtt, vagy külön, játékosított mérési módszerként. A játékok, illetve a játékosítás alkalmazása a hagyományos kvízjátékon vagy keresztrejtvény-fejtésen kívül számos lehetőséget rejt, akár offline, akár online megoldásban gondolkodunk.

Ha a „játékosítást” mint kifejezést akarom értelmezni, akkor ezen gamifikációs lehetőségeknél a fókuszt leginkább azokra a módszerekre helyezem, melyek során az eredeti eszköz valamilyen játékos elemmel egészül ki, és a gamifikációt inkább ösztönzésre, mint a tudás átadására használják.

Anadea (2018) szerint tipikusan ilyen, általános játékosítást alkalmazó elemeknek tekinthetők a jelvények, ranglisták, pontok vagy pontszámok, szintek és kihívások. Zichermann és Linder

(2013) a pontrendszert, szinteket, jelvényeket és díjakat, ranglistákat sorolja a gamifikációs elemek közé.

Ezek alapján én az általam tartott gamifikációs képzésben a 2. táblázatban bemutatott típusokat különböztettem meg a klasszikus gamifikációs eszközök között (Oroszi, 2023):

Elem	Meghatározás
Badge-ek, kitűzők	A felhasználó valamilyen pontszám eléréséért, valamilyen cselekmény végrehajtásáért kapja jutalmul, mellyel megkülönböztetheti magát más felhasználóktól.
Rangsor, verseny	A felhasználó pontjai vagy egyéb eredményei alapján azonosíthatja saját helyzetét a csoportban, mely ösztönzi a jobb teljesítményre.
Pontok	A felhasználó valamilyen tevékenység végrehajtásáért kapja jutalmul és gyűjtheti őket meghatározott céllal. Ide érthető például a pecsétek használata, egyéb gyűjthető eredmények osztása.
Szintek	Pontok vagy egyéb eredmények alapján előre meghatározott célok, melyek elérésével a felhasználó akár badge-et vagy más jutalmat kaphat.
Kihívások	Valamilyen tevékenység véghezvitelére ösztönző események vagy célok, melyek teljesítése esetén a felhasználó pontot, badge-et vagy más jutalmat kaphat.
Díjak, verseny	Valamilyen verseny során megszerzett virtuális vagy valós elismerés, pl. Tárgy, kupa, stb. (*Nem azért kapom, mert megcsináltam, hanem mert "jól" csináltam.*)
Ajándékok	Valamilyen feltétel teljesítése során megszerzett virtuális vagy valós elismerés, pl. Tárgy, kupa, stb. (*Azért kapom mert megcsináltam, függetlenül a teljesítményemtől.*)

2. táblázat: Gamifikációs elemek a biztonságtudatossági fejlesztésekben (forrás: Oroszi, 2023)

A bemutatott módszereket alkalmazva a résztvevők könnyen azonosíthatják fejlődésüket és eredményeiket, és egymást is motiválhatják – de nem a pontok által tanulnak. Ezen módszerek alkalmazásának lényege, hogy a felhasználók pontokat kapnak a különböző oktatásokon való részvételért, kvízek és tesztek megoldásáért, egyéb kampányelemek, játékok teljesítéséért, amelyek arra ösztönzik őket, hogy csinálják meg azokat a feladatokat, melyekért pontokat kapnak – és melyekkel nem mellesleg tanulnak. Az eredményeket pedig a szervezet intranetes oldalain, az e-Learning alkalmazásban vagy más képzési rendszerben/alkalmazásban lehet rögzíteni és nyomon követni. Emellett más típusú kampányelemek, például plakátok, képernyővédők segíthetnek a pontszerzéshez kapcsolódó tesztek megfelelő megoldásainak azonosításában, ezért a felhasználók motiváltak az információbiztonsági tudatossági kampány tartalmának és akcióinak követésében.

A TalentLMS kutatása szerint a legnépszerűbb gamifikációs módszerek közé tartozik a jelvények használata (71%), illetve a pontok vagy egyéb értékelések gyűjtése valamilyen alkalmazáson keresztül (59%), a legkevésbé elterjedt technikának pedig a szintek alkalmazása (47%) számít. (TalentLMS, 2020)

A bemutatott módszerek előnye, hogy viszonylag könnyen és költséghatékonyan bevezethetőek, gyakorlatilag a pontok publikálásához egy intranetes vagy más megosztható felület elengedő lehet, nem kell feltétlenül e-Learning integrációval megvalósítani, vagy mobilapplikáció bevezetésben gondolkodnunk. Saját tapasztalat alapján fontos viszont a

rendszeres kommunikáció és a következetes pont-osztás, a pontszerzési lehetőségek és gyűjthető értékek előzetes meghatározása, illetve a kampányelemek megfelelő időben történő egymásra építése. (Oroszi, 2023)

2.5.3. BIZTONSÁGTUDATOSSÁGI SZABADULÓSZOBA

A játék-alapú tanulás egy típusaként a biztonságtudatossági szabadulószoba is a biztonságtudatosságot fejlesztő programok egy új, lehetséges eleme. Papaioannou és szerzőtársai (2022) szerint a szabadulószobák bármilyen témára vagy témakörre készülhetnek, ezért ideális oktatási módszert jelenthetnek bármely korosztály számára, ráadásul kooperációs megközelítést alkalmaznak, tehát a játék megnyeréséhez egyben csapatmunka is szükséges. Ez munkahelyi környezetben kifejezetten hasznos lehet, ha a szervezet esetlegesen nem támogatja a versengést, vagy amennyiben csapatépítőn, egyéb közösségi programon valósítja meg a programot. A csapatmunka ráadásul az egymástól való tanulást is segíti, melyet sokszor tapasztalhatunk munkahelyi környezetben: a munkatársak előszeretettel kérnek segítséget inkább egy közeli kollégától, mint például a biztonsági területtől, de szintén előfordul, hogy más, nem szakértő munkatárs információbiztonsághoz kapcsolódó előadása, cikke, jobban felkelti a figyelmet és a megértést, mint az információbiztonsági területé. Ha a szabadulószobát meghatározott oktatási céllal alakítják ki, akkor a játékosok aktívan, akár a csapattársakkal megosztott információk alapján is tanulhatnak, ráadásul a hagyományos oktatási módszerekhez nem hasonlítható élményt nyújtanak. (Nicholson, 2018)

A biztonságtudatossági szabadulószoba a logikai és tipikusan ügyességen alapuló szabadulószoba-feladatok (például célba-dobás, vagy egy kulcs kihalászása egy akváriumból stb.) helyett kizárólag információbiztonsági ismeretekkel kapcsolatos elemeket használ. (Oroszi, 2017) A játék célja az emberi tényezőn alapuló kockázatok csökkentése a felhasználók érzékenyítésével, az általános rossz szokások és a hiányos biztonságtudatossági ismeretek kiemelésével, illetve a biztonságtudatos viselkedés és a biztonsági szabályok betartásának fontosságának bemutatásával. A program résztvevői megtapasztalhatják, hogy milyen könnyű az emberi tényezőn alapuló támadásokat végrehajtani, ha a felhasználó nem elég biztonságtudatos. (Oroszi, 2017) Az ilyen jellegű tudatosságnövelő akciók előnye, hogy támogatják a csapatépítést, javítják a kritikai gondolkodást, tesztelik a problémamegoldó készséget, segíthetnek a valós környezetek szimulálásában, és nagyfokú testre szabási lehetőségekkel rendelkeznek. (Karagiannis és szerzőtársai, 2020) A szabadulószoba alkalmazásának további előnye, hogy lehetővé teszi a visszajelzést, mely nagyon fontos oktatási funkció, a játékosok tájékoztatást kaphatnak a végén arról, hogy mi volt a helyes

megfejtés, és miért kell a kapcsolódó ismereteket elsajátítani. (Papaioannou, 2022) Az oktatási célú szabadulószobák kialakításánál nagyon fontos arra figyelni, hogy a kijutás célja illeszkedjen a tanulási célhoz és ne a klasszikus kvízek és más jellemző elemek domináljanak. (Nicholson, 2018)

Schneider és Zanwar (2020), Clarke és szerzőtársai (2017), valamint Heikkinen és Shumeyko (2016) publikációja alapján a következő ajánlásokat gyűjtöttem össze szabadulószoba tervezéséhez:

- **Résztvevők**: A játékban résztvevő felhasználók igényeinek elemzése és megértése az első legfontosabb lépés. A résztvevők körének megismerése segít a szerkezet, a nehézségi szint, az időtartam, valamint a létszám eldöntésében.
- **Célok**: Fontos, hogy tisztában legyünk a játék során elérendő konkrét célokkal és eredményekkel, hogy ennek megfelelően alakíthassuk a forgatókönyvet és a megszerzendő tapasztalatokat. Ezenkívül a játéktervezőknek olyan soft-skill-eket kell alkalmazniuk, mint a csapatépítés és a koordináció, a problémamegoldó és a kommunikációs készség.
- **Téma**: Minden szabadulószoba középpontjában egy téma közvetíti a narratívát, kontextust biztosít és indokolja azokat a feladatokat, amelyeket a résztvevőknek meg kell oldaniuk, illetve tapasztalniuk. A téma képezi a későbbi elemek alapját.
- **Rejtvények**: Az olyan rejtvények, mint a szórejtvények, a fizikai gyakorlatok és a csapatmunkát, a kereteken kívüli gondolkodás képességét igénylő feladatok alkotják a játék gerincét. Lehetőség van a feladványok kombinálására, azaz az egyes megoldások összekapcsolásával megtalálják a megoldást, amely a szobából való kimenekküléshez szükséges.
- **Helyszín és felszerelés**: Gyakorlatilag minden fizikai funkciót integrálni kell a játékba. A környezetnek, amelyben a játék lebonyolításra kerül, biztonságosnak és kellemesnek kell lennie.
- **Értékelés**: A szabadulószoba értékelése és folyamatos finomítása fontos feladat a kitűzött célok elérésében.

A biztonságtudatossági szabadulószobák forgatókönyvét tekintve megkülönböztethetünk védekező és támadó szcenáriójú változatokat. Első esetben a játékosoknak hibákat, sebezhetőségeket kell javítaniuk, hogy pontokat szerezzenek, illetve azonosítsák a támadót, míg a támadó szcenárió esetén a játékosok testesítik meg az ártó szándékú hackercsapatot. (Beguin és szerzőtársai, 2019) Általában inkább a támadó szcenáriójú változatok dominálnak,

a tapasztalat azt mutatja, hogy a résztvevők izgalmasabbnak tartják azt a megközelítést, amikor egy támadó bőrébe bújhatnak.

Biztonságtudatossági szabadulószobákat tekintve rengeteg megoldás érhető el a piacon, ráadásul nem is kell feltétlenül szolgáltatásként igénybe vennünk, gyakorlatilag bárki készíthet saját megoldást, melyet a munkahelyén alkalmazni tud. Schneider és Zanwar (2020) egy olyan, **CySecEscape** nevű szabadulószoba prototípust alakítottak ki, mely kifejezetten kis- és középvállalatok számára nyújt megoldást a biztonságtudatosság fejlesztésében. A játék forgatókönyve egy pénzügyi csaláshoz kapcsolódik, a résztvevőknek 40 perc áll rendelkezésére az esemény kivizsgálására. A játék kellékei könnyen beszerezhetőek és hordozhatóak, így egyszerűen kitelepíthetőek a célközönséghez. A hasonló biztonságtudatossági szabadulószoba szolgáltatások szinte az összes hazai információbiztonsági tanácsadó cég portfóliójában megtalálhatóak hasonló paraméterekkel.

Bár Magyarországon nem jelentek meg, de a kitelepülős szolgáltatások mellett elérhetőek bérelt vagy megvásárolt eszközös, konténeres szolgáltatások is. Egy ilyen például az **Infosequre Cyber Security Escape Room** kamionja (https://www.infosequre.com/security-awareness-escape-room, utolsó elérés: 2023.03.26), a **Thales Cyber Escape Room** mobil-szabadulószobája, mely gyakorlatilag egy 1,5x2x2 méteres doboz, ami egy 10 perc alatt megoldható, bármely irodában elhelyezhető szabadulószoba élményt jelent. (https://www.thalesgroup.com/en/cyber-escape-room, utolsó elérés: 2023.03.26) A **CGI Cyber Escape** szolgáltatása szintén egy kitelepíthető, konténeres megoldás, mely felépítését és kialakítását tekintve a leginkább követi a hagyományos szabadulószobák világát és hangulatát. (https://www.cgi.com/uk/en-gb/cyberescape, utolsó elérés: 2023.03.26)

Saját, 2014-ben kialakított, először a 2015. évben rendezett Ethical Hacking konferencián kipróbálható szabadulószoba módszertanomat először 2017. májusában mutattam be egy ISACA 2. szerdai előadás során (Oroszi, 2017), majd több hazai és nemzetközi felületen is publikáltam: CyberScience 2019 (Oroszi, 2019), Dunakavics 2020/3. (Oroszi, 2020a), ISACA Journal 2020/4. (Oroszi, 2020c). A saját biztonságtudatossági szabadulószoba módszer kialakítását a disszertáció 5. fejezetében mutatom be részletesen.

A szabadulószoba hatékonyságát egyetemista hallgatók körében Borrego és szerzőtársai (2017) vizsgálták, és azt állapították meg, hogy nagyon hatékonyan tudja ösztönzni a résztvevőket a tanulásra.

2.5.3.1. Online adaptációk

Ahogyan a valós szabadulószobáknak, úgy a biztonságtudatossági szabadulószobáknak is készült online játék adaptációja, mely akár mobil applikáció formájában, akár böngészőn keresztül elérhető. A Living Security **CyberEscape Online** játékában (https://www.livingsecurity.com/security-awareness-training-games/cyberescape-cybersecurity-escape-room, utolsó elérés: 2023.03.26) a résztvevők online, közösen oldanak meg egy adott időkeretben különböző információbiztonsági feladatokat, leginkább rejtvényeket.

A DEVPOST projektek között elérhető **Cyber Security Escape Room,** Thijs Bosschert és Asby játéka, egy valósághű, 3D-s, igényes grafikai kivitelezésű felhő alapú játék, mely 25 különböző biztonságtudatossági ismeretet gyakoroltat, különböző nehézségi szinteket kínálva a játékosoknak. Ezen túlmenően a hagyományos szabadulószobák végén készített fotókhoz hasonlóan a fejlesztők létrehoztak benne egy „End-selfie" modult, valamint lehetőség van oklevél nyomtatására és az eredmények dashboard-on történő megjelenítésére. (https://devpost.com/software/cyber-security-escape-room-menx73, utolsó elérés: 2023.03.26). Magyarországon pedig a **Cyex Awareness Platform** megoldása nyújt VR támogatással rendelkező, valódi, akár realisztikus környezetben játszódó szabadulószoba élményt, a játék során a különböző szituációk pedig a felhasználó válaszai alapján változnak (https://cyex.io/cyex-platform/, utolsó elérés: 2023.03.26).

A fizikai szabadulószobák virtuális adaptációját a legjobban a **CySecEscape** példája mutatja be, mely 1.0-ás fizikai verziójából egy 2.0-ás virtuális megoldás került létrehozásra. (Löffler és szerzőtársai, 2021)

2.5.3.2. Dobozos társasjáték adaptáció

Az online adaptációk mellett szintén elterjedtek a klasszikus szabadulószobák dobozos, társasjáték formájában elérhető termékei. Ezeknek az előnye, hogy otthon, többször is lejátszható megoldások, mely egyben hátrányt is jelent, mert a legtöbbnek egy megoldása van. Természetesen a biztonságtudatossági szabadulószobák is megjelentek hasonló kivitelezésben, dobozos termékként vagy akár letölthető verzióként.

A **TPT Cyber Security Escape Room** játéka egy Power Point prezentáció alapú megoldás (https://www.teacherspayteachers.com/Product/Cyber-Security-Escape-Room-8528112, utolsó elérés: 2023.03.26) a **Cre8tive** szintén **Cyber Security Escape Room** nevet viselő megoldása pedig ugyanezt a költséghatékony megközelítést képviseli

(https://www.tes.com/teaching-resource/cyber-security-escape-room-12733865, utolsó elérés: 2023.03.26).

A szakirodalom feltárás során a vizsgált forrásokban dobozos formában elérhető megoldást nem találtam, de ez nem zárja ki ennek létezését.

2.5.4. BIZTONSÁGTUDATOSSÁGI TÁRSASJÁTÉK

A szabadulószobához hasonlóan a társasjátékok, kártyajátékok is nagyon népszerűek, a stratégiai-kooperatív társasjátékok pedig napjainkban komoly célközönséggel rendelkeznek Magyarországon. A kikapcsolódás mellett a szakértők a társasjátékok esetében is felismerték, hogy oktatási célokra is alkalmas eszközök lehetnek, és legalább koncepcionális szinten létrejöttek számos olyan, biztonságtudatosságot fejlesztő társasjátékok, amelyek az információbiztonsági ismeretek bővítésére szolgálnak. Legtöbbjük papír alapú vagy letölthető kiadvány, de találkozhatunk kereskedelmi forgalomba hozott kiadásokkal, online megoldásokkal és vegyes módszerekkel is. A „társasjáték" fogalma alatt a továbbiakban kizárólag a fizikai játékelemeket tartalmazó játékot értem, a számítógépen vagy okostelefonon keresztül játszható változatokat a 2.4.5 és 2.4.6 pontban mutatom be.

Denning és szerzőtársai (2013) alapján társasjátékok előnye, hogy azokat is elérhetik vele, akik nem szeretik a számítógépes játékokat, nincsen szükségük speciális eszközökre, nincs jelentős erőforrás-függésük, a játékosok akkor is elolvashatják az ismereteket átadó kártyákat, ha azokat nem is használják aktívan a játék során. Emellett a fizikai játékok külön előnye, hogy közösségi környezetet hoznak létre, ami elősegíti a felmerült kérdések, ötletek megvitatását, valamint alkalmasak társasági összejöveteleken való alkalmazásra is.

Információbiztonsági ismereteket fejlesztő játékok közül Adam Shostack összegyűjtött, és röviden bemutatott néhányat a weboldalán: https://adam.shostack.org/games.html. (utolsó elérés: 2021.08.08.) Az itt bemutatott játékok némelyike inkább szórakozásra szolgál, egy kicsit fűszerezve a biztonságtudatosság témáival és alapjaival, de vannak olyan komolyabb játékok is, amelyeket célirányosan használnak vállalati környezetben, és céljuk inkább a tudatosítás, mint a kikapcsolódás. Az ilyen jellegű tudatosító társasjátékok hatékonyan bemutatják, hogy mi lehet a célja és szerepe az emberi tényezőnek az információbiztonságban, így általában a játék megnyeréséhez a játékosoknak meg kell akadályozniuk különböző információbiztonsági támadásokat, biztonsági intézkedéseket kell meghatározniuk, figyelembe kell venniük a biztonságos fejlesztés, üzemeltetés szabályait, de akár egy biztonsági incidens kivizsgálását is támogathatják. A társasjátékok alkalmazásának előnye a motiváció és az elköteleződés növelése, valamint a tapasztalati úton való tanulás biztosítása. Ezek a társasjátékok nem

feltétlenül gyerekeknek, diákoknak vagy akár magánszemélyeknek szólnak, hanem inkább szervezetek alkalmazottainak, általános felhasználóknak, szakembereknek, illetve akár célirányosan vezetőknek. Cook és társai (2016) például bemutatták a **Simulated Critical Infrastructure Protection Scenarios (SCIPS)** nevű játékot, amelyet a kritikus infrastruktúrák döntéshozói számára terveztek a kibertámadások következményeinek bemutatására, valamint az információbiztonsági beruházások és ellenőrzések fontosságának kiemelésére. A Hart és szerzőtársai (2020) által bemutatott **Riskio** (https://www.riskio.co.uk, utolsó elérés: 2021.08.08.) pedig egy információbiztonsági ismereteket bővítő asztali játék 3-5 játékos számára, mely akár műszaki háttér nélkül is megoldható. A célközönségben diákok, magánszemélyek és szervezetek egyaránt megtalálhatóak. A játék elemei a következők: három játéktábla (irodai, hálózati és adatáramlási diagramok), három kártyapakli (támadás, információ, védelem). A játék szolgáltatásként érhető el, egy információbiztonsági szakértő instruktori segítsége mellett.

Vannak speciálisabb ismereteket átadó játékok is, mint például a **[d0x3d!]** (https://d0x3d.com/d0x3d/welcome.html, utolsó elérés: 2021.08.08.), mely egy nyílt forráskódú, szabadon elérhető és akár testre is szabható kooperatív társasjáték. Ez a játék elsősorban a hálózatbiztonságra fókuszál, a témák és elsajátítható tudás az ehhez kapcsolódó terminológiára, támadásokra és védelmi intézkedésekre koncentrál. A játékot Matt Leacock (a népszerű "Pandemic" játék szerzője) "Forbidden Island" című játéka ihlette. Az **OWASP Cornucopia** (https://owasp.org/www-project-cornucopia/, utolsó elérés: 2021.08.08.) a biztonságtudatossági kártyajátékok szintén speciális típusa, mivel egy meghatározott felhasználói csoport, a fejlesztők számára készült, és témája kifejezetten a biztonságos fejlesztés. A Cornucopia szerzőinek célja, hogy a játék segítse a fejlesztőket az alkalmazások biztonsági követelményeinek azonosításában és alkalmazásában. A játék ingyenesen használható, bárki letöltheti és kinyomtathatja a kártyákat, vagy akár előre nyomtatott paklit is vásárolhat. Szintén a biztonságos fejlesztést támogató játékok a Microsoft **Elevation of Privilege** című kártyajátéka (https://www.microsoft.com/en-us/SDL/adopt/eop.aspx, utolsó elérés 2023.04.03), vagy a Thinkfun kiadásában megjelent **Hacker** című társasjáték a biztonságos kódolás jegyében (https://www.thinkfun.com/learn-coding/hacker, utolsó elérés: 2023.04.03).

Kereskedelmi forgalomban is megjelent játékok közül még a **Control-Alt-Hack**-et (http://www.controlalthack.com, utolsó elérés: 2021.08.08) emelném ki, mely a Steve Jackson Games Ninja Burger című társasjátékának játékmechanikáján alapuló kártyajáték 3-6 résztvevő számára. A játék története szerint a játékosok etikus hackerek, akik auditokat végeznek és egy

biztonsági tanácsadó cégnek dolgoznak. A játék létrehozásának elsődleges célja a tudatosítás, annak érdekében, hogy a közönség jobban megértse a felhasználókat érintő információbiztonsági kockázatokat. A játékhoz kapcsolódik egy kutatás is, melynek során az Egyesült Államokban 22 oktató, akik több, mint 450 hallgatóval játszottak a játékkal, töltött ki egy kérdőíves felmérést, mely alátámasztotta, hogy a játék segítette a résztvevők biztonságtudatosságának fejlesztését. (Denning és szerzőtársai, 2013)

Beckers és Pape (2016) fejlesztettek egy társasjátékot a Social Engineering támadások elleni védekezés támogatására. A játékot először számítógépes játéknak tervezték, de Denning és szerzőtársai (2013) alapján figyelembe vették, hogy a hagyományos társasjáték azoknak is vonzó lehet, akik nem szeretik a számítógépes játékokat, ennek ráadásul nincsen hardver vagy egyéb speciális igénye, csak egy asztalra van szüksége, ezen kívül a komponensei akár önállóan is használhatóak. A játék hatékonyságát egy kutatás során vizsgálták 27 fő munkavállaló bevonásával, akik a célközönségüknek leginkább megfeleltek. A tesztek igazolták, hogy a játék bővítette a résztvevők ismereteit és egyben élezték a programot, az eredmények pedig hasznos inputokat adtak a továbbfejlesztéshez. (Beckers és Pape, 2016)

A disszertáció 6. fejezetében vizsgált, saját fejlesztésű, **SILENT SIGNAL – A biztonságtudatossági játék** című társasjáték koncepcióját 2022. májusában mutattam be a Hétpecsét szakmai fórumán. (Oroszi, 2022)

2.5.5. ONLINE ÉS VIDEOJÁTÉKOK

A biztonságtudatossággal kapcsolatos online és videojátékok tervezésének kétféle megközelítése lehet: amikor a felhasználók egyfajta tesztként használják a játékot, és nem cél a tudásmegosztás, a másik út pedig, amikor a fejlesztők játékalapú tanulási módszereket alkalmaznak, vagy a játékba képzési elemeket is beépítenek (például segédlet, tananyag). Az online vagy videojátékok a gamifikáció teljes palettáját kimeríthetik: alkalmazhatnak egyszerű, klasszikus gamifikációs elemeket, mint a kvízek, rejtvények, ezekért járó pontok, jelvények, rangok, de lehetnek olyan komoly játékok, mint a biztonságtudatossági szabadulószoba és társasjáték adaptációk.

Khan és szerzőtársai (2011) szerint a videojátékok jó megoldások a felhasználók motivációjának és elkötelezettségének javítására, de nem a leghatékonyabb biztonságtudatosság fejlesztő módszerek közé tartoznak. Mielőtt azonban munkahelyi környezetben egy online megoldás használata mellett döntünk, fontos ismerni és felmérni a kockázatokat: a játékok esetében a legtöbben a „kézzelfogható” dolgokat és a személyes

csapatmunkát szeretik, a rosszul megtervezett és nem kellően kreatív alkalmazások pedig hamar unalmassá válhatnak a játékosok számára. (Oroszi, 2020c)

A következőkben néhány információbiztonsággal kapcsolatos online vagy videojátékot mutatok be, melyek nem mobilalkalmazások, és nem biztonságtudatossági szabadulószoba vagy társasjáték adaptációk.

A **CyberCIEGE** (https://nps.edu/web/c3o/cyberciege, utolsó elérés: 2021.08.08.) egy 3D-s grafikával rendelkező szerepjáték, amely a számítógép- és hálózatbiztonságra összpontosít egy lehetséges rendszertámadás szimulálásával. (Hendrix és szerzőtársai, 2016) A megoldást a Naval Postgraduate School fejlesztette ki, és először a felsőoktatásban használták. A játékban a felhasználók egy vállalat döntéshozói, és céljuk a szervezet eszközeinek védelme, melyhez eszközöket, szervereket, hálózatbiztonsági megoldásokat kell vásárolniuk, fel kell mérniük a kockázatokat, valamint emellett küzdeniük kell a különböző kibertámadások, például a kártékony kódok, a szoftverek sebezhetőségeit kihasználó fenyegetések ellen. A játék több mint húsz forgatókönyvet tartalmaz, és az információbiztonság számos témakörét lefedi, mint például a VPN, DMZ, tűzfalak, titkosítás. (Thompson és Irvine, 2011).

Az **Anti-Phishing Phil** (https://cups.cs.cmu.edu/antiphishing_phil/, utolsó elérés: 2021.08.08.) egy szerepjáték, amely az adathalász URL-ek felismerésére összpontosít, így megtanítja a felhasználókat arra, hogyan ismerjék fel a lehetséges adathalász oldalakat. Ennek az oktatószoftvernek a gamifikációs eleme az, hogy megjelenít egy halat, amely megeszik egy kukacot, ha az egy biztonságos URL-t mutat, és elutasítja a csalit, ha az URL rosszindulatú lehet. A játék korlátozása, hogy csak hamis URL-eket és domain neveket használ, de nem vizsgálja a tartalomalapú támadásokat, így a felhasználók sebezhetőek maradnak ezekkel a módszerekkel szemben, emellett az URL szintaxisára összpontosít, anélkül, hogy foglalkozna az URL szemantikájával. (Wen és szerzőtársai, 2019)

A **What.Hack** játék prototípusát Wen és szerzőtársai (2019) fejlesztették ki. Ez az alkalmazás is az adathalász-támadások elleni védekezésre összpontosít szerepjátékos módszerekkel. Az alapvető játékmechanika szerint a felhasználóknak el kell dönteniük, hogy a megjelenített e-mailek valós megkeresések, vagy adathalász kísérletek, illetve bizonytalanság esetén segítséget is kérhetnek a játékban. A fejlesztők célja a játék létrehozásával az volt, hogy megtanítsák a játékosokat az adathalász-támadások elleni védekezésre, a fokozatosan nehezedő tesztekkel növeljék a felhasználók elkötelezettségét, és visszajelzést adjanak a biztonságtudatossági ismereteikről. A játék legfontosabb előnye, hogy olyan valósághű adathalász-támadás szimulálására törekszik, amely akár a való életben is megtörténhet. A fejlesztők kutatási eredményei szerint a What.Hackhez hasonló szituációs, tapasztalati tanulás fontos szerepet

játszik a biztonsággal kapcsolatos oktatási anyagokban, és segít a felhasználók tudatossági szintjének növelésében.

Egy másik példa a **Cyber Air Strike**, amely egy 2D-s webes alkalmazás, és a publikálása idején még csak elméleti síkon létezett, játékosokkal nem tesztelték. (Bhardwaj, 2019) A játék célja és a játékosítási mód érdekes: a felhasználónak a lehető legnagyobb távolságot kell megtenniük egy repülővel, miközben meg kell védeniük azt a különböző kibertámadásoktól. A játék több biztonságtudatossági témát is felölel, mint például adathalász támadások felismerése, vírusvédelmi ismeretek, jelszavak biztonsága. (Hill és szerzőtársai, 2020).

Magyar fejlesztésű, szolgáltatásként elérhető biztonságtudatossági online játékként a Silent Signal Kft. **Awareness Game** (https://silentsignal.hu/termekeink#ag, utolsó elérés: 2023.04.03) megoldását tudom példaként kiemelni, melynek fejlesztésében részt vettem. A játék a klasszikus gamifikációs módok (pontgyűjtés, ranglista) mellett játékos formában gyakoroltatja be egy irodai környezetben felmerülő lehetséges kockázatok csökkentését, így például a dokumentumok bizalmassági besorolásának alkalmazását, az iratmegsemmisítés fontosságát, helyes jelszó választását, gyanús levelek azonosítását. illetve a tiszta asztal, tiszta képernyő politika alkalmazását.

2.5.6. MOBILAPPLIKÁCIÓK

A mobilalkalmazások manapság még népszerűbb oktatási felületnek számítanak, sok oktatási anyagot és oktatójátékot fejlesztenek Android és iOS platformokra egyaránt. Előnyük, hogy ezek bármikor és bárhol elérhetőek a felhasználók számára, például a munkahelyen, otthon, útközben, üzleti út során. Ezek az alkalmazások általában rövid és hasznos információkat, gyors játékokat és kvízeket tartalmaznak, és kevés időt igényelnek a felhasználóktól, emellett nem csak hasznosak, de szórakoztatóak is. Az olyan tipikus gamifikációs módszerek, mint a szintek, pontszámok, jelvények stb. könnyen megvalósíthatók a segítségükkel, sőt általában ezek a mobilalkalmazások alapelemei.

A biztonságtudatosság fejlesztéséhez egy mobilalkalmazás az eddig vizsgáltak alapján a következő tartalmakkal és elemekkel rendelkezhet (Oroszi, 2023):

- hírek, hírlevelek
- videók
- képzési anyagok
- biztonságtudatossági tippek és javaslatok
- kvízek, tesztek, feladványok
- játékok (például virtuális szabadulószoba)

- jelvények, kitűzők
- rangsor és kihívások
- a szervezet információbiztonsági területének elérhetőségei vagy általános forródrótok
- incidensjelentési lehetőségek és felhasználóknak szóló riasztások

A következőkben néhány különböző megközelítésű, hazai és nemzetközi publikációkban is megjelent információbiztonsági mobilalkalmazást mutatok be.

Az **Aware** (https://aware.eccouncil.org, utolsó elérés: 2021.08.08.) az EC-Council biztonságtudatosságot fejlesztő mobilalkalmazása. Ez egy komplex, interaktív megoldás, amely képzési videókat, kihívásokat, kvízkérdéseket, rangsorokat, adathalász-szimulációkat tartalmaz a felhasználók információbiztonsági tudatosságának értékelésére. Az alkalmazás testre szabható, lehetőség van a vállalat iparágához és üzleti igényeihez igazodó, releváns témák kiválasztására.

Az **Enter - IT Security Game** (https://entergame.ch/de/, utolsó elérés: 2021.08.08.) egy Android és iOS rendszereken elérhető mobilalkalmazás, amelyet a Blindflug fejlesztett. A kirakós játékban a játékosoknak támadóként az alkalmazottak rossz szokásait és az emberi tényező gyengeségeit kihasználva kell ellopniuk a világ legnagyobb gyémántját. Emellett a technikai tudásukat is be kell vetniük, hogy minél több információt gyűjtsenek, és még közelebb kerüljenek a célhoz. A játék nagyon jó designnal és élvezetes grafikával rendelkezik, a szintek szobaként vannak ábrázolva, és az információbiztonsági ismeretek számos elemét mutatják be, mint például a Social Engineering trükkök, lehallgatás, adathalászat, kukabúvárkodás, WiFi biztonság, USB adattárolók kezelése, biztonságos nyomtatás, közösségi média. A célközönség mind a szervezetek alkalmazottai, mind a magánszemélyek, sőt még a gyerekek is.

A **NoPhish** alkalmazást Canova és szerzőtársai (2014) fejlesztették ki, és kizárólag az adathalász-támadások megelőzésére és felderítésére összpontosít. A játék Android platformon érhető el, mivel az alkalmazást fejlesztő kutatók szerint az ilyen mobil operációs rendszert használó felhasználók sebezhetőbbek az adathalász támadásokkal szemben, és nagyobb valószínűséggel válnak áldozatává a csaló megkereséseknek. A játék célja, tudatosítsa a felhasználókban az URL-ek megtekintését és ellenőrzését, melynek érdekében pedig tíz szintet tartalmaz, amelyek mindegyike egy-egy URL-hamisítási trükköt mutat be. Minden szintnek van egy oktatási blokkja és egy gyakorlati része, amikor a felhasználók tesztelhetik tudásukat, és eldönthetik, hogy a megjelenített URL megbízható webcím vagy adathalász-támadás.

Scholefield és Shepherd (2019) egy Android platformon is futó szerepjátékos kvízalkalmazás prototípusát fejlesztette ki. A fejlesztők célja az volt, hogy felmérjék, mennyire lehet hatékony

egy mobilalkalmazás a biztonságtudatosság javításában, azon belül is kizárólag a jelszavak biztonságára koncentrálva. Az alkalmazás teljesen gamifikációs megközelítésű: az arany lovag (a játékos) és a sötét lovag harcolnak egymás ellen. A harc menete az, hogy a játékosnak arany lovagként helyesen kell válaszolnia a megjelenő kvíz-kérdésekre, ebben az esetben a sötét lovag életpontokat veszít, rossz válasz esetén pedig a játékos teszi ugyanezt. Ha valamelyik lovag elveszíti az összes életpontját, a játék véget ér. A felhasználók a képernyőn láthatják előrehaladásukat, eredményüket pedig a ranglistán tekinthetik meg. A játékhoz egy kutatás is készült, amely az alkalmazás hatékonyságát vizsgálta. A felmérés egy 5 pontos Likert-skálát használt, és az alkalmazás ismeretét, hasznosságát és élvezetességét mérte. A kutatást készítők következtetése az volt, hogy a gamifikációs módszerek és a szerepjátékos kvízalkalmazások pozitív visszajelzést kaptak a résztvevőktől, és a játékosok úgy érezték, hogy a játék használata után biztonságtudatosabbak lettek.

A bemutatottakon kívül több hasonló mobilapplikációt is azonosíthatunk, melyek egy része korlátozottan elérhető, vállalati alkalmazás. Hazai, biztonságtudatosságot fejlesztő alkalmazás a 9-13 éve korosztály számára készült **Mongu for Teen** applikáció, mely a mobileszközök és közösségi média felületek biztonságtudatos használatára edukálja eredményesen a felhasználóit. (Legárd, 2021)

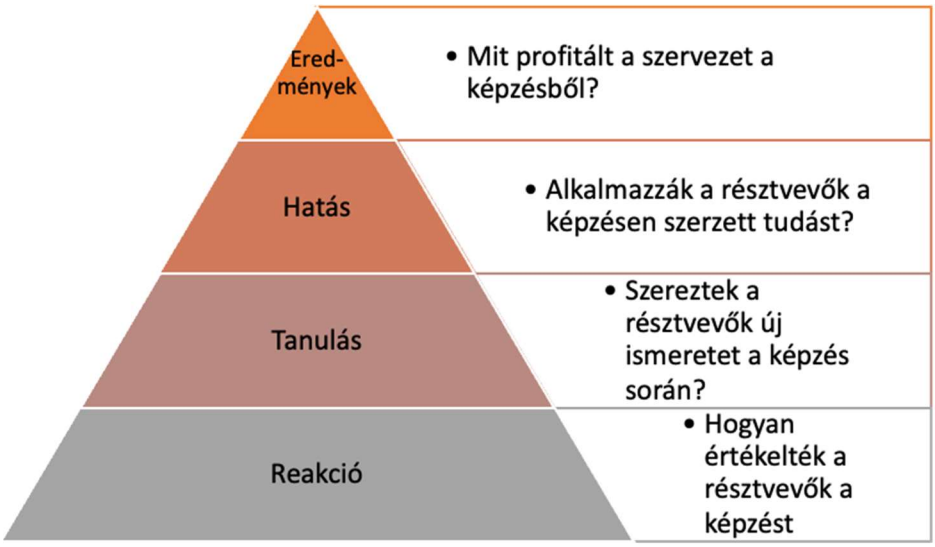
2.6. A KÉPZÉSI ÉS BIZTONSÁGTUDATOSSÁG FEJLESZTÉSI MÓDSZEREK HATÉKONYSÁG MÉRÉSÉNEK LEHETŐSÉGEI ÉS EREDMÉNYEI

Disszertációmnak kifejezett célja a különböző, részben fentiekben is bemutatott biztonságtudatossági fejlesztési lehetőségek hatékonyságának vizsgálata, és annak megállapítása, hogy mennyire alkalmazhatóak a gamifikációs módszerek a biztonságtudatosság fejlesztésére. Mielőtt azonban saját kutatásom eredményeit bemutatnám, összegyűjtöttem és megvizsgáltam néhány általános, illetve kifejezetten biztonságtudatossági képzések hatékonyság-mérésére vonatkozó publikációt és módszert.

2.6.1. ÁLTALÁNOS KÉPZÉSEKRE VONATKOZÓ HATÉKONYSÁG-MÉRÉSEK

A biztonságtudatossági képzések hatékonyságának vizsgálata előtt megnéztem, hogy általánosságban milyen lehetőségek vannak a képzések hatékonyságának mérésére, és mit alkalmaznak leggyakrabban Magyarországon a különböző oktatások értékelésére és azok hogyan kerülnek megvalósításra.

Legnépszerűbb módszerként (Durugy, 2019; Bálity és szerzőtársai, 2020; Márkus és Rácz, 2018; Poór és szerzőtársai, 2018) a Kirkpatrick-modellt (Kirkpartick és Kirkpatrick, 2006) azonosítottam, mely négy egymásra épülő szint mentén értékeli a képzések sikerességét, melyeket a 2. ábra mutat be.



2. ábra: A Kirkpatrick-modell bemutatása (forrás: saját szerkesztés Kirkpatrick és Kirkpatrick, 2006 alapján)

Ennek mentén a saját kutatásom esetében megállapítottam, hogy a tervezett felmérésemmel csak az első és a második szintet tudom mérni, tehát a biztonságtudatossági képzési módszerekre adott reakciót (mennyire nyeri el az adott módszer a résztvevők tetszését) és a tanultakat tudom vizsgálni hatékonyság szempontjából (vagyis, hogy a résztvevők új ismeretekkel távoztak-e a képzésről, illetve amennyiben igen, mennyi új tudásra tettek szert). Ugyan ezt a második lépcsős felmérést, a viselkedési hatás szintjét egy hónappal később is meg tudom ismételni, a hatást, vagyis, hogy tényleg alkalmazzák is a tanultakat, kizárólag valamilyen szimulációs teszt vagy Social Engineering audit keretein belül tudnám megvalósítani – ez azonban egy 300 fős mintán nagyon erőforrás igényes vállalkozás lett volna, így ezt a későbbiekben egy külön felmérés keretein belül érdemes megvalósítani. Ahogyan Poór és szerzőtársai (2018) is kiemelték, a 3. és 4. szinteken akkor lehet mérést folytatni, ha az értékelők a képzési program előtt és után is kapcsolatban vannak a résztvevőkkel és az őket foglalkoztató szervezetekkel, és lehetőség szerint interjú vagy a megfigyelés módszerét tudják alkalmazni a felmérés során. Ennek megfelelően az eredményesség, vagyis szervezeti hatás mérésére sem nyílt lehetőségem.

2.6.2. BIZTONSÁGTUDATOSSÁGI KÉPZÉSEKRE VONATKOZÓ HATÉKONYSÁG-MÉRÉSEK

Kifejezetten biztonságtudatossági programokra vonatkozó hatékonyság-mérést bemutató publikációkat is találtam, melyek hasonló módszerekkel mérték az általuk vizsgált különböző képzési lehetőségek hatékonyságát.

Khan és szerzőtársai (2011) hét különböző biztonságtudatosságot fejlesztő oktatási módszer hatékonyságát vizsgálták: oktatási prezentációk, e-mail üzenetek, csoportos beszélgetések, hírlevelek, videójátékok, CBT (Computer-Based Training) és a poszterek szerepeltek a felmérésben. A vizsgálatot a KAB modell (Baranowski és szerzőtársai, 2003; Kruger és Kearney, 2006), vagyis a Knowledge-Attitude-Behaviour (tudás, attitűd és viselkedés) és a TPB modell, vagyis Theory of Planned Behavior (Fishbein and Ajzen, 1975) szerint végezték és 5 pontos Likert-skálán értékelték az egyes programokat. Értékelésük szerint összességében a leghatékonyabb oktatási forma a csoportos beszélgetések (workshopok) tartása, ezt követi az oktatási prezentációk (tantermi oktatások), majd az e-mail üzenetek kategóriája, tehát az ő értékelésük szerint a gamifikációs módszerek kevésbé hatékonyak.

Abawajy (2014) felmérte, hogy melyek a leginkább preferált biztonságtudatosság fejlesztési lehetőségek, és eredménye alapján a felhasználók a videó-alapú módszereket részesítik előnyben a szöveg- vagy játék-alapú megoldásokkal szemben. Ugyanakkor a szerző azt is kimutatta, hogy hatékonyság szempontjából jelentős különbségeket nem azonosított a preferált módszer, a különböző lehetőségek ugyanúgy hatékonyan fejlesztették a résztvevők biztonságtudatosságát adathalászat témában.

Tschakert és Ngamsuriyaroj (2019) a videó-, játék- és szöveg-alapú képzések, valamint a személyes oktatások hatékonyságát, illetve ezek kombinációit vizsgálták az adathalász támadásokkal szembeni ellenállóképesség növelésének vonatkozásában. Ehhez a tesztcsoportoknak a képzések előtt, illetve után tesztlevelet küldtek, illetve egy kérdőívet is kitöltettek a résztvevőkkel, melyben megkérdezték a véleményüket a képzésről, illetve arról, hogy fejlődött-e a biztonságtudatosságuk. Eredményeik alapján a felhasználók leginkább a személyes, tantermi képzéseket, illetve a videó-alapú képzéseket preferálják, de nem tapasztaltak jelentős különbséget a vizsgált módszerek hatékonysága között.

Legárd (2020) azt vizsgálta, hogy a belső PR eszközök hogyan használhatóak biztonságtudatossági fejlesztések céljából, és arra a megállapításra jutott, hogy a tudatosítási programok tekintetében nem határozható meg egy minden szervezetre érvényes megoldási javaslat, amely egyformán hatékony és sikeres, a tudatosító programokat minden szervezetnek saját magára kell szabnia és változatos kommunikációs csatornákat kell alkalmaznia.

2.7. LEVONT KÖVETKEZTETÉSEK

A szakirodalom feltárást követően a következőket állapítottam meg, és az alábbi következtetéseket vontam le:

- A biztonságtudatosság fejlesztését a saját érdeken és belső szabályozáson túl a legtöbb hazai szervezet számára valamilyen jogszabály előírja. Ezek azonban minimális követelményeket tartalmaznak, az oktatások módjára nem alkalmaznak semmilyen kitételt.
- A gamifikációs biztonságtudatosság-fejlesztő megoldások nemzetközi szinten elterjedtek, hazai viszonylatban pedig egyre inkább megjelennek legalább vizsgálat, illetve szolgáltatások szintjén a feltárt források alapján. Ezek alkalmazására azonban egységes módszertant, segédanyagot a publikációkon túl nem találtam.
- A szakirodalom feltárásban hivatkozott szerzők mindegyike azonosítja a játékosított módszerek előnyeit, és alkalmazhatónak véli azokat a biztonságtudatossági fejlesztések során.
- A rendelkezésemre álló, a különböző biztonságtudatosságot fejlesztő oktatási módszerek hatékonyságát vizsgáló tanulmányok nagyon eltérő eredményeket és megállapításokat mutatnak, viszont mindegyikük bizonyítja, hogy a gamifikáció képes a biztonságtudatosság fejlesztésére.
- Hazai viszonylatban nem tártam fel olyan forrást, mely kifejezetten Magyarországon vizsgálná a különböző biztonságtudatosság-fejlesztési módszerek, köztük a gamifikációs megoldások hatékonyságát.

3. A BIZTONSÁGTUDATOSSÁG FEJLESZTÉSI MÓDSZEREK HATÉKONYSÁGÁNAK VIZSGÁLATA A FELHASZNÁLÓI ÉLMÉNY TÜKRÉBEN

Disszertációmban egyik célul tűztem ki azt, hogy megvizsgálom, mely biztonságtudatosságot fejlesztő képzési módszereket hogyan értékelik a résztvevő felhasználók a felhasználói élmény szempontjából, vagyis mennyire tartják élvezetesnek a programot (Kirkpatrick-modell első szintje), valamint ezek milyen hatékonysággal fejlesztik a munkavállalók biztonságtudatossági szintjét, azaz mely módszerek fejlesztik a legtöbb felhasználó ismereteit (vagyis azon felhasználók számát, akik legalább egy új ismerettel gazdagodtak a programon való részvételt követően), illetve melyek adják át a legtöbb információt a munkavállalóknak (azaz melyik módszer adta át a legtöbb tudáselemet a munkavállalóknak), és végül összességében melyik bizonyul leghatékonyabbnak a tudás átadására (Kirkpatrick-modell második szintje).
Mindehhez egy olyan gyakorlati kutatást folytattam, melynek során a felhasználók különböző biztonságtudatosság fejlesztési programokon vettek részt, és ezek előtt, illetve után egy-egy kérdőívet töltöttek ki, melyben többek között szabadszövegesen kellett leírniuk, hogy milyen információbiztonság-tudatossági ismeretekkel rendelkeznek. A kutatást részletesen a 3.2 pontban mutatom be.

3.1. KAPCSOLÓDÓ 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.”

Ezen hipotézis igazolására vagy cáfolására a 3. fejezetben bemutatott kutatást folytattam 5 db Magyarországon elhelyezkedő, privát szektorban működő, illetve 5 db, szintén hazai állami szervezetnél, melynek során hat különböző módszer hatékonyságát vizsgáltam abból a szempontból, hogy melyik milyen mértékben bővíti a résztvevők információbiztonsági ismereteit, ezáltal feltételezhetően fejlesztve a biztonságtudatosságukat. A vizsgálat során értékelési szempont volt a különböző módszerek hatékonyságának összehasonlítása mellett az is, hogy a felhasználók mennyire preferálják az adott programot, valamint mennyire tartják

élvezetesnek (*élmény-index*), illetve hasznosnak (*hasznosság-index*) az egyes programokat, és ennek milyen hatása van a biztonságtudatossági ismeretek bővülésére (*átlagos új ismeretszám*), vagy a biztonságtudatos felhasználók számának növelésére (*legalább egy új ismeretet szerző résztvevő felhasználók aránya*).

A hipotézis igazoláshoz kifejlesztettem egy gyakorlati felmérési módszertant a biztonságtudatosságot fejlesztő módszerek hatékonyságának összehasonlítására, melyet jelen fejezetben mutatok be.

A vizsgálat során azt igazoltam, hogy a felhasználók által értékelt preferencia, felhasználói élmény, valamint a hasznosság közül legnagyobb hatással a felhasználói élmény van a hatékonyságra, vagyis a biztonságtudatossági szint fokozására, valamint a biztonságtudatosabb felhasználók számának növelésére.

3.2. A DISSZERTÁCIÓHOZ KÉSZÍTETT KUTATÁS BEMUTATÁSA

A disszertációhoz kapcsolódó, biztonságtudatossági képzési módszerek hatékonyságát összehasonlító kutatást 2021. augusztus 31. és 2023. április 6. között folytattam le tíz szervezetnél, melyek fele az állami szférába, másik fele pedig a privát szektorba tartozott. Jelen kutatásba kizárólag Magyarországon, azon belül is Budapesten vagy megyeszékhelyen elhelyezkedő vállalatokat vontam be, melyek legalább 30 fő munkavállalóval rendelkeznek (ez nem zárja ki a vizsgált módszerek kisebb méretű szervezeteknél való alkalmazhatóságát, viszont az összehasonlíthatóság miatt csak olyan szervezeteket vonhattam be, melyeknél a létszám meghaladta a kutatáshoz minimálisan szükséges 30 főt). A résztvevő szervezetek mindegyike 30 felhasználót vont be a kutatásba, akiket 6 darab 5 fős csoportra bontottam, amelyek az egyes különböző programokon vettek részt. Így a felmérés során összesen 300 fős mintával dolgoztam.

A kutatásban bármely felhasználó önként vagy delegáltan részt vehetett, a résztvevő munkavállalókkal kapcsolatban nem alkalmaztam olyan megkötéseket, mint

- nemre, korra, pozícióra vonatkozó elvárások,
- önkéntes jelentkezés vagy delegálás elvárása,
- előző biztonságtudatossági oktatáson való részvétellel, vagy annak hiányával kapcsolatos elvárások.

Egyedül azt a nem kikényszerített preferenciákat támasztottam a szervezetekkel és résztvevőkkel szemben, hogy a szervezet ne a biztonsági terület munkavállalóit delegálja a

felmérésbe, valamint a résztvevők ne közvetlenül a kutatási program előtt részesüljenek más jellegű biztonságtudatossági oktatásban.

3.2.1. VIZSGÁLT BIZTONSÁGTUDATOSSÁG FEJLESZTÉSI PROGRAMOK

A kutatásban a biztonságtudatossági fejlesztési módszerek hatékonyságának felmérése során hat, általam kiválasztott képzési módszer került vizsgálatra gyakorlati megközelítéssel:

- személyes előadás,
- online előadás,
- e-Learning,
- biztonságtudatossági szabadulószoba,
- biztonságtudatossági társasjáték,
- kiosztott kampányelemek (pl. plakát, hírlevél, stb.).

Jelen kutatás kifejezetten csak ezen hat, általam választott biztonságtudatossági fejlesztési módszerre korlátozódott, melyek kiválasztása az alábbi szempontok szerint történt:

- a kiválasztott módszerek fele igényeljen mindenképpen személyes jelenlétet,
- a kiválasztott módszerek harmada tisztán gamifikációs elem legyen,
- a kiválasztott módszerek minden szervezetnél megvalósíthatóak legyenek, speciális tudás és a szervezet részéről igényelt erőforrás, külön beruházás ne legyen szükséges az alkalmazhatósághoz (ezáltal az online játékot és a mobilapplikációt kizártam),
- a kiválasztott módszerek mindegyike limitálható, de értelmesen végrehajtható legyen egy fél órás időkeretben (ezáltal a különböző pontgyűjtő akciókat, versenyeket kizártam).

Ezen korlátozásokkal biztosítottam, hogy a végrehajtott kutatás minden szervezetre értelmezhető, ugyanakkor bármilyen más szervezetnél, eltérő módszerek bevonásával megismételhető legyen.

A biztonságtudatosság fejlesztési módszerek kiválasztása során figyelembe vettem az elmúlt évek általam tartott biztonságtudatosság fejlesztő projektjeivel szemben támasztott külső igényeket, a Khan és szerzőtársai (2011) által vizsgált módszereket, valamint Alhashmi és szerzőtársai (2021) publikációját a képzési módok csoportosításáról.

Jelen kutatás során a kiválasztott 6 módszert az alábbiak szerint értelmeztem és hajtottam végre a 30 perces blokkokban.

3.2.1.1. Biztonságtudatossági oktatás – személyes

A személyes biztonságtudatossági oktatás során klasszikus, tantermi oktatást hajtottam végre, mely egy előadásból állt. Az előadás prezentációja csak kivetítésre került, a felhasználók nem kapták meg sem előzetesen, sem utólag. Az előadás a felmérés összehasonlíthatósága miatt nem volt interaktív, kérdések feltételére az előadást követően, a végén kerülhetett sor. Ennek ellenére nem zárható ki, hogy az oktatás során előadóként, a részvevők személyes jelenléte miatt, a hallgatóság reakcióját látva az egyes témakörök eltérő mélységben kerültek átadásra (érdeklődő, illetve unatkozó reakciók).

3.2.1.2. Biztonságtudatossági oktatás – online (élő)

Az online biztonságtudatossági oktatást élőben, de távolról, az adott szervezet által támogatott videokonferencia alkalmazáson keresztül tartottam meg. A prezentáció teljes mértékben megegyezett a 3.2.1.1 pontban bemutatott személyes oktatás prezentációjával, és szintén nem került megosztásra a résztvevőkkel. Tekintve, hogy itt nem volt kötelező a kamera használata, a felhasználói reakciók kevésbé torzíthatták az egyes tudatossági elemek bemutatásának mértékét. Az előadás videón történő rögzítése nem volt engedélyezett, de tiltása technikailag nem is volt tiltott.

3.2.1.3. E-Learning

E-Learning tananyagként a 3.2.1.1 pontban bemutatott oktatási anyagot dolgoztam át, szöveges kiegészítésekkel. A prezentáció olyan formában került elkészítésre, hogy egy általános e-Learning felületet szimuláljon és akár betölthető legyen bármely e-Learning rendszerbe, azonban a kutatás során a szervezetenként azonos körülmények biztosítása érdekében a megosztása csak a PowerPoint prezentáció formában történt meg egy általam kialakított OneDrive felületen, mely csak a képzés idejére volt elérhető a résztvevőknek (azonban nem zárható ki, hogy letöltötték, vagy egyéb formában megörökítették azt).

3.2.1.4. Biztonságtudatossági kampányelemek

A biztonságtudatossági kampányelemek alatt azt a tevékenységet értettem, amikor a felhasználók különböző online és offline, biztonságtudatosságra figyelemfelkeltő információval találkoznak, például plakátokkal, hírlevelekkel. Ezek a kutatás során saját előállításban, csomagokban kerültek kiosztásra a résztvevőknek, akiknek 30 perce volt áttekinteni azokat. Ezen programelem személyesen és online is megtartható volt, és a résztvevők a kapott anyagokat megtarthatták.

A kampányelemek értékeléséhez tartozott egy különálló kérdőív, melyet a kampányok résztvevőivel töltettem ki anonim módon. A felmérés eredményéből egy, a szakirodalom

feltárásban is felhasznált tanulmány készült, mely a szervezeteket hivatott segíteni a biztonságtudatossági kampányokra való felkészülésben. (Laczkó és Oroszi, 2022)

3.2.1.5. Biztonságtudatossági szabadulószoba

A biztonságtudatossági szabadulószoba személyes formában került megrendezésre, minden szervezet számára ugyanazon forgatókönyvvel és tartalmi elemekkel. A játékidő az egyébként átlagosnak mondott 30 percben volt maximalizálva. A biztonságtudatossági szabadulószoba kialakítását és részletes bemutatását az 5. fejezet tartalmazza.

3.2.1.6. Biztonságtudatossági társasjáték

A biztonságtudatossági társasjáték személyes formában került megrendezésre. A játékidő 30 percben volt maximalizálva, mely 3-4 körre volt elegendő. A játék során a limitált időkeretre való tekintettel a cselekménykártyákat előválogattam, hogy minél relevánsabb támadásokkal nézzenek szembe a játékosok. A biztonságtudatossági ismeret-kártyák számát ez a szűkítés nem befolyásolta. A biztonságtudatossági társasjáték kialakítását és részletes bemutatását az 6. fejezet tartalmazza.

A biztonságtudatossági társasjáték értékeléséhez tartozott egy különálló kérdőív, melyet a kampányok résztvevőivel töltettem ki anonim módon, ennek eredményeit a vonatkozó részben szintén felhasználom.

3.2.2. VIZSGÁLT BIZTONSÁGTUDATOSSÁGI ISMERETEK

A kutatásban vizsgált mindegyik tudatosító módszer kitért ugyanazon 10 biztonságtudatossági ismeretre vagy ismeret-csoportra, melyek a következők:

- tiszta asztal politika
- tiszta képernyő politika
- kulcsok és felhasználó azonosításra szolgáló eszközök kezelése
- hardver eszközök biztonsága
- jelszóválasztás és jelszavak biztonsága
- iratmegsemmisítés
- adathalászat
- vírusvédelem
- közösségi média biztonságtudatos használata
- okos eszközök biztonsága

Jelen kutatás során azt tűztem ki célul, hogy olyan tíz darab biztonságtudatossági ismeret meglétét vagy hiányát azonosítsam, melyek általánosságban megjelennek a

biztonságtudatossági oktatások tematikájában. Ezek meghatározásához figyelembe vettem az elmúlt években tartott biztonságtudatossági oktatásaim során felmerült igényeket, valamint olyan ajánlásokban szereplő ismereteket, mint a Security Awareness Program Special Interest Group PCI Security Standards Council Information Supplement: Best Practices for Implementing a Security Awareness Program (2014) ajánlása, a CISA Cybersecurity Awareness Month Publications segédanyagai, valamint a szakirodalom feltárás során vizsgált gamifikációs módszerek által fejlesztett biztonságtudatossági ismereteket.

Mindezek alapján az alábbi szempontok alapján választottam ki a fent jelölt ismereteket:

- a vizsgált ismeretek fele számítógépen keresztüli, másik fele számítógépet mellőző támadási technikák megelőzésére szolgáljon,
- egy ismeret csak egyszer szerepeljen, egyik se kerüljön alsóbb rendű kategóriákra bontásra,
- egyik se tartozzon szándékosan a kutatásban résztvevő szervezetek célirányos fejlesztési témaköréhez,
- mindegyik ismeret megjeleníthető legyen minden, a kutatásba bevont fejlesztési módszer során.

Ezen korlátozásokkal biztosítottam, hogy a végrehajtott kutatás minden szervezetre értelmezhető, ugyanakkor bármilyen más szervezetnél, eltérő biztonságtudatossági ismeretek bevonásával megismételhető.

Az egyes biztonságtudatossági ismeretek különböző programokban való megjelenési formája a következő az 1. számú mellékletben kerül bemutatásra. programban a biztonságtudatossági ismeretek felmérése során szabadszöveges válaszadást alkalmaztam, emiatt természetesen az ismeretek nem feltétlenül ezekben a megfogalmazásokban kerültek rögzítésre a felhasználók által, így készítettem egy táblázatot, melyben előzetesen rögzítettem, hogy milyen jellegű válaszokat mely kategóriákba sorolok be (3. táblázat).

Ismeret	***Kapcsolódó kifejezések***
Tiszta asztal	tiszta asztal, üres asztal, elpakol, elzár, asztalon hagy, rendet rak, szekrényben tárol, bezár, nem marad ott dokumentum, clean desk, illetéktelenek hozzáférése a dokumentumokhoz
Tiszta képernyő	tiszta képernyő, clean screen, zárolás, lockolás, lezárás, jelszavazás, képernyő jelszavas védelme, képernyőkímélő indítása, illetéktelenek hozzáférése az eszközhöz

Ismeret	***Kapcsolódó kifejezések***
Kulcsok, kártyák	belépőkártya, kulcs, bezárás, iroda zárása, beléptető rendszer, illetéktelenek kizárása
Hardver eszközök	csak szervezeti eszközök, elvesztés, utazás, autóban hagyás, token, laptop, pendrive, merevlemez
Jelszavak	jelszavak használata, erős jelszó, jelszóhossz, komplexitás, konvenció, megváltoztatás, különböző jelszavak, tárolás, megjegyezni, nem leírni, nem megosztani, jelszószéf, kódok, kétfaktoros authentikáció, MFA
Iratmegsemmisítés	iratmegsemmisítő, kuka, ledarálás, égetés, szelektív hulladékgyűjtés, szenzitív iratokat gyűjtő konténer
Adathalászat	adathalász levél, gyanús levél, ismeretlen feladó, gyanús link, adathalász oldal, gyanús oldal, jelszó kérése, bankkártya adatok kérése, személyes információk kérése, adatok megadásának mellőzése weboldalon, URL ellenőrzése, feladó ellenőrzése, phishing
Vírusvédelem	vírus, kártékony kód, kártékony program, kártékony szoftver, fertőzés, malware, zsarolóvírus, ransomware, vírusvédelem, vírusirtó, gyanús levél, gyanús link, gyanús csatolmány, gyanús melléklet, ismeretlen feladó, feladó ellenőrzése, URL ellenőrzése, csatolmány ellenőrzése, melléklet ellenőrzése
Közösségi média	közösségi média, social media, Facebook, LinkedIn, megosztás, ismerősök, privát megosztás, publikus megosztás, idegenek, jelölés, követés, információmegosztás közösségi média felületen, posztolás
Telefon és okos eszközök	mobiltelefon, okostelefon, PIN kód, jelkód, számkód, alkalmazások, telefonos csalások, gyanús hívások, visszaellenőrzés, hívó fél kilétének ellenőrzése

3. táblázat: Besoroló táblázat a szabadszövegesen írt biztonságtudatossági ismeretekhez (forrás: saját szerkesztés)

Ezektől függetlenül az eltérő megfogalmazásokat egyedileg mérlegeltem és soroltam be a különböző kategóriákba.

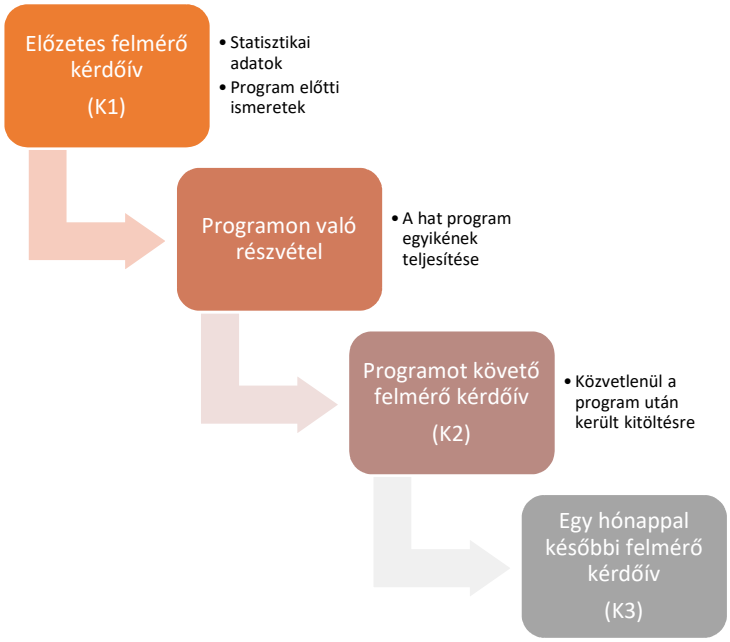
Azokat az ismereteket, melyek relevánsak voltak (tehát információbiztonsághoz kapcsolódtak), de nem szerepeltek a 10 vizsgált ismeret között, illetve egyértelműen nem voltak hozzá köthetőek, külön megjegyzésben vezettem és csoportosítottam. Ezek alapján gyakran előforduló kifejezések voltak még a következő témák:

- adatok biztonsági besorolása, osztályozása
- adatvédelem
- biztonsági mentés
- frissítések
- fizikai biztonság
- GDPR
- idegenek, látogatók
- incidensek és események jelentése
- jogosultságok
- kamera takarása
- monitor takarás, betekintés védelem
- munka és magánélet szétválasztása
- nyomtatás felügyelete
- szabályzatok elolvasása, betartása
- titkosítás, titkosított tárolás, titkosított küldés
- utazás, autó, tömegközlekedés biztonsági szabályai
- VPN használat
- Wifi biztonsága

Azon ismereteket, melyek nem voltak relevánsak információbiztonság szempontjából (például munkavédelem, tűzvédelem, környezetvédelem stb.), nem vizsgáltam és nem rögzítettem.

3.2.3. A FELMÉRÉS MENETE

A kutatás során végrehajtott felmérés a 3. ábrán feltüntetett négy lépésből állt:



3. ábra: A disszertációhoz készített kutatás végrehajtásának lépései (forrás: saját szerkesztés)

A vizsgálatban összesen 300 fő vett részt, a kérdőív (K1 és K2) a személyes programok esetében papír alapon, online végrehajtandó vagy online is végrehajtható programok esetében Google Űrlapon elektronikusan, illetve harmadik körben (K3) szervezeti igény szerint papír alapon vagy elektronikusan került kitöltetésre. Az egyes kérdőívek kitöltésére 10-15 perce volt a résztvevőknek mind a programot megelőzően, mind a képzést követően. Az utolsó körös kérdőívnél (K3) ez a limitációt nem tudtam ellenőrizni.

Mivel az egyes kérdőíveket össze kellett kapcsolnom egymással, annak érdekében, hogy lássam az egyes résztvevők fejlődését, ezért az összekapcsolhatóság végett, de az anonimitás érdekében azt egy egyedi, de könnyen megjegyezhető 13 karakteres azonosítóval kell ellátnia a kitöltőnek, mely a következőkből állt:

- Aznapi dátum (8 karakter)
- Születési dátum napja (2 karakter)
- Telefonszám utolsó 3 számjegye (3 karakter)

A három különböző kérdőív sablonját a 2., 3. és 4. számú mellékletek tartalmazzák.

A kérdőíves felmérés során az ismeretekre vonatkozóan szabadszöveges válaszadást kértem, mellyel csökkentettem annak kockázatát, hogy egy listából választva olyan ismereteket is bejelöljenek a válaszadók egy potenciálisan jobbnak vélt eredmény elérése érdekében, melyet ténylegesen nem, vagy nem olyan mélységben ismernek. Ezáltal olyan „mély” tudáselemeket sikerült azonosítanom, melyeket a felhasználók nagyobb valószínűséggel ténylegesen alkalmaznak a mindennapokban. Annak kockázatát, hogy az előzetesen kitöltött (K1)

kérdőíven bizonyos ismeretek nem jutnak eszébe a kitöltőnek, elhanyagolhatóra ítéltem, hiszen ezeket a második kérdőíven (K2) felelevenítést követően rögzíteni tudják, kontrollként pedig az utolsó, egy hónappal későbbi kérdőívben (K3) szintén megjelenhetnek.
A kérdőívekre adott válaszok kiértékelése során összehasonlításra került, hogy mely - új, vagy felelevenített - biztonságtudatossági ismeretek származnak a különböző programelemekből, illetve ezek közül melyek rögződtek tartósan, egy hónappal az esemény után. A további bekért adatok függvényében pedig értékelhettem ezek egyéb paraméterekkel való kapcsolatát, így például megkérdeztem a preferált módszereket, az adott program értékelését hasznosság, illetve élvezetesség szempontjából, melyet a továbbiakban szintén vizsgáltam.
Jelen vizsgálat nem terjedt ki arra, hogy a felhasználók tényleges biztonságtudatossági szintjét, tehát a ténylegesen alkalmazott tudásukat és képességeiket is értékeljem az egyes programokon való részvétel előtt, illetve után, például szimulációs módszerek, gyakorlati tesztek (például bejárás), vagy Social Engineering audit keretein belül. A minta nagyságát tekintve (300 fő) kizárólag a kérdőív keretein belül adott válaszaik alapján mérhettem fel jelenlegi ismereteiket, azok tényleges és helyes alkalmazását nem teszteltem, így gyakorlatilag a Kirkpatrick modell *Reakció* és *Tanulás* szintjeit tudtam mérni, a *Viselkedést* és az *Eredményeket* nem.

A kutatás tehát csak arra terjedt ki és azt bizonyította, hogy a résztvevők hogyan értékelték az egyes programokat, és mely módszer alapján tanultak új ismereteket, azt, hogy ezeket a gyakorlatban is alkalmazzák-e (tehát ténylegesen biztonságtudatosabbak) nem vizsgálta és nem igazolta. Továbbfejlesztési lehetőség a kutatás megismétlése gyakorlati vizsgálattal kiegészítve - és jelentős erőforrás igénye miatt ennek megfelelő – minta-nagyság és/vagy scope szűkítéssel (például kifejezetten adathalász megkeresésekkel szembeni ellenállóképességet fokozó képzések és adathalász szimulációk ezek előtt, illetve után).

3.2.4. A KUTATÁSI EREDMÉNYEK FELDOLGOZÁSA, KIÉRTÉKELÉSÉRE HASZNÁLT ESZKÖZÖK

A felmérés során kitöltött kérdőíveket (K1, K2 és K3) egy Excel táblázatban dolgoztam fel, melyben a következőket rögzítettem:

- szervezet azonosítója (tekintve, hogy az egyes szervezetek saját magukra vonatkozóan is megkapják a statisztikát)
- szervezet besorolása (állami/privát, saját besorolás alapján)
- szervezet elhelyezkedése (Budapest/megyeszékhely)
- munkavállalói létszám (publikusan elérhető információk alapján saját nagyságrendi besorolás)
- fő profil (publikusan elérhető tevékenység alapján saját besorolás)
- képzés módszere (amilyen programon részt vett a válaszadó, automatikusan tartalmazta a kérdőív) (K1, K2, K3)
- válaszadó azonosítója (3.2.3. pontban generált anonim azonosító) (K1, K2, K3)
- kérdőív státusza (kizárt, lezárt, nincs utolsó kérdőív)
- válaszadó neme (K1)
- válaszadó kora (30 év alatt, 30-39, 40-49, 50-59 és 60 év feletti kategóriákban) (K1)
- válaszadó pozíciója (felsővezető, középvezető, alkalmazott, külső munkavállaló) (K1)
- utolsó oktatás időpontja (elmúlt 1 évben, elmúlt 2 évben, elmúlt 3-5 évben, több mint 5 éve, soha) (K1)
- utolsó oktatás módszere (tantermi oktatás, online oktatás, e-Learning, kampány, e-mail tájékoztató, hírlevél, gamifikációs megoldás, illetve nem releváns) (K1)
- preferált biztonságtudatosságot fejlesztő módszer a program előtt (tantermi oktatás, online oktatás, e-Learning, e-mail tájékoztatás, kampány, kvízjáték, szabadulószoba, társasjáték, mobilapplikáció, online játék) – több válasz jelölhető (K1)
- szabadszöveges válaszadások a 10 biztonságtudatosság szerinti bontásban (K1)
- be nem sorolt ismeret megjegyzés (K1)
- preferált biztonságtudatosságot fejlesztő módszer a program után (tantermi oktatás, online oktatás, e-Learning, e-mail tájékoztatás, kampány, kvízjáték, szabadulószoba, társasjáték, mobilapplikáció, online játék) – több válasz jelölhető (K2)

- program hasznosságának értékelése (1= egyáltalán nem, 2 = inkább nem, 3 = inkább igen, 4 = egyértelműen igen) (K2)
- program élvezetességének értékelése (1= egyáltalán nem, 2 = inkább nem, 3 = inkább igen, 4 = egyértelműen igen) (K2)
- program ajánlása (igen, nem, nem tudom/nem szeretnék válaszolni) (K2)
- szabadszöveges válaszadások a 10 biztonságtudatosság szerinti bontásban (K2)
- be nem sorolt ismeret megjegyzés (K2)
- részvétel a programot követően más biztonságtudatossági képzésen (igen, nem, amennyiben igen, milyen eseményen) (K3)
- szabadszöveges válaszadások a 10 biztonságtudatosság szerinti bontásban (K3)
- be nem sorolt ismeret megjegyzés (K3)

Az eredményeket a következőképpen alakítottam és számoltam:

- hasznosság-index: hasznosság értékelési pontok átlaga
- élményindex: élvezetesség értékelési pontok átlaga
- biztonságtudatossági ismeretek bővítése felhasználószám szerint: legalább egy új biztonságtudatossági ismerettel rendelkező felhasználók aránya (%)
- biztonságtudatossági ismeretek bővítése megszerzett ismeretek száma szerint: új biztonságtudatossági ismeretek számának átlaga

A hagyományos statisztikai elemzéseken túl az alábbi számításokat alkalmaztam az Excelben elérhető statisztikai függvényekkel:

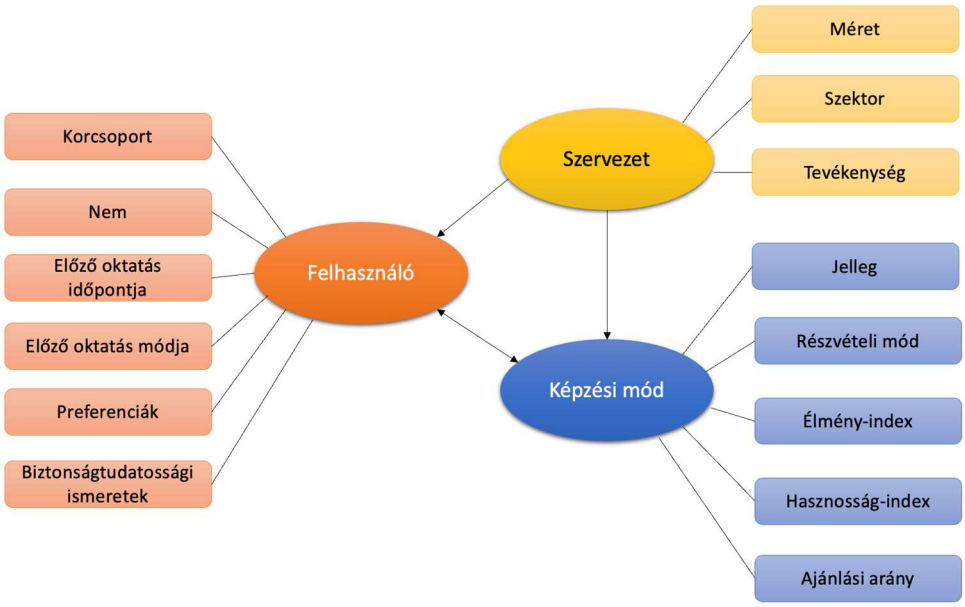
- **Korreláció számítás**: két érték közötti lineáris kapcsolat szorosságának vizsgálatára (Alkalmazott függvény: *KORREL*)
- **Spearman-féle rang-korreláció**: nem lineáris kapcsolat, illetve kiugró értékek esetén, ordinális mérési szintű változók közötti kapcsolat szorosságának vizsgálatára. (Alkalmazott függvények: *RANG.ÁTLAG* és *KORREL*)
- **Khi-négyzet próba**: nominális változók és ordinális változók közötti összefüggés vizsgálatára, ahol az elvégezhetőségi feltétel teljesült (tehát az összes cella maximum 20%-ában lehet az elvárt gyakoriság száma kevesebb, mint 5). (Alkalmazott függvény: *KHINÉGYZET.PRÓBA*)
- **Klaszterelemzés**: Az általános statisztikai elemzések mellett klaszterelemzést végeztem az IBM SPSS Statistics (továbbiakban: SPSS) alkalmazással.

3.2.5. A KUTATÁSHOZ HASZNÁLT ADATOK ÁTTEKINTÉSE

A kutatás tervezése során első lépésként olyan tényezőket gyűjtöttem össze, melyek hatással lehetnek a felhasználók biztonságtudatossági ismereteinek fejlesztésére. Vizsgálatom során a következőket tártam fel:

- Munkahelyi/szervezeti jellemzők
    - szektor (állami vagy privát szféra)
    - iparág/tevékenység
    - szervezet méret (munkavállalói létszám)
    - szervezet elhelyezkedés (Budapest vagy vidék)
- Felhasználói jellemzők
    - nem
    - korcsoport
    - pozíció/beosztás
    - utolsó oktatás időpontja (kategória besorolás)
    - utolsó oktatás jellege
- Biztonságtudatossági fejlesztési módszer
    - jellege (hagyományos vagy gamifikációs)
    - részvétel módja (online vagy személyes)
    - preferenciája a program előtt (K1)
    - preferenciája a program után (K2)
    - ajánlása
    - élmény-indexe
    - hatékonyság indexe
- Tudatossági szint mérési módja
    - Biztonságtudatosabb felhasználók száma
    - Új biztonságtudatossági ismeretek száma (felhasználónként)

Fentiekből a gyakorlati vizsgálat során a 4. ábrán szemléltetetteket alkalmaztam.



4. 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.

Szervezet szempontjából annak szektor szerinti besorolását, tevékenységét (iparág), valamint méretét vettem figyelembe a vizsgálatok során, melyek mindegyike hatással lehet a felhasználók utolsó oktatására (például eltérő előírások és gyakorlat miatt), de még akár a felhasználók nemére, illetve korára (például egészségügyi ágazatban a nők domináltak, míg informatikai fő tevékenységű vállalatoknál előfordult, hogy a férfiak vettek részt nagyobb számban). A képzés jellegére és részvételi módjára a kutatás során ezen változóknak közvetlenül nem volt hatása, hiszen minden szervezetnél mind a 6, vizsgált képzés típus szerepelt, de általánosságban ez is egy szervezeti jellemző lehet, hogy milyen típusú oktatásokat biztosítanak, így közvetett hatása lehetett az eredményekre (például adott szervezetnél az online kommunikáció preferálása miatt jobb értéket értek el a felhasználók az online oktatási módszerek során).

Felhasználók vonatkozásában kizárólag a felhasználó korát, nemét, valamint az utolsó oktatásának időpontját és módszerét vizsgáltam (utóbbit ugyan elsősorban a szervezet befolyásolja, de feltételeztem, hogy a felhasználó egyéb keretek között, vagy korábbi munkahelyén is képezhette magát). A felhasználók beosztását nem vizsgáltam a továbbiakban részletesen, mert a válaszadók jelentős része alkalmazott volt. A felhasználók iskolai végzettségére nem irányult kérdés, mert a vizsgált szervezetek jellegéből fakadóan következtetni lehetett a minimum elvárt végzettségre. A felhasználókhoz rendeltem továbbá a

preferenciát, valamint a biztonságtudatossági ismereteket is, melynek mind a növekedését (legalább 1 új ismerettel való bővülés), mind a növekedésének számosságát (átlag új tudás) vizsgáltam a későbbiekben.

Képzés típusok esetében a képzés jellegét vettem figyelembe, vagyis, hogy hagyományos megoldás, vagy gamifikációs, valamint a képzésen való részvételi módot, mely lehet személyes, online, vagy esetleg hibrid. Ezeket elsősorban nem külön bontásban, hanem a 6, vizsgált képzés szerint vizsgáltam. Emellett mindegyik módszerhez élmény-, valamint hasznosság-indexet rendeltem, valamint vizsgáltam az ajánlási arányt is.

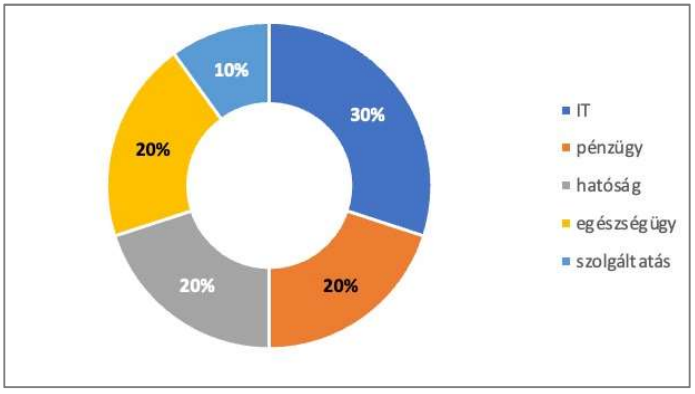
A **biztonságtudatossági szint fejlődését**, az egyes képzési típusok hatékonyságát a fent vázolt változók szerint vizsgáltam, megkülönböztetve, hogy az adott módszer hogyan hat a megszerzett új ismeretek számára (vagyis egy felhasználó hány darab új ismeretet szerez a képzés után), valamint a biztonságtudatosabb felhasználók számának növelésére (vagyis a programot követően hány felhasználó távozik legalább 1 db új biztonságtudatossági ismerettel.

3.3. A KUTATÁS ÁLTALÁNOS STATISZTIKAI ADATAI

Az alábbiakban röviden bemutatom a kutatásban anonim módon résztvevő szervezetek és felhasználók statisztikai adatait, valamint a felmérés főbb általános eredményeit.

3.3.1. A RÉSZTVEVŐ SZERVEZETEK BEMUTATÁSA

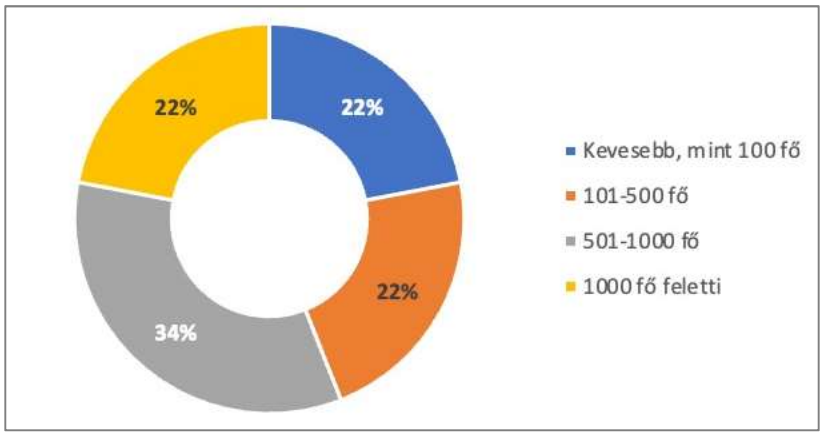
A kutatásba bevont szervezetek az eredeti céloknak megfelelően 50-50%-ban képviselték az állami, illetve a privát szférát. Tevékenység jellege szerint a vizsgált szervezetek 30%-a az IT, 20% a pénzügyi, 20%-a hatósági, 20%-a egészségügyi, illetve 10%-a a szolgáltatási szektorban helyezkedett el (1. diagram).



1. diagram: Bevont szervezetek ágazat szerinti megoszlása (forrás: saját szerkesztés)

Elhelyezkedés szempontjából 80%-uk budapesti telephellyel rendelkező, míg 20%-uk vidéki, de megyeszékhelyen elhelyezkedő szervezet volt, így a fővárosi és vidéki telephelyek jellegzetességeit nem vizsgáltam.

Munkavállalói létszám tekintetében a szervezetek 22%-ának személyi állománya nem haladta meg a 100 főt, 22%-a 101-500 fős létszámmal, 34%-a 501-1000 fős létszámmal működött, 22%-a pedig meghaladta az 1000 főt (2. diagram).



2. diagram: Bevont szervezetek méret (létszám) szerinti megoszlása (forrás: saját szerkesztés)

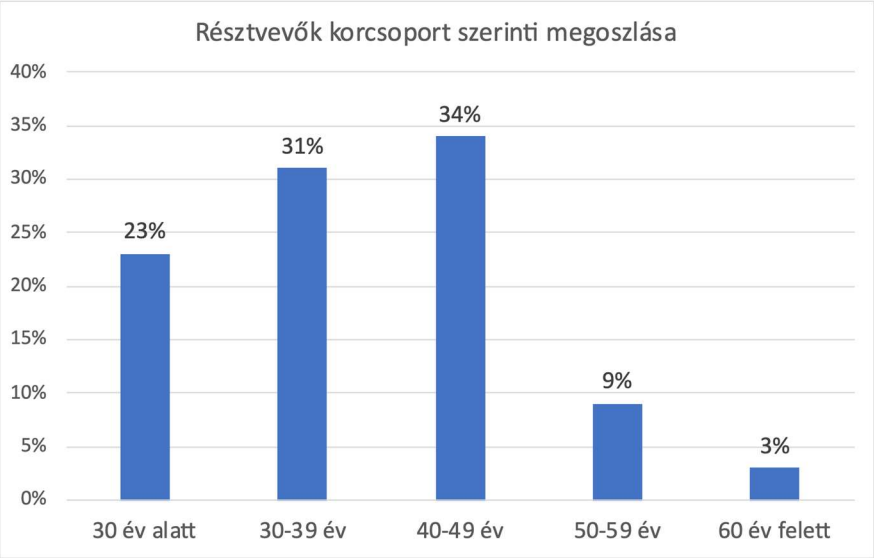
Az egyes kérdőívek kitöltésére vonatkozó szervezeti statisztikákat a 4.táblázat foglalja össze:

Szektor	Méret	K1 kérdőív (db)	K2 kérdőív (db)	K3 kérdőív (db)
Állami	100 fő alatt	30	30	14
	101-500 fő	52	52	39
	501-1000 fő	30	30	25
	1000 fő felett	30	30	17
	Összesen	***142***	***142***	***95***
Privát	100 fő alatt	27	27	12
	101-500 fő	28	28	19
	501-1000 fő	30	30	20
	1000 fő felett	57	57	48
	Összesen	***142***	***142***	***99***
MINDÖSSZESEN		**284**	**284**	**194**

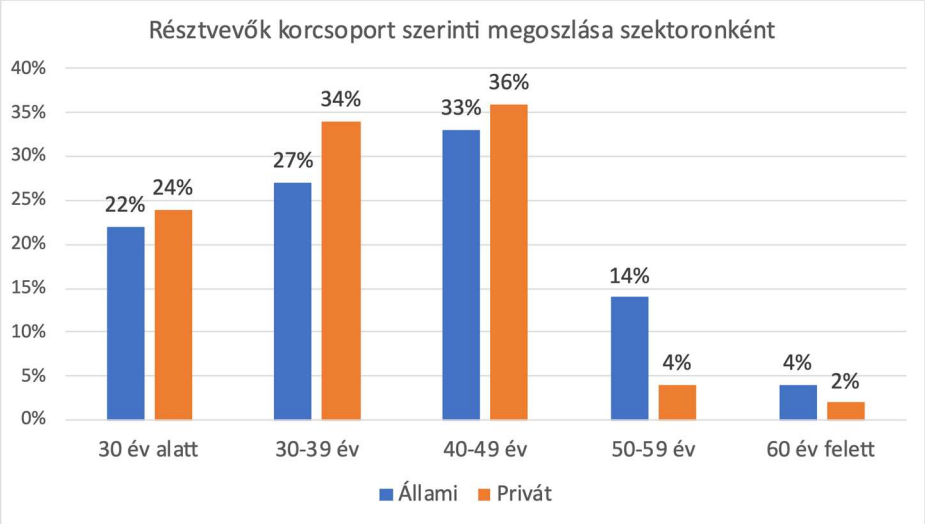
4. táblázat: A kutatás során feldolgozott kérdőívek (forrás: saját szerkesztés)

3.3.2. A RÉSZTVEVŐ FELHASZNÁLÓK BEMUTATÁSA

A résztvevők életkorát tekintve az alábbi arányokkal számolhatunk, mely alapján elmondhatjuk, hogy elsősorban a 30-49 éves korosztály képviseltette magát a felmérésben összességében (3. diagram), illetve szervezet besorolása szerint is (4. diagram).



3. diagram: A felmérésben résztvevő munkavállalók korcsoport szerinti megoszlása (forrás: saját szerkesztés)



4. diagram: A felmérésben résztvevő munkavállalók korcsoport szerinti megoszlása szektoronként (forrás: saját szerkesztés)

Nemek szerinti megoszlást tekintve összességében a résztvevők 48%-a férfi, 52%-a nő volt. Szektor szerinti bontásban itt már jelentősebbek a különbségek: állami szférában a válaszadók 56%-a férfi, míg 44%-a nő, privát szektorban pedig ez az arány megfordul és 41%-a férfi, 59%-a pedig nő.

Beosztás tekintetében a kutatás résztvevői elsődlegesen alkalmazottak voltak (83,8%), a kitöltők 11,27%-a volt középvezető, 2,46%-a felsővezető, 2,46%-a pedig külső munkavállaló. Külső munkavállalók kizárólag a privát szférában működő vállalatok esetében kerültek be a kutatásba, és érdekesség, hogy a felsővezetők leginkább az állami szférában voltak képviselve (a felsővezető válaszadók 85,71%-a az állami szférát képviselte).

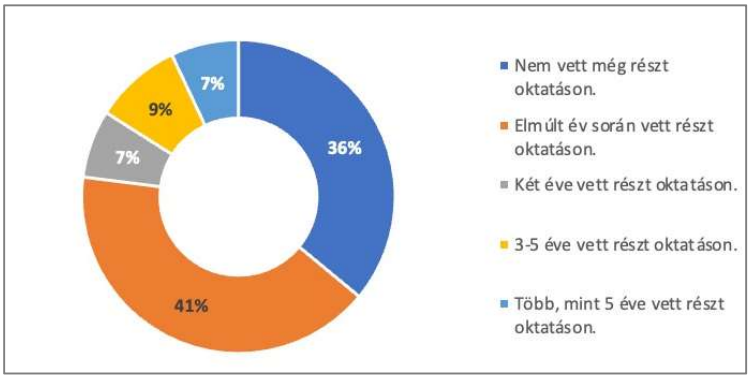
Az egyes kérdőívek kitöltésére vonatkozó felhasználói statisztikákat az 5. táblázat foglalja össze:

Nem	Korcsoport	K1 kérdőív (db)	K2 kérdőív (db)	K3 kérdőív (db)
Férfi	30 év alatt	24	24	18
	30-39 év	43	43	31
	40-49 év	52	52	32
	50-59 év	15	15	10
	60 év felett	3	3	3
	Összesen	***137***	***137***	***94***
Nő	30 év alatt	41	41	24
	30-39 év	44	44	32
	40-49 év	46	46	32
	50-59 év	10	10	8
	60 év felett	6	6	4
	Összesen	***147***	***147***	***100***
MINDÖSSZESEN		**284**	**284**	**194**

5. táblázat: Felhasználói statisztikák az egyes kérdőívek kitöltésére vonatkozóan (forrás: saját szerkesztés)

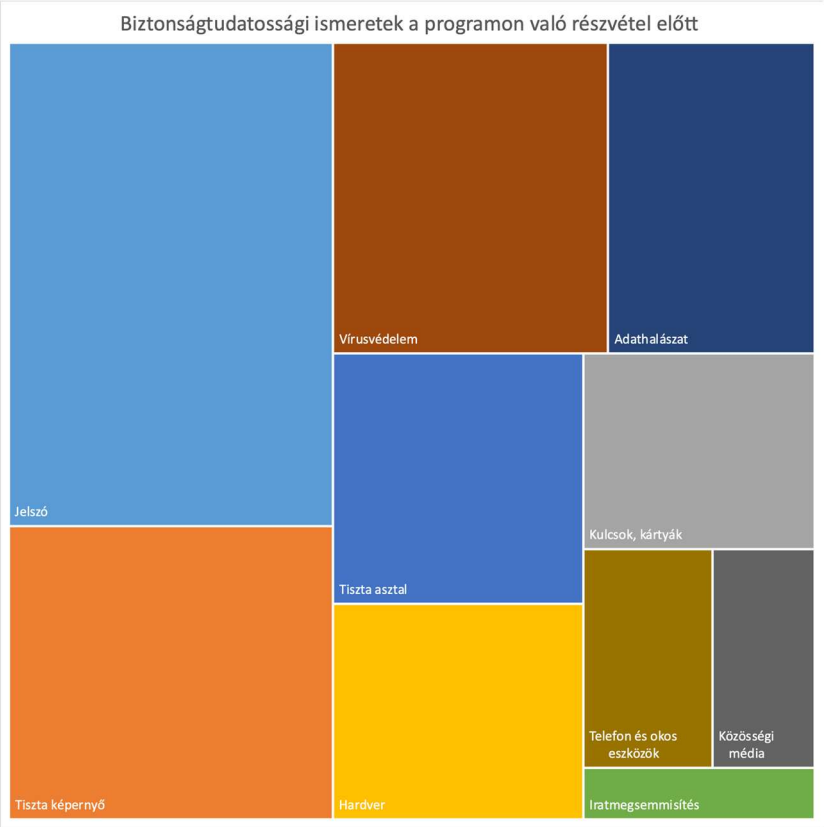
3.3.3. A RÉSZTVEVŐ FELHASZNÁLÓK BIZTONSÁGTUDATOSSÁGI ISMERETEI A PROGRAM ELŐTT

A kutatás során természetesen vizsgálnom kellett azt, hogy a résztvevők milyen biztonságtudatossági szinttel rendelkeznek, milyen ismeretekkel „indulnak". A programban résztvevő válaszadók saját bevallása szerint 36%-uk soha nem vett még részt biztonságtudatossági képzésen, 41%-uk pedig az elmúlt év során részesült ilyen jellegű oktatásban. A kérdőív kitöltőinek 7%-a nyilatkozta, hogy az elmúlt 2 évben volt része ilyen jellegű képzésben, 9%-a az elmúlt 3-5 évben, 7%-a pedig több, mint 5 éve vett részt az utolsó oktatáson (5. diagram).



5. diagram: Résztvevők utolsó biztonságtudatossági oktatásának időpontja (forrás: saját szerkesztés)

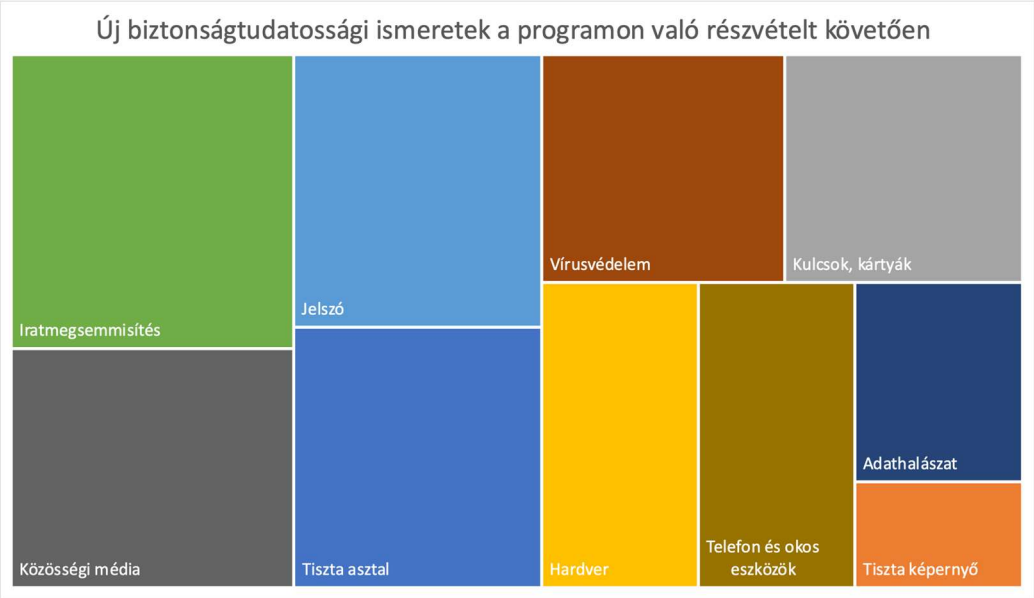
A 6. diagramon ábrázolva jól látjuk, hogy az első (K1) kérdőív eredményei alapján felhasználók leginkább a jelszavakkal kapcsolatos ismeretekkel, a tiszta képernyő fontosságával, illetve a vírusvédelemmel vannak tisztában a felhasználók. A legkevésbé domináns ismeretek az iratmegsemmisítéshez, a közösség média használathoz, illetve a telefonok és okos eszközök témájához kapcsolódtak.



6. diagram: Meglevő biztonságtudatossági ismeretek aránya vizsgált típusonként a program előtt (forrás: saját szerkesztés)

3.3.4. BIZTONSÁGTUDATOSSÁGI ISMERETEK VÁLTOZÁSA KÖZVETLENÜL A PROGRAM UTÁN

Tekintve, hogy a biztonságtudatossági programokon átadni kívánt ismeretek általánosak voltak, és nem épültek az előzetes eredményekre (ezeket a programok előtt nem is volt lehetőségem elemezni), feltételeztem, hogy a kevésbé ismert biztonságtudatossági ismereteket hatékonyan fejlesztik majd a különböző képzések, tehát új ismeretként ezeket írják majd a résztvevők a második kérdőíven (K2). Ez a feltételezésem részben be is igazolódott, a program után írt új ismeretek arányának a tree-map diagramja a következőképpen néz ki, mely szerint az iratmegsemmisítéssel és a közösségi médiával kapcsolatos fejlesztések célba értek, és valamilyen szintű javulás látható a telefon és okos eszközökkel kapcsolatos ismeretek esetén is (7. diagram):



7. diagram: Újonnan azonosított biztonságtudatossági ismeretek aránya vizsgált típusonként közvetlenül a programot követően (forrás: saját szerkesztés)

Összehasonlításképpen az egyes biztonságtudatossági ismeretek fejlődését az 5. számú melléklet is szemlélteti.

3.3.5. A KUTATÁS EREDMÉNYEI

A kutatás során 284 darab értékelhető kérdőív született, ez azt jelenti, hogy a résztvevők 94,67%-ának válaszait tudtam értékelni az első és második körös felmérések során. Kizárásra kerültek azok a résztvevők, melyeknél a felhasználó nem adott le első (K1) vagy második (K2) kérdőívet, illetve ahol ezek leadásra kerültek ugyan, de nem voltak összekapcsolhatóak (például olyan mértékben elírásra került az azonosító, hogy a rendelkezésemre álló ismeretek alapján nem tudtam javítani), vagy a felhasználók értelmezhetetlen választ adtak le. Az egy hónappal későbbi, utolsó körök kérdőívet (K3) már jóval kevesebben, a felhasználóknak pusztán 68,3%-a töltötte ki.

Programelemeken való részvétel tekintetében a következőképpen alakult az értelmezhető válaszok száma (6. táblázat):

Módszer	***Részvételi arány (%)***
e-Learning	84%
Kampányelemek	94%
Online oktatás	98%
Szabadulószoba	96%
Személyes oktatás	100%
Társasjáték	96%

6. táblázat: Részvételi arány az egyes képzéseken (forrás: saját szerkesztés)

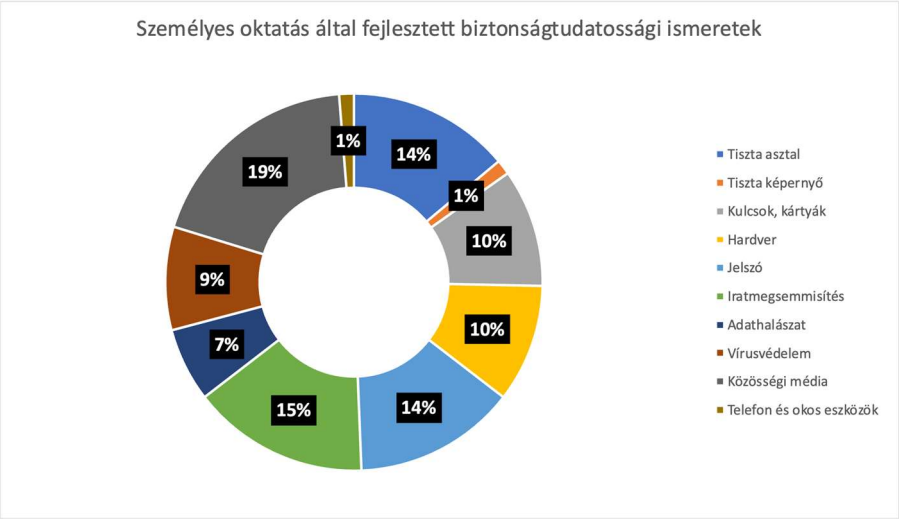
Fentiek alapján elmondható, hogy az e-Learning képzés résztvevői adták le a legkevesebb értékelhető kérdőívet, mely azt jelentette, hogy vagy nem vettek részt a programon, vagy félbehagyták a programot, vagy nem értelmezhető, esetleg nem összerendelhető adatokat adtak meg. Ez az eredmény tükrözi egyben az e-Learning-gel szembeni azon feltételezésemet, miszerint a felhasználók kevésbé tudnak figyelni az ilyen jellegű képzésekre, inkább megszakítják a tanulási folyamatot és kevésbé elkötelezettek a tanulás iránt.

3.4. AZ EGYES VIZSGÁLT PROGRAMELEMEK ÁLTAL FEJLESZTETT ISMERETEK

Mielőtt az egyes módszerek hatékonyságának értékelésére rátérek, röviden összefoglalom, hogy a korábban bemutatott hat biztonságtudatosság fejlesztési módszer hogyan fejlesztette a résztvevők biztonságtudatossági ismereteit témakörönkénti bontásban.

3.4.1. BIZTONSÁGTUDATOSSÁGI OKTATÁS – SZEMÉLYES

A személyes oktatás során leginkább a közösségi média (19%) és az iratmegsemmisítés (15%) ismeretei bővültek, melyek az előzetes eredmények alapján igencsak fejlesztésre szorultak. A módszer legkevésbé a tiszta képernyő politika és a telefon és okos eszközök ismereteinek bővítésére volt alkalmas (1%) (8. diagram).

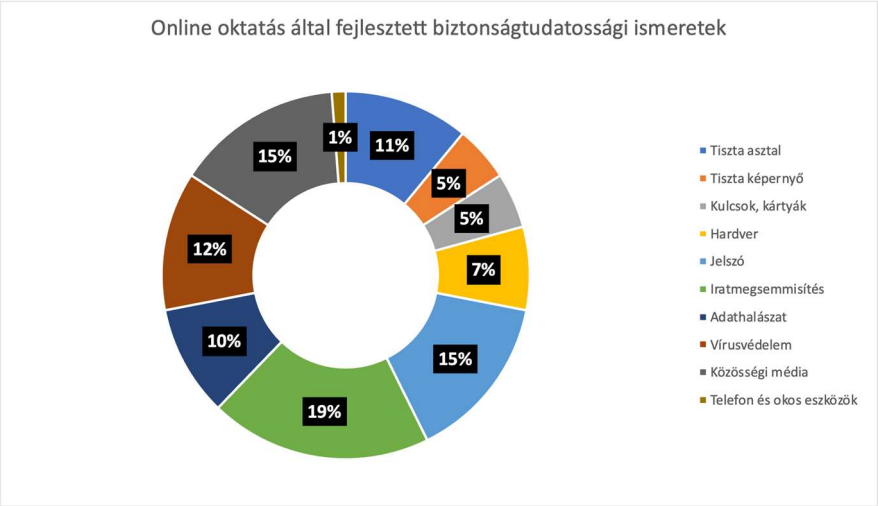


8. diagram: Személyes oktatás által fejlesztett biztonságtudatossági ismeretek közvetlenül a programon való részvétel után (forrás: saját szerkesztés)

3.4.2. BIZTONSÁGTUDATOSSÁGI OKTATÁS – ONLINE (ÉLŐ)

Az online biztonságtudatossági oktatás szintén az iratmegsemmisítést (19%) és a közösségi média (15%) biztonságtudatossági ismereteit fejlesztette, azonban pont fordított eredményességgel. Ugyanolyan alacsony hatásfokkal működött a telefon és okoseszközök

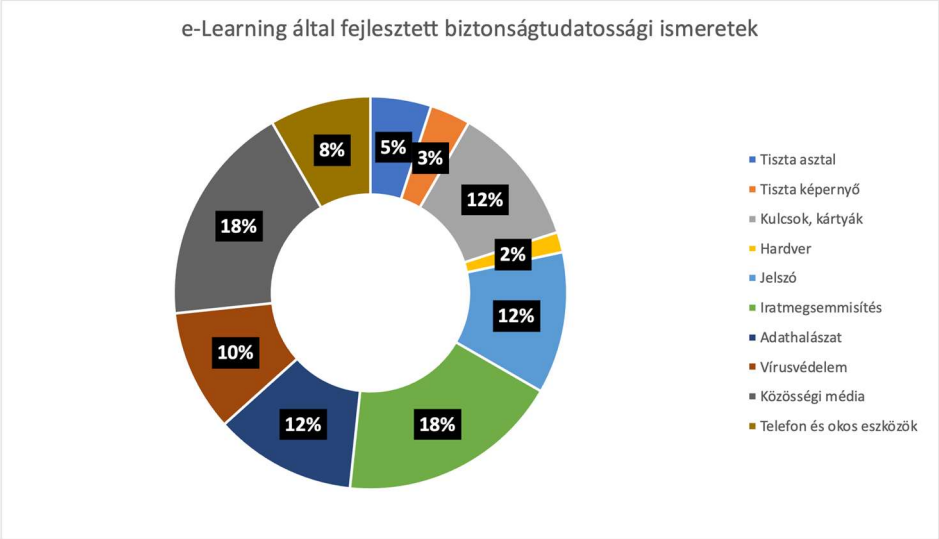
esetében (1%), és kevésbé volt hatékony a tiszta asztal, kulcsok, kártyák és hardver eszközök használatával kapcsolatos tudatosítás esetén (kevesebb, mint 10%-ot ért el) (9. diagram).



9. diagram: Online oktatás által fejlesztett biztonságtudatossági ismeretek közvetlenül a programon való részvétel után (forrás: saját szerkesztés)

3.4.3. E-LEARNING

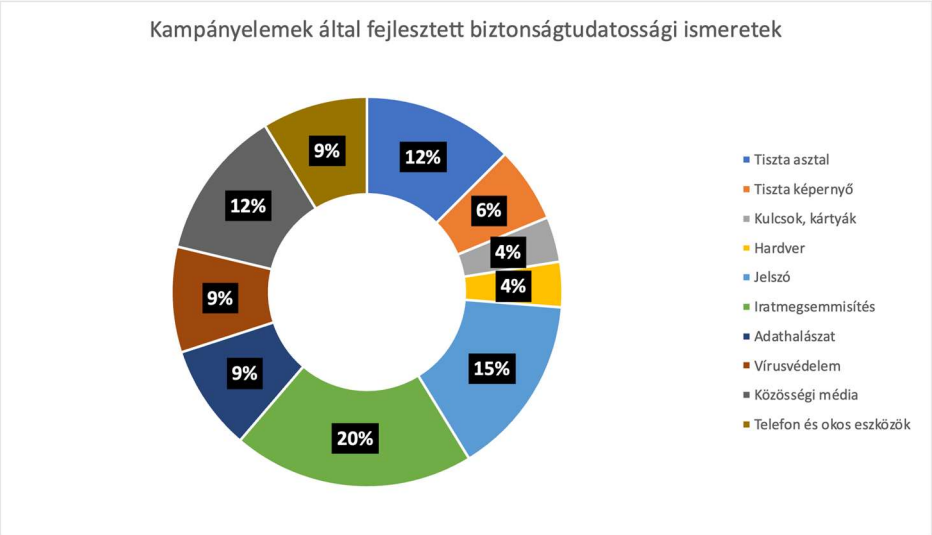
Az e-Learning esetében szintén az iratmegsemmisítés és a közösségi média jelentette az újdonságot (18-18%). Legkevésbé fejlesztett ismeretek voltak a hardver eszközökkel, tiszta képernyő politikával és tiszta asztal politikával kapcsolatos biztonsági előírások (10. diagram).



10. diagram: E-Learning által fejlesztett biztonságtudatossági ismeretek közvetlenül a programon való részvétel után (forrás: saját szerkesztés)

3.4.4. BIZTONSÁGTUDATOSSÁGI KAMPÁNYELEMEK

A biztonságtudatossági kampányelemeknél 20%-kal szintén az iratmegsemmisítés áll az élen, ezt követi 15%-kal a jelszó és 12-12%-kal a közösségi média és a tiszta asztal. 9%-os értéket ért itt viszont el a telefon és okos eszközökre vonatkozó anyag, és legkevésbé a kulcsok, kártyák, valamint a hardver eszközökkel kapcsolatos ismeretek fejlődtek (11. diagram).



11. diagram: Kampányelemek által fejlesztett biztonságtudatossági ismeretek közvetlenül a programon való részvétel után (forrás: saját szerkesztés)

A biztonságtudatossági szabadulószoba és a biztonságtudatossági társasjáték alkalmazásának hatékonyságát és általa fejlesztett ismereteket az 5. és a 6. fejezetekben értékelem.

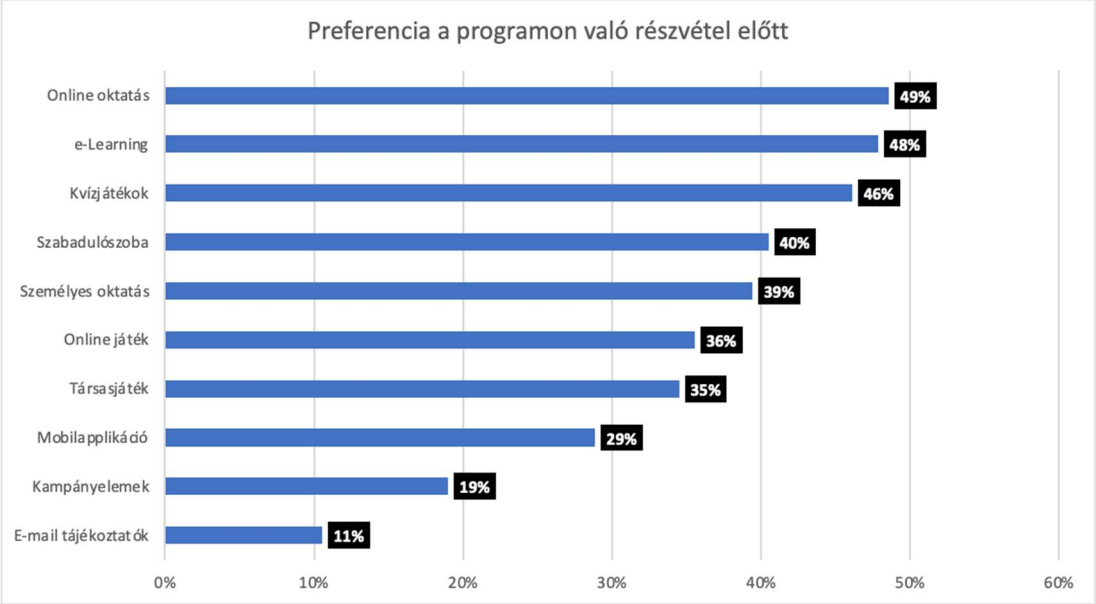
A különböző biztonságtudatosság fejlesztési módszerek összesített értékelését hatékonyság szerint a vonatkozó fejezetekben elemzem.

3.5. A FELHASZNÁLÓI PREFERENCIA ÉS A HATÉKONYSÁG KAPCSOLATÁNAK VIZSGÁLATA

Mivel a célom az volt, hogy azonosítani tudjam, milyen felhasználói értékeléssel rendelkező programok fejlesztik hatékonyan a biztonságtudatosságot, ezért első lépésként a preferencia szerinti értékelést néztem meg, és azt vizsgáltam, hogy a felhasználói preferenciának milyen hatása van az adott módszer hatékonyságára. A vizsgálat során azt értékeltem, hogy azok a felhasználók, akik előzetesen (K1) jelölték preferenciaként az adott programot, melyen részt vettek, több biztonságtudatossági ismeretet sajátítottak el, vagy többek biztonságtudatossági ismerete bővült legalább egy elemmel, mint azok, akik előzetesen nem preferált képzésben részesültek.

A kutatás során előzetesen azzal nem foglalkoztam, illetve nem tettem kikötést arra vonatkozóan, hogy a felhasználók általuk preferált, vagy nem preferált oktatási módszerben részesüljenek. Az első kérdőívben azonban megkértem a válaszadókat, hogy jelöljék be, milyen oktatási módokat preferálnak, milyen képzéseken vennének részt szívesen. Egy felhasználó több választ is megjelölhetett, illetve nem csak a kutatásba bevont módszerek közül választhatott.

Az eredményeket a következőképp alakultak:



12. diagram: A résztvevők által preferált képzési módszerek a programon való részvétel előtt (forrás: saját szerkesztés)

Ahogyan a 12. diagramon látszódik, az első kérdőíven (K1) az online hagyományos megoldások vezetnek preferencia szempontjából, de például a kvízjátékok már felkeltették az érdeklődést és a válaszadók 46%-a jelölte, hogy előnyben részesíti ezeket.

Ezt követően minden felhasználóhoz hozzárendeltem, hogy olyan programon vett-e részt, mely szerepelt a preferenciái között, vagy sem. Az eredmények alapján a válaszadók 50,35%-a számára preferált programban vett részt, 49,65%-a pedig olyan képzésen, melyet egyébként nem részesített előnyben. Megnéztem ezt követően, hogy a két csoport átlagosan hány új biztonságtudatossági ismerettel gazdagodott, illetve a résztvevők hány százalékának bővültek az ismeretei.

A vizsgálathoz a 7. táblázatot készítettem el:

Mennyire befolyásolja az előzetes preferencia a hatékonyságot?	***Preferált módszeren vett részt***	***Nem preferált módszeren vett részt***
Résztvevők száma (%)	50,35%	49,65%
Résztvevők száma, akik legalább egy új ismerettel gazdagodtak a programon való részvételt követően (%)	79,72%	79,43%
Új ismeretek számának átlaga a programot követően (db)	0,80	0,79

7. táblázat: Preferencia szerinti eredmények a programot követően (forrás: saját szerkesztés)

Ez alapján megállapítottam, hogy az, hogy a képzési program előzetesen szerepelt-e a résztvevő preferencia listáján, szemmel láthatólag nem befolyásolta jelentős mértékben a biztonságtudatossági ismereteinek növekedését, vagy a biztonságtudatosabb felhasználók számát, a két csoport között minimális eltérés azonosítható a preferált módszerek előnyére. (Ezt egy Khi-négyzet próbával is teszteltem, az eredmény 0,9594 lett, mely alapján szintén elmondható, hogy a képzési mód előzetes preferenciája és a tanulás mértéke a biztonságtudatosság terén nagymértékben függetlenek egymástól.)

A preferencia tehát nem bizonyult egy, a biztonságtudatossági képzés hatékonyságát befolyásoló tényezőnek.

Ezt követően egy hasonló táblázatot készítettem arra is, hogy a felhasználói élménynek milyen hatása lehet a képzési eredményekre, tehát összegyűjtöttem a részvételi arány mellett, hogy a résztvevők hány százaléka tanult a programból (azaz a felhasználók hány százaléka szerzett legalább 1 db új ismeretet a programot követően), illetve átlagosan hány ismeretet szereztek a résztvevők.

A 8. táblázat már nagyobb különbségeket mutat a két csoport között:

Mennyire befolyásolja a program élvezetessége a hatékonyságot?	***Élvezte***	***Nem élvezte***
Résztvevők száma (%)	84,51%	15,49%
Résztvevők száma, akik legalább egy új ismerettel gazdagodtak a programon való részvételt követően (%)	81,25%	70,45%
Új ismeretek számának átlaga a programot követően (db)	1,76	1,43

8. táblázat: Felhasználói élmény szerinti eredmények a programot követően (forrás: saját szerkesztés)

Egy Khi-négyzet próbát elvégezve ugyanezen értékekre itt az eredmény 0,0138 lett, mely azt tükrözi, hogy az új ismeretekkel gazdagodott felhasználók száma nagymértékben függ a program élvezetességétől.

Mindezek alapján a felhasználói élményt, mint az oktatás hatékonyságát befolyásoló tényezőt tovább vizsgáltam a következő alfejezetben.

3.6. A FELHASZNÁLÓI ÉLMÉNY ÉS A HATÉKONYSÁG KAPCSOLATÁNAK VIZSGÁLATA

Mivel megállapítottam, hogy az előzetes preferencia nem befolyásolja a hatékonyságot, következő lépésként az előbbiekben már igazoltan függést mutató felhasználó élményt vizsgáltam, mint hatékonyságot befolyásoló tényező. Ennek vizsgálata során azt a kérdést vettem figyelembe a második kérdőíven (K2), hogy a válaszadó „*Mennyire tartotta élvezetesnek a programot, amin részt vett*?”, melyre egy négy-pontú Likert-skálán kellett egy értéket jelölnie a résztvevőnek a programot követően.

A vizsgálat során szándékosan páros számú skálát választottam, mert mindenképpen ki szerettem volna kényszeríteni, hogy a válaszadó határolja el magát valamelyik irányba, semleges válaszadásra nem hagytam lehetőséget.

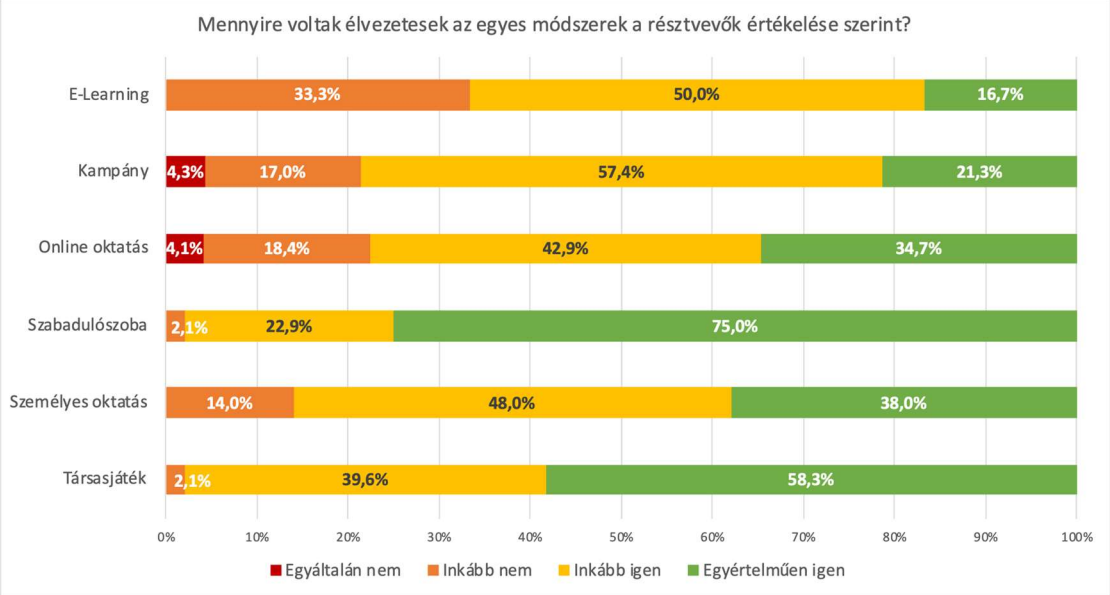
A felhasználói élmény alapján az egyes biztonságtudatossági programok a következő eredményeket érték el (adott válaszok átlaga), melyet élmény-indexként használok a továbbiakban (9. táblázat):

Program típusok és élmény-indexük	*Összességében*	*Állami szférában*	*Privát szférában*
e-Learning	2,83	3,00	2,68
kampányelemek	2,96	3,04	2,87
online oktatás	3,08	3,08	3,08
szabadulószoba	3,73	3,79	3,67
személyes oktatás	3,24	3,16	3,32
társasjáték	3,56	3,54	3,58

9. táblázat: Az egyes programtípusok élmény-indexe összességében, valamint állami és privát szféra bontásában (forrás: saját szerkesztés)

Az eredményekből látszódik, hogy legkevésbé élvezetesnek az e-Learninget (2,83) és a kampányelemeket (2,96) vélték a résztvevők mind az állami, mind a privát szféra szervezetei esetében. A vártaknak megfelelően magas értékelést kaptak a gamifikációs programok, melyek közül a legmagasabb átlagpontszámot a szabadulószoba kapta (3,73). Látható továbbá, hogy az állami szférában és a privát szférában dolgozók értékelései között nincsenek lényeges különbségek, felhasználói élmény értékelésében nincs számottevő különbség a két szektor között.

A részletes értékeléseket a 13. diagram szemlélteti:



13. diagram: Az egyes programtípusok élvezetesség szerinti értékelése (forrás: saját szerkesztés)

Az eredmények megerősítik, hogy a legjobb értékelés szempontjából is a szabadulószoba bizonyult a legélvezetesebb megoldásnak, a válaszadók 75%-a a „*Egyértelműen élvezetes*” programnak jelölte. „*Egyáltalán nem*” értékelést csak az egyébként összességében a középmezőnyben végző online oktatás (4,1%), illetve a kampányelemek (4,3%) kaptak.

Mindezen eredmények ezúton is tükrözték azt a tapasztalatomat, hogy ezen hagyományos módszerek a felhasználói élmény szempontjából már nem elegendőek a munkavállalóknak, ezért szükséges a biztonságtudatossági programok újdonságokkal történő színesítése.

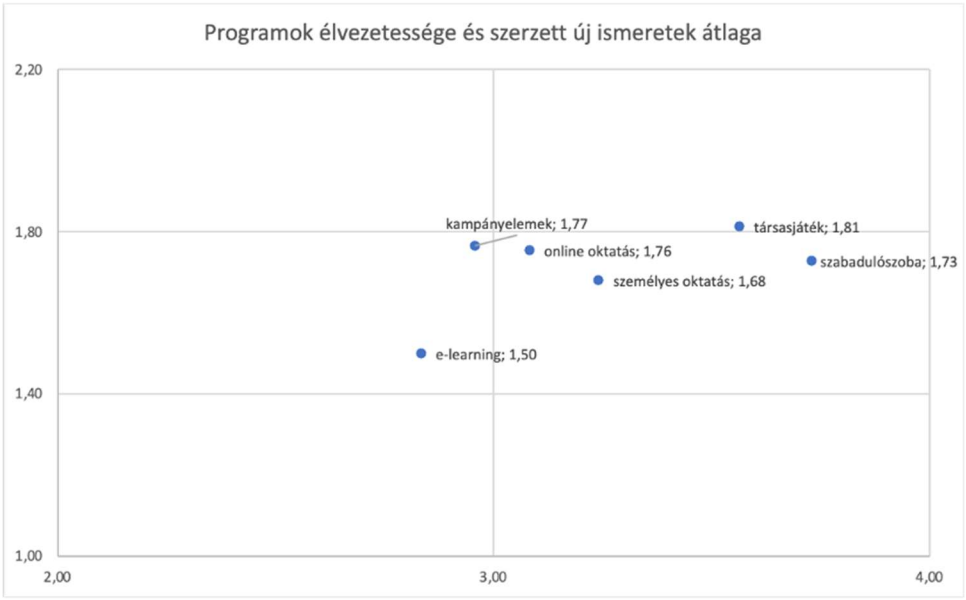
Hatékonyság szempontjából először azt néztem meg, hogy az egyes programok résztvevői hány darab új biztonságtudatossági ismerettel gazdagodtak a képzést követően, ezek átlagát szerepeltetem a 10. táblázatban:

Program típusok és új ismeretek átlaga (db)	***Összességé-ben***	***Állami szférában***	***Privát szférában***
e-Learning	1,50	1,50	1,50
kampányelemek	1,77	2,04	1,48
online oktatás	1,76	1,84	1,67
szabadulószoba	1,73	1,67	1,79
személyes oktatás	1,68	1,72	1,64
társasjáték	1,81	2,29	1,33

10. táblázat: Az egyes programtípusok során szerzett új ismeretek átlaga összességében, valamint állami és privát szféra bontásában (forrás: saját szerkesztés)

Bár az előző pontban a szabadulószoba volt a legjobbra értékelt a felhasználói élmény szempontjából, összességében a társasjátékot, mint második legélvezetesebb biztonságtudatosságot fejlesztő megoldást követően tettek szert a legtöbb biztonságtudatossági ismeretre (átlag 1,81 db), és a szabadulószoba csak a 4. helyen szerepelt, átlagosan 1,73 db biztonságtudatossági ismeretet adott. Kiemelve azonban a privát szektort, nagyon érdekesen alakulnak az eredmények, mert ott a szabadulószoba érte el a legjobb értéket (1,79 db), míg a társasjáték a legkevésbé hatékony helyen (1,33 db) végez. Állami szférában szintén a társasjáték a leghatékonyabb, 2,29 db új ismerettel, míg a szabadulószoba utolsó előtt, 5. helyet ért el, tehát kevesebb felhasználót ér el.

Az eredményeket a 14. diagramon helyeztem el, mely jól szemlélteti, hogy szemmel láthatólag sem érdemes lineáris trendet alkalmazni:



14. diagram: Az egyes programtípusok szemléltetése pont-diagramon felhasználói élmény (x, élményindex) és megszerzett átlag új tudás (y, darabszám) vonatkozásában (forrás: saját szerkesztés)

A diagram alapján látható, hogy nincsen lineáris kapcsolat az egyes programelemek értékelése, és a szerzett ismeretek számossága között, ezért Spearman-féle rangkorrelációt számoltam az Excelben az alábbi adatokra (11. táblázat):

Program típusok	***Élmény-index***	***Új ismeretek átlaga (db)***
e-Learning	2,83	1,50
kampányelemek	2,96	1,77
online oktatás	3,08	1,76
szabadulószoba	3,73	1,73
személyes oktatás	3,24	1,68
társasjáték	3,56	1,81

11. táblázat: A felhasználói élmény és az új ismeretek közötti összefüggés vizsgálata az egyes programok vonatkozásában (forrás: saját szerkesztés)

Az eredmény 0,3142 lett, mely egy gyenge pozitív kapcsolatot mutat a felhasználói értékelés és az új ismeretek számának bővülésében (ez az érték az állami szférában 0,2-re csökken). Összességében megvizsgáltam az eredmények szórását is, melyek között nincsenek kiugró értékek. (12. táblázat)

Program típusok	*Új ismeretek szórása összességében (db)*
e-Learning	1,40
kampányelemek	1,41
online oktatás	1,42
szabadulószoba	1,42
személyes oktatás	1,43
társasjáték	1,41

12. táblázat: Átlag új tudás szórása (forrás: saját szerkesztés)

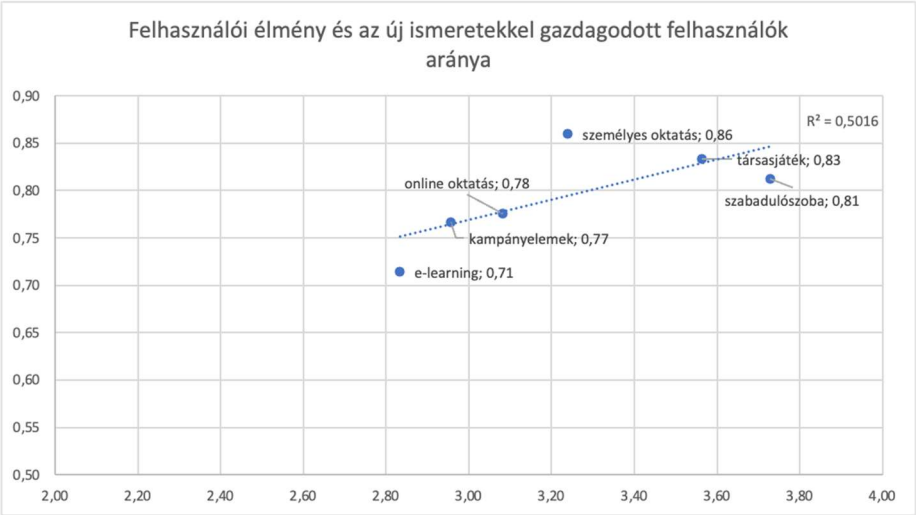
Megnéztem ezt követően, hogy az egyes módszerek mennyire voltak hatékonyak aszerint, hogy a résztvevő felhasználók hány százaléka gazdagodott legalább egy új biztonságtudatossági ismerettel, tehát a programot követő kérdőívre legalább egy új, értékelhető ismeretet írt. Az eredmények a következők lettek (13. táblázat):

Program típusok és új ismerettel gazdagodott felhasználók aránya	*Összességében*	*Állami szférában*	*Privát szférában*
e-Learning	71%	70%	73%
kampányelemek	77%	83%	70%
online oktatás	78%	76%	79%
szabadulószoba	81%	83%	79%
személyes oktatás	86%	92%	80%
társasjáték	83%	92%	75%

13. táblázat: Az egyes programokon legalább egy új ismerettel gazdagodott résztvevők aránya programonkénti bontásban (forrás: saját szerkesztés)

Ezen a téren összességében és szektoronkénti bontásban is a személyes oktatás bizonyult a leghatékonyabbnak (86% - 92% - 80%), vagyis ezen oktatási mód résztvevői közül távoztak a legtöbben legalább egy új biztonságtudatossági ismerettel. Ezt követte a felhasználói élmény szempontjából második helyen álló társasjáték (83%), mely az állami szférában holtversenyben (92%), míg a privát szektorban csak a 4. helyen (75%) végzett.

Ezekre is készítettem egy hasonló pont-diagramot, melyre az egy kiugró érték (személyes oktatás) ellenére egy lineáris trendet vettem fel, melyet azonban az R^2 értéke (0,5016) miatt el is vetettem (15. diagram).



15. diagram: Az egyes programtípusok szemléltetése pont-diagramon felhasználói élmény (x, élményindex) és fejlesztett felhasználók arányának (y, darabszám átlaga) vonatkozásában (forrás: saját szerkesztés)

Spearman-féle rang-korrelációt számoltam viszont az alábbi adatokra (14. táblázat):

Program típusok	***Élmény-index***	***Új ismeretekkel gazdagodott felhasználók aránya (%)***
e-Learning	2,83	71%
kampányelemek	2,96	77%
online oktatás	3,08	78%
szabadulószoba	3,73	81%
személyes oktatás	3,24	86%
társasjáték	3,56	83%

14. táblázat: A felhasználói élmény és az új ismeretekkel gazdagodott felhasználók kapcsolata programonkénti bontásban (forrás: saját szerkesztés)

Ennek értéke 0,7712 lett, mely erős pozitív kapcsolatot mutat a képzés által nyújtott felhasználói élmény értékelése és a biztonságtudatossági ismeretekkel gazdagodott résztvevők aránya között. (Állami szférára levetítve az eredmény 0,6087, privát szektorra pedig 0,5797.)

Ez alapján elmondhatjuk, hogy amennyiben az a célunk, hogy minél több felhasználót érjünk el és érzékenyítsünk a biztonságtudatosság iránt, érdemes megvizsgálnunk, hogy mely biztonságtudatosságot fokozó programok milyen élvezeti értékkel bírnak a munkavállalóink körében.

3.7. A FELHASZNÁLÓI ÉLMÉNY ÉS A FELHASZNÁLÓ ÁLTAL VÉLT HASZNOSSÁG, VALAMINT A HATÉKONYSÁG KAPCSOLATÁNAK VIZSGÁLATA

A teljesség kedvéért megnéztem azt is, hogy a felhasználók által hasznosnak vélt programok ténylegesen mennyire hatékonyak, illetve milyen kapcsolat van a hasznosság értékelése és az élvezetesség értékelése között, tehát amit a felhasználók jobban élveznek, azt hasznosabbnak is gondolják-e.

Ezek vizsgálata során az előbbiek mellett azt a kérdést is figyelembe vettem, hogy a válaszadó „*Mennyire tartotta hasznosnak a programot, amin részt vett*?", melyre szintén egy négy-pontú Likert-skálán kellett egy értéket jelölnie a résztvevőnek a programot követően. A vizsgálat során itt szándékosan páros számú skálát választottam, mert mindenképpen ki szerettem volna kényszeríteni, hogy a válaszadó határolja el magát valamelyik irányba, semleges válaszadásra nem hagytam lehetőséget.

A felhasználói hasznosság-értékelés alapján az egyes biztonságtudatossági programok a következő eredményeket érték el (adott válaszok átlaga), melyet hasznosság-indexként használok a továbbiakban (15. táblázat):

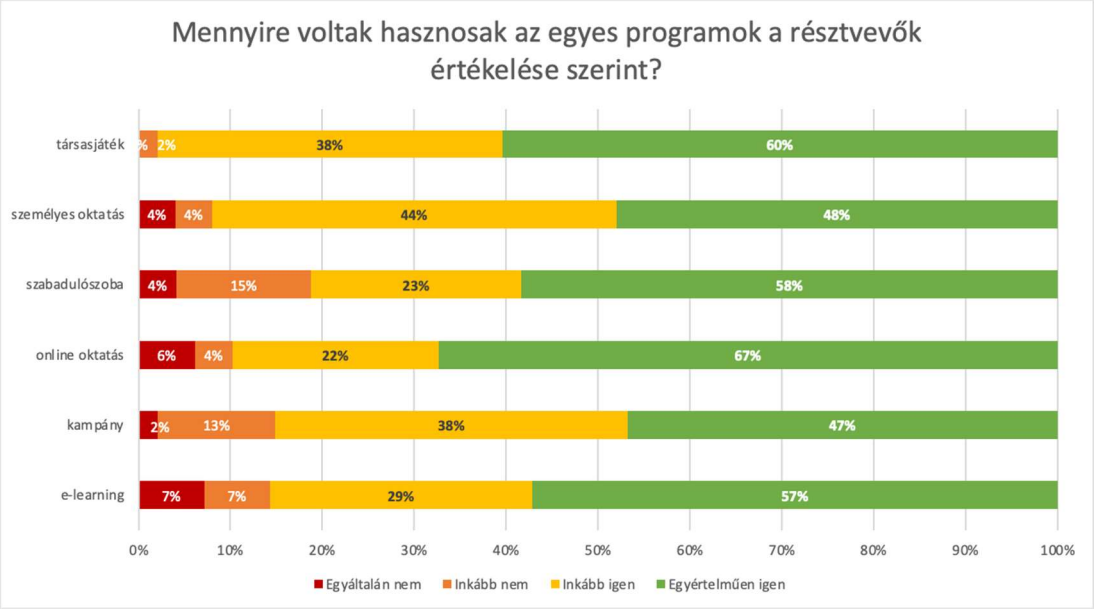
Program típusok és hasznosság-index	***Összességé-ben***	***Állami szférában***	***Privát szférában***
e-Learning	3,36	3,45	3,27
kampányelemek	3,30	3,38	3,22
online oktatás	3,51	3,56	3,46
szabadulószoba	3,35	3,54	3,17
személyes oktatás	3,36	3,12	3,60
társasjáték	3,58	3,54	3,62

15. táblázat: Az egyes programtípusok értékelése hasznosság szempontjából a programot követően (forrás: saját szerkesztés)

Az eredményekből látszódik, hogy összességében legkevésbé hasznosnak a kampányelemeket (3,30) és a szabadulószobát (3,35) vélték a résztvevők, leghasznosabbnak pedig az értékelésük alapján a társasjáték bizonyult (3,58). Nagy különbségek mutatkoznak azonban az állami szféra és a privát szektor értékelése között a többi programelem vonatkozásában. Míg az állami szektorban a személyes oktatás szerepelt a legrosszabbul hasznosság tekintetében (3,12), addig a privát szektorban ez a társasjátékot követő második leghasznosabbnak vélt oktatási forma (3,60). A privát szférában legkevésbé hasznosnak tartott szabadulószoba (3,17) pedig

holtversenyben második helyen szerepel a társasjátékkal (3,54) az állami szervezetek munkavállalóinak értékelése alapján.

A részletes értékeléseket a 16. diagram szemlélteti:

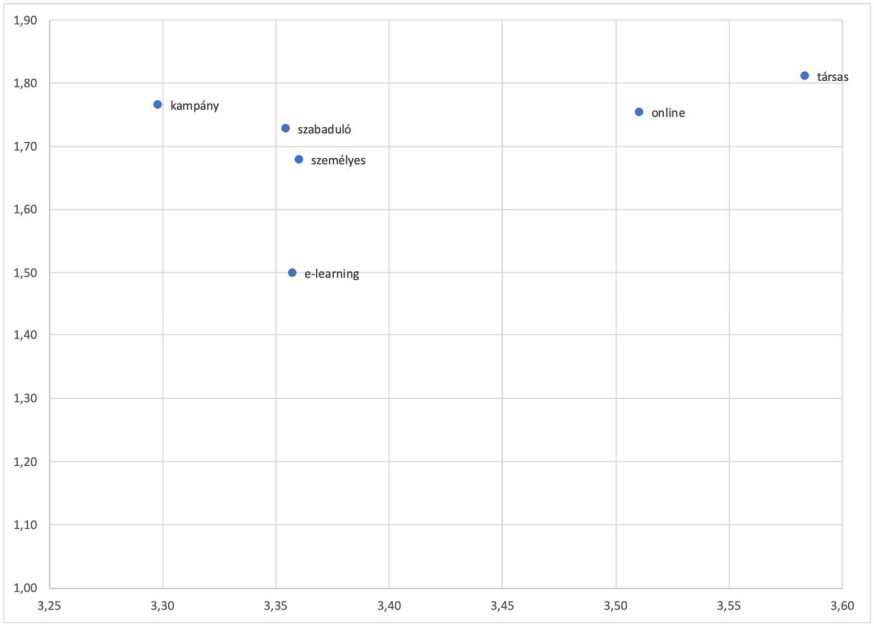


16. diagram: Az egyes programtípusok értékelése hasznosság szempontjából a programot követően (forrás: saját szerkesztés)

A legjobb értékelés szempontjából is az online oktatás bizonyult a leghasznosabbnak ítélt megoldásnak, a válaszadók 67%-a „*Egyértelműen hasznos*” programnak jelölte. „*Egyáltalán nem*” értékelést a társasjáték kivételével minden más programelem kapott, legnagyobb mértékben az e-Learning (7%), illetve maga az online oktatás is (6%).

Hatékonyság értékelésének a szempontjából a korábbi adatokkal dolgoztam, és azt néztem meg, hogy az egyes programok résztvevői hány új biztonságtudatossági ismerettel gazdagodtak a képzést követően.

Az eredményeket itt is egy hasonló pont-diagramon helyeztem el, mely jól szemlélteti, hogy szemmel láthatólag itt sem érdemes lineáris trendet alkalmazni (17. diagram):



17. diagram: Az egyes programtípusok szemléltetése pont-diagramon hasznosság (x) és megszerzett átlag új tudás (y) vonatkozásában (forrás: saját szerkesztés)

A diagram alapján látható, hogy nincsen lineáris kapcsolat az egyes programelemek értékelése, és a szerzett ismeretek számossága között, ezért Spearman-féle rangkorrelációt számoltam az Excelben az alábbi adatokra (16. táblázat):

Program típusok	***Hasznosság-index***	***Új ismeretek átlaga (db)***
e-Learning	3,36	1,50
kampányelemek	3,30	1,77
online oktatás	3,51	1,76
szabadulószoba	3,35	1,73
személyes oktatás	3,36	1,68
társasjáték	3,58	1,81

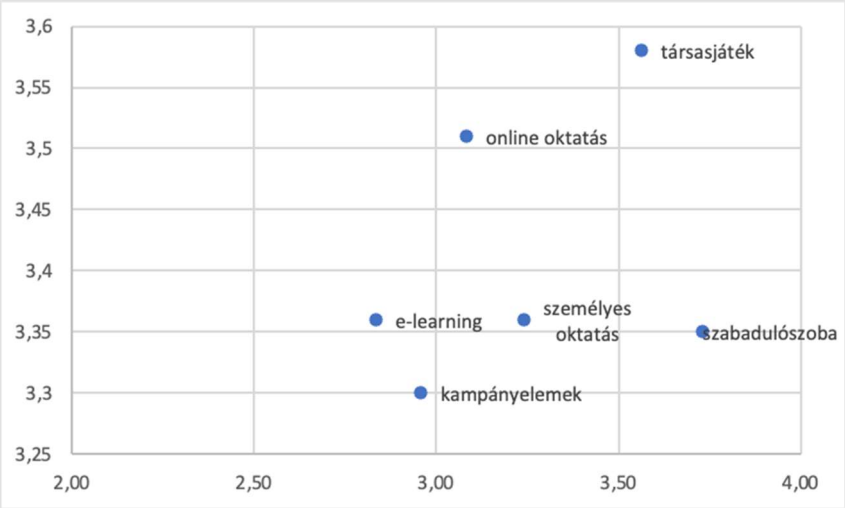
16. táblázat: A hasznosság értékelése és az új ismeretek közötti összefüggés vizsgálata az egyes programok vonatkozásában (forrás: saját szerkesztés)

Az eredmény 0,2571 lett, mely egy gyenge pozitív kapcsolatot mutat a hasznosság felhasználói értékelése és az új ismeretek számának bővülésében.

Megnéztem ezt követően itt is, hogy az egyes módszerek mennyire voltak hatékonyak aszerint, hogy a résztvevő felhasználók hány százaléka gazdagodott legalább egy új biztonságtudatossági ismerettel, tehát a programot követő kérdőívre legalább egy új, értékelhető ismeretet írt.

A Spearman-féle rang-korreláció értéke ott 0,3478 lett, tehát itt is gyenge kapcsolat van a képzés által hasznosságának értékelése és a biztonságtudatossági ismeretekkel gazdagodott résztvevők aránya között.

Végül megvizsgáltam azt is, hogy milyen a kapcsolat a hasznosság és az élvezetesség értékelése között, tehát amit a felhasználók élvezetesnek tartottak, azt hasznosabbnak is vélték-e. Erre is egy pont-diagramot készítettem (18. diagram):



18. diagram: Az egyes programtípusok szemléltetése pont-diagramon hasznosság (x) és fejlesztett felhasználók arányának (y) vonatkozásában (forrás: saját szerkesztés)

Itt sem feltételeztem szoros kapcsolatot, melyet a 17. táblázat adataira készített Spearman-féle rang-korrelációs érték is tükröz: 0,1739, tehát nagyon gyenge a kapcsolat aközött, hogy a felhasználók mennyire élvezik, és mennyire tartják hasznosnak az adott programot.

Program típusok	***Hasznosság-index***	***Élmény-index***
e-Learning	2,83	3,36
kampányelemek	2,96	3,30
online oktatás	3,08	3,51
szabadulószoba	3,73	3,35
személyes oktatás	3,24	3,36
társasjáték	3,56	3,58

17. táblázat: A hasznosság és az élvezetesség értékelésének összefüggés vizsgálata az egyes programok vonatkozásában (forrás: saját szerkesztés)

Mindezek alapján elmondhatjuk, hogy a hasznosság és az élvezetesség értékelése között sincsen szoros összefüggés, az pedig, hogy a felhasználók mennyire ítélnek egy programot hasznosnak, kevésbé van hatással annak tényleges hatékonyságára.

Amennyiben felhasználói értékelés alapján szeretnénk biztonságtudatossági program típus mellett dönteni, a hasznosnak ítélés helyett inkább a felhasználói élményt vegyük figyelembe.

3.8. LEVONT KÖVETKEZTETÉSEK

Ebben a fejezetben elsődlegesen azt vizsgáltam meg, hogy a különböző biztonságtudatossági programok preferenciájának, azok által nyújtott felhasználói élménynek, valamint a hasznosság értékelésének milyen hatása van az adott módszer hatékonyságára.

A vizsgálat során megállapítottam a következőket, és az alábbi következtetéseket vontam le:

- A felhasználói előzetes preferencia nem befolyásolja a képzés hatékonyságát. Ebből kifolyólag azok a munkavállalók, akik előzetesen nem preferált képzésen vesznek részt, nagy valószínűséggel nem fognak kevesebb ismeretet szerezni, illetve a preferált képzésen résztvevők esetében sem számíthatunk kiemelkedő fejlődésre.
- 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. Következésképpen érdemes olyan programelemet is beillesztenünk a biztonságtudatossági fejlesztésekbe, mely magasabb felhasználói élményt nyújt.
- A képzés által nyújtott felhasználói élmény értékelése és a biztonságtudatossági ismeretekkel gazdagodott résztvevők aránya között mind összességében, mind az állami és privát szféra esetében szoros pozitív kapcsolat van, tehát az élvezetesebb programok elsősorban érzékenyítésre, több felhasználó elérésére alkalmasak.
- A képzés által nyújtott felhasználói élmény értékelése és az új ismeretek számának bővülése között gyenge pozitív kapcsolat van, tehát az élvezetesebb programok minimális szinten pozitív irányba befolyásolják a megszerzett ismeretek számának gyarapodását, tehát aki élvezetesebb programon vesz részt, valószínűleg minimális mértékben, de többet tanul.
- Vizsgálatom gyenge pozitív kapcsolatot mutat a hasznosság felhasználó általi értékelése és az új ismeretek számának bővülésében, valamint a biztonságtudatosabb felhasználók számának növelésében is, mely alapján elmondhatom, hogy ezen értékelés, bár hasznos eleme lehet a biztonságtudatossági program elemeinek összeállítása során, kevésbé befolyásolja úgy az eredményességet, mint a felhasználói élmény figyelembe vétele.
- Az eredmények alapján elmondhatjuk, hogy amennyiben az a célunk, hogy minél több felhasználót érjünk el és érzékenyítsünk a biztonságtudatosság iránt, esetleg konkrét, szűkebb témakörben szeretnénk információbiztonsági ismereteket átadni, érdemes megvizsgálnunk, hogy mely biztonságtudatosságot fokozó programok milyen élvezeti

értékkel bírnak a munkavállalóink körében és aszerint kiválasztani az alkalmazott módszereket.

- A fentiek mellett természetesen érdemes több különböző programot is alkalmaznunk, mert ahogyan láttuk, hatékonyság szempontjából nagyon különböző értékekkel bírnak az egyes módszerek akár csak szektor szerinti bontásban is.

Vizsgálatom igazolta a hipotézist, mely szerint elmondható, 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 azok a megoldások, melyeket a felhasználók preferálnak, vagy hasznosnak értékelnek.

4. A GAMIFIKÁCIÓ ALKALMAZHATÓSÁGA A FELHASZNÁLÓK BIZTONSÁGTUDATOSSÁGI ISMERETEINEK BŐVÍTÉSÉRE

A 3. fejezetben bebizonyítottam, hogy a preferencia, élvezetesség és hasznosság értékelése közül a felhasználói élmény befolyásolja legnagyobb mértékben azt, hogy milyen mértékben nő a több biztonságtudatossági ismerettel rendelkező felhasználók száma, és kis mértékben, de van arra hatása, hogy az egyes felhasználók mennyit tanulnak a képzésekből (átlagosan hány új ismeretre tesznek szert), tehát összességében elmondható, hogy az élvezetesebb programok hatékonyabbnak bizonyulnak azoknál, melyeket a felhasználók preferálnak, vagy hasznosnak tartanak.

Ebben a fejezetben azt vizsgálom, hogy a magasabb felhasználói élményt nyújtó gamifikációs programok alkalmazhatóak-e és milyen hatékonysággal a biztonságtudatossági képzések során.

4.1. KAPCSOLÓDÓ 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 igazolására vagy cáfolására az előző pontban alkalmazott kutatás eredményeit használatam fel, melynek során hat különböző, köztük két gamifikációs módszer élvezetességét és hatékonyságát vizsgáltam abból a szempontból, hogy melyiknek milyen hatása van a biztonságtudatossági ismeretek bővülésére (*átlagos új ismeretszám*), vagy a biztonságtudatos felhasználók számának növelésére (*legalább egy új ismeretet szerző résztvevő felhasználók aránya*). Az eredményeket a disszertáció 4. fejezete mutatja be.

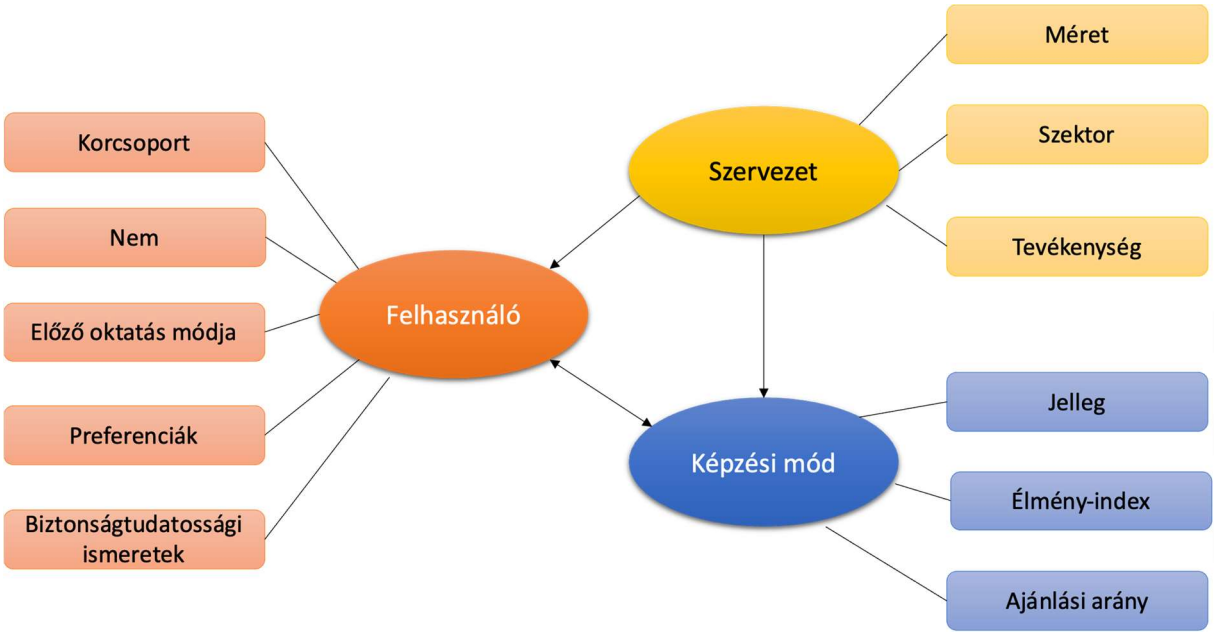
A hipotézis igazoláshoz kifejlesztettem egy gyakorlati felmérési módszertant a biztonságtudatosságot fejlesztő módszerek hatékonyságának összehasonlítására, melyet a 3. fejezetben mutattam be.

A vizsgálattal célom annak bizonyítása, hogy a gamifikációs módszerek képesek a biztonságtudatossági szint fejlesztésére mind az ismeretek bővítése, mind a biztonságtudatosabb felhasználók számának növelése szempontjából.

4.2. A VIZSGÁLATHOZ FELHASZNÁLT ADATOK

A gamifikációs módszerek alkalmazhatóságának vizsgálata során a 3. fejezetben bemutatott kutatás eredményei támaszkodtam.

A jelen hipotézist érintő vizsgálat során az 5. ábrán szemléltetett adatokkal dolgoztam:



5. ábra: A kutatásban használt adatok a hipotézis vizsgálata során (forrás: saját szerkesztés)

Az adatok gyűjtése és a kérdőívek kitöltési aránya felhasználói, illetve szervezeti ismérvek vonatkozásában megegyezik a 3. fejezetben bemutatottakkal.

Az egyes képzési módokra vonatkozó kitöltési statisztikákat a 18. táblázat szemlélteti:

Program-típus	K1 kérdőív (db)	K2 kérdőív (db)	K3 kérdőív (db)
E-Learning	42	42	26
Kampány	47	47	31
Online oktatás	49	49	30
Szabadulószoba	48	48	37
Személyes oktatás	50	50	36
Társasjáték	48	48	34
Összesen:	**284**	**284**	**194**

18. táblázat: Kitöltési statisztikák (forrás: saját szerkesztés)

Ezen fejezetben a vizsgálat során hagyományos, illetve gamifikációs jelleg szerint csoportosítva vizsgálatam az egyes program-típusokat, oktatási módszereket. Hagyományos módszernek tekintettem a személyes oktatást, online oktatást, e-Learning-et, valamint a kampányelemeket, gamifikációs megoldásnak pedig a szabadulószobát és a társasjátékot.

4.3. GAMIFIKÁCIÓS MÓDSZEREK JELENLEGI ALKALMAZÁSA A SZERVEZETEKNÉL

A szakirodalom kutatás során feltártam, hogy a gamifikációs módszerek nemzetközi szinten töretlen népszerűségnek örvendenek, hazánkban pedig egyre elterjedtebbé kezdenek válni. Tanulmányok szintén igazolták már azt, hogy az információbiztonsági oktatásokban is megjelennek játékosított megoldások, sőt ezek hatékonyságát is vizsgálták már (Abawajy, 2014; Khan és szerzőtársai, 2011; Tschakert és Ngamsuriyaroj, 2019).

A hazai szervezetek vonatkozásában több szervezetnél volt már lehetőségem gamifikációs biztonságtudatossági képzést tartani a kutatás keretein kívül is, viszont emellett sok szervezetnél tapasztalatom azt, hogy az előnyök azonosítása mellett negatív előfeltételezések is megjelennek a játékosított képzésekkel kapcsolatban. Ezek általában a következők:

- A résztvevők nem veszik komolyan játékos megoldásokat, ezáltal nem fejlődik kellő mértékben a biztonságtudatosságuk, cserébe a képzésre fordított idő a munka rovására megy.
- A munkavállalókat nem érdekli majd egy „gyerekesnek” tűnő képzési módszer, ezért nem vesznek részt a programban.
- A résztvevők nem veszik majd komolyan a játékos formában átadott információbiztonsági szabályokat, illetve az információbiztonsági területet sem.

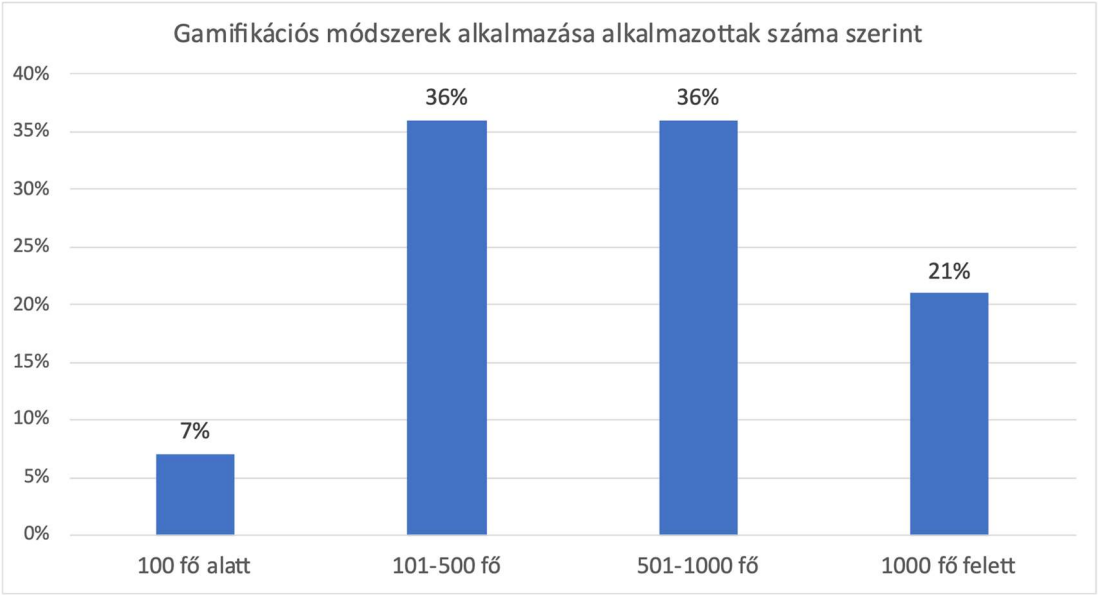
Az eddigi tapasztalataim – ahogyan azt a szabadulószoba és a társasjáték esetében külön be is mutatom – megcáfolják ezeket, és a félelmek ellenére nagyon sikeres, és a felhasználók által nagyon pozitívan értékelt programokat sikerült megvalósítani.

A gamifikációs módszerek munkahelyi környezetben való alkalmazhatóságát és hatékonyságát azonban a disszertációmban kívántam igazolni.

A kutatásom készítése során nem találtam arra vonatkozó statisztikát, hogy Magyarországon a biztonságtudatossági képzésekben milyen arányban jelennek meg játékosított megoldások, ezért a kutatáshoz készített kérdőívemben (K1) azt is megkérdeztem, hogy a felhasználók mikor, illetve milyen oktatási módszerben vettek részt korábbi képzésük során.

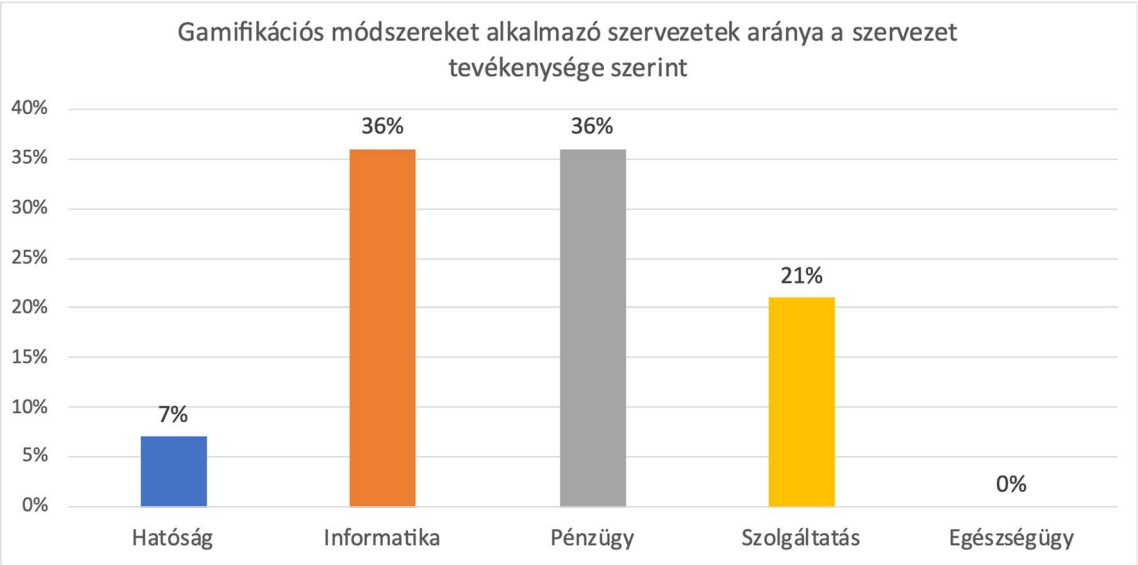
Az eredmények alapján elmondható, hogy a vizsgálatba bevont, oktatásban már részesült felhasználóknak (a válaszadók 64,08%-a) csupán 7,69%-a vett részt gamifikációs módszerű oktatásban. A játékosított programban résztvevő felhasználók 42,86%-a az állami szférában elhelyezkedő munkavállaló, 57,14%-uk a privát szektor vállalatainak dolgozója, ami az előfeltételezésemhez képest eltérés, mert úgy gondoltam, hogy a gamifikációs módszereket elsősorban a piaci szektorban elhelyezkedő vállalatok alkalmazzák.

A gamifikációt alkalmazó szervezetek méretével kapcsolatban is volt előfeltételezésem, méghozzá az, hogy a több munkavállalót foglalkoztató szervezetek alkalmazzák inkább ezen új megoldásokat. Az alábbi diagramon szemléltetett eredmények szerint valóban a nagyobb méretű szervezetek alkalmazottai nyilatkoztak úgy, hogy vettek már részt játékosított, biztonságtudatosságot fejlesztő programban, és a kisebb szervezetek elhanyagolható mértékben alkalmazták ezt a megoldást (19. diagram).



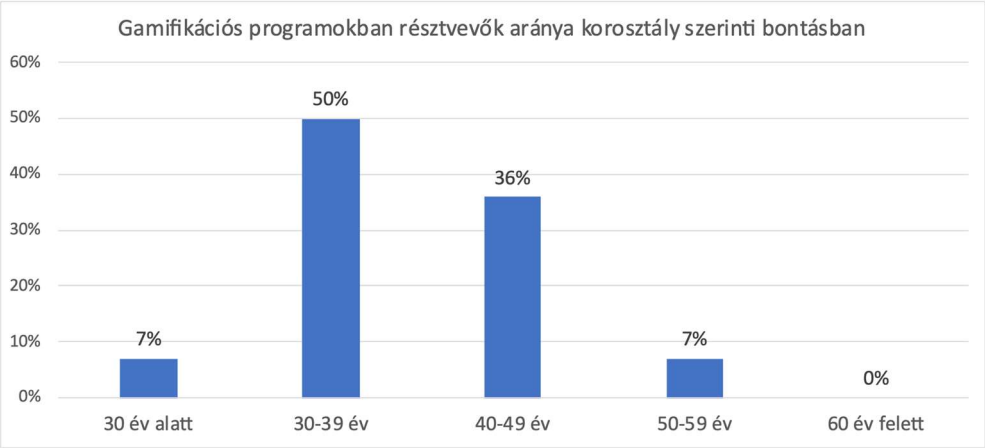
19. diagram: Gamifikációs módszerek alkalmazása az információbiztonsági képzésekben szervezeti méret szerint (forrás: saját szerkesztés)

Ha a gamifikációs módszereket alkalmazó szervezetek tevékenységi profilját nézzük, az alkalmazók legnagyobb része az IT, illetve szolgáltatási szektorba tartozik (20. diagram).



20. diagram: Gamifikációs módszerek alkalmazása az információbiztonsági képzésekben a szervezet tevékenységének jellege szerint (forrás: saját szerkesztés)

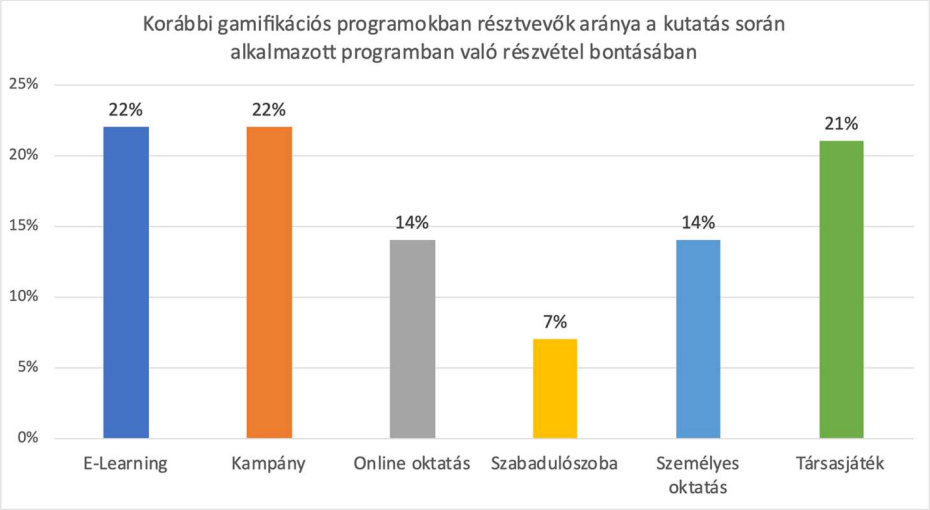
Korosztály szerinti bontásban a gamifikációs programban résztvevő válaszadók legnagyobb része a 30-39 éves korosztályt képviselte (50%), 36%-uk pedig a 40-49 éves csoportot (21. diagram).



21. diagram: A gamifikációs programban résztvevők aránya korosztály szerint (forrás: saját szerkesztés)

A játékosított módszerek alkalmazásának újszerűségét az is bizonyítja, hogy a gamifikációs módszert jelölő válaszadók 92,85%-a az elmúlt egy évben vett részt utoljára biztonságtudatossági oktatáson, és csak egy válaszadó volt, aki azt jelölte, hogy az elmúlt 3-5 évben volt játékosított programban része.

A kutatásban szereplő programok között elmondható, hogy a gamifikációs ismeretekkel már rendelkező felhasználók mind a 6 programban az alábbi arányokkal képviseltették magukat, kiugróan alacsony értékkel csak a szabadulószoba (7%) rendelkezik. Ezek alapján elmondható, hogy minden vizsgált programelemben volt olyan résztvevő, aki már találkozott valamilyen játékosított megoldással, és volt összehasonlítási alapja is (22. diagram).



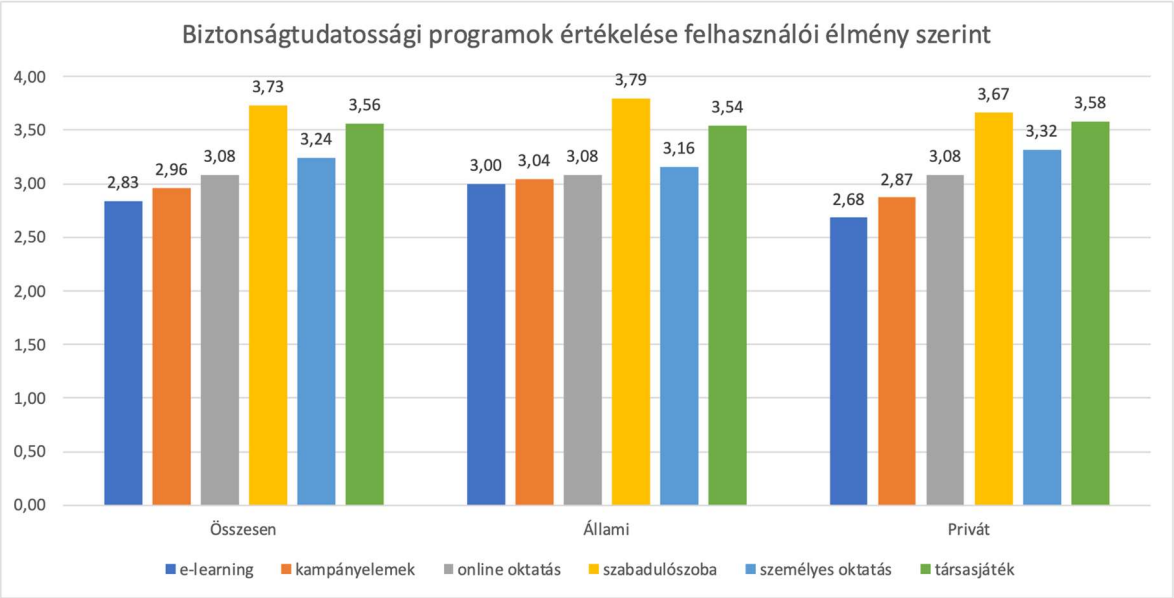
22. diagram: Azon felhasználók aránya, akik már vettek részt gamifikációs programban, a kutatásban alkalmazott programon való részvétel bontásában (forrás: saját szerkesztés)

A fentiek alapján elmondható, hogy a vizsgált szervezetek munkavállalói által adott válaszok alapján a gamifikációs módszerek hazánkban még nem terjedtek el a biztonságtudatosságot fejlesztő módszerek között.

4.4. A KUTATÁSBA BEVONT GAMIFIKÁCIÓS PROGRAMOK ÉRTÉKELÉSE

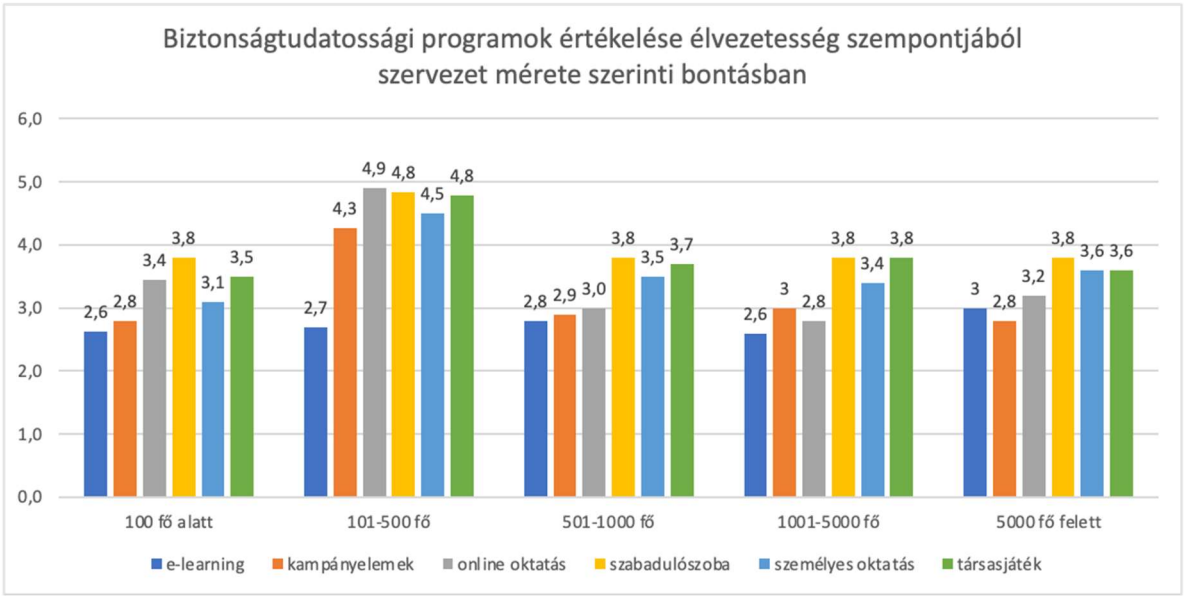
A kutatás során két gamifikációs módszert alkalmaztam, a szabadulószobát és a társasjátékot. Azt már az előző fejezetben is bemutattam, hogy minél élvezetesebb egy biztonságtudatosságot fejlesztő program, annál nagyobb mértékben fejleszti a biztonságtudatosságot közvetlenül a program után, elsősorban a legalább egy új ismerettel rendelkező felhasználók arányának növekedésében, és másodsorban az új ismeretek számának bővítésében.

Felhasználói élmény szerint, ahogyan a 23. diagram is mutatja, a kutatásba bevont gamifikációs programok a két legjobb helyen végeztek a felhasználók értékelése alapján (elsődlegesen a szabadulószoba, majd ezt követően a társasjáték) mind összességében, mind szektoronkénti bontásban, így további vizsgálatuknak létjogosultsága van.



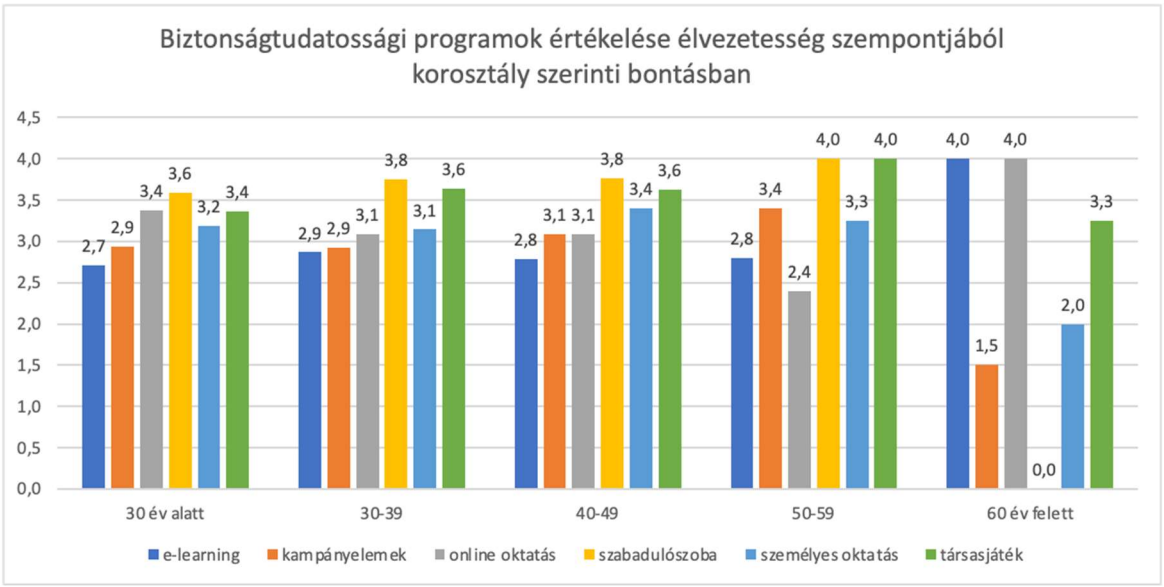
23. diagram: A kutatásba bevont különböző programok értékelése felhasználói élmény szempontjából, összességében és szektoronkénti bontásban (élmény-index) (forrás: saját szerkesztés)

A szervezet méretét tekintve a szabadulószoba a 101-500 fős szervezetek kivételével mindenhol a legjobb értékelést kapta felhasználói élmény szempontjából, a társasjáték pedig ugyanezen kategóriában mindenhol a második helyen végzett (előző típusnál holtversenyben a szabadulószobával) (24. diagram).



24. diagram: A kutatásba bevont különböző programok értékelése felhasználói élmény szempontjából a szervezetek mérete szerinti bontásban (élmény-index) (forrás: saját szerkesztés)

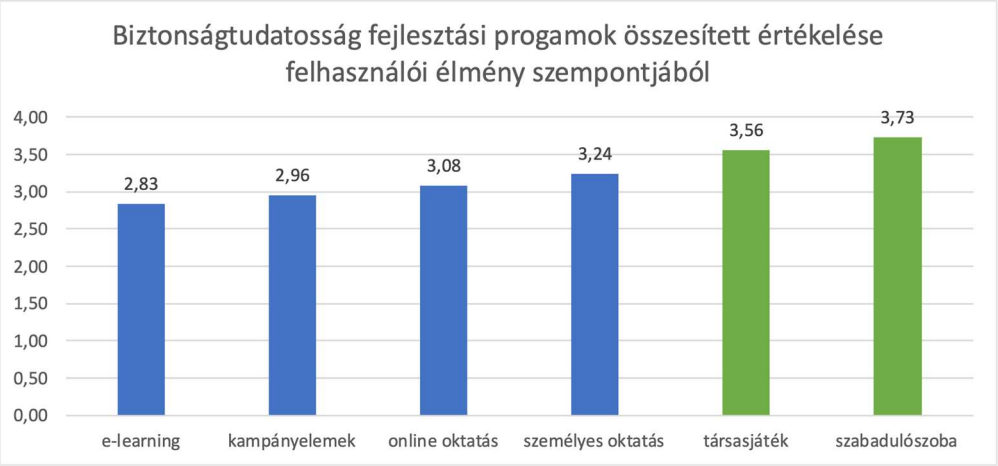
A 25. diagramon azt is láthatjuk, hogy a két gamifikációs módszer, a szabadulószoba és a társasjáték minden, 60 év alatti korosztályba tartozó felhasználó esetében a legmagasabb értékelést kapta (a szabadulószoba programnak nem volt 60 év feletti képviselője, az érték ott azért 0).



25. diagram: A kutatásba bevont különböző programok értékelése felhasználói élmény szempontjából, korosztály szerinti bontásban (élmény-index) (forrás: saját szerkesztés)

Értékelés szempontjából, ha a végleges, összesített rangsort szeretnénk látni, akkor a 26. diagram tökéletesen mutatja, hogy a szabadulószoba és a társasjáték érték el a legjobb

eredményeket felhasználói élmény szempontjából, ezek rendelkeznek a legmagasabb élmény-index-szel.



26. diagram: A kutatásba bevont különböző programok összesített eredmények alapján meghatározott rangsora a felhasználói élmény szempontjából (élmény-index) (forrás: saját szerkesztés)

A 19. táblázat bemutatja, hogy nemek szerinti bontásban a gamifikációs elemeket inkább a férfiak értékelték jobban, esetükben a társasjáték és a szabadulószoba közel azonos pozitív értékelést kapott. Nők esetében azonban egy jól látható különbség (0,28 pontérték) volt a szabadulószoba javára, tehát esetükben nagyobb érdeklődésre számíthatunk, ha ezt a programelemet szervezzük.

Résztvevő neme / élmény-index	***Szabadulószoba***	***Társasjáték***	***Összesen***
férfi	3,73	3,74	3,73
nő	3,73	3,45	3,57

19. táblázat: A kutatásba bevont gamifikációs programok értékelése felhasználói élmény szempontjából, nemek szerinti bontásban (élmény-index) (forrás: saját szerkesztés)

A fentiek alapján elmondható, 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.

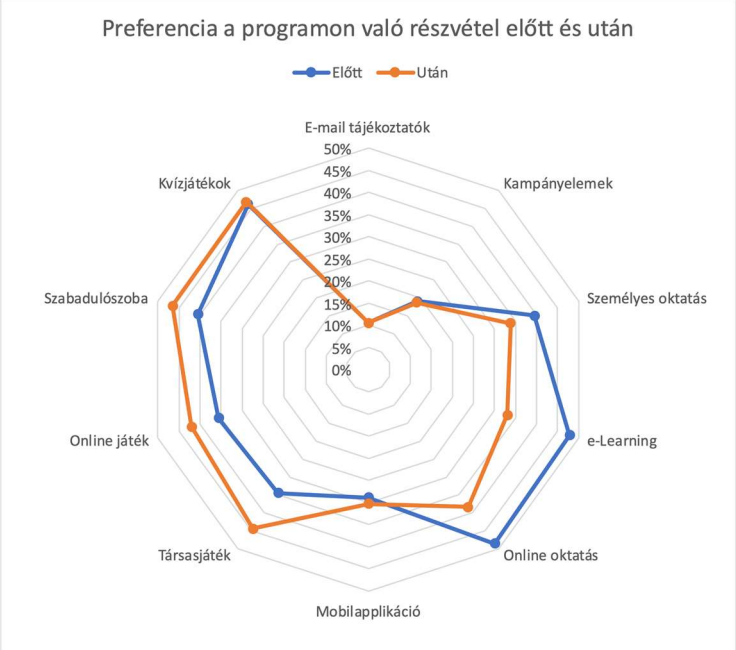
4.5. FELHASZNÁLÓI PREFERENCIA VÁLTOZÁSA A KUTATÁS SORÁN

Annak igazolását követően, hogy a gamifikációs módszerek minden vizsgált szervezet esetében a leginkább élvezetesebb biztonságtudatosságot fejlesztő programnak bizonyultak, következő lépésként ebben az esetben is a preferenciát vizsgáltam, ezen belül is, hogy a programon való részvételt követően változott-e, és ha igen, hogyan az egyes képzési módok felhasználói

preferenciája, elsősorban a gamifikációs módszerek javára (tehát a részvételt követően nőtt-e azon válaszadók számra, akik preferenciaként jelölték valamely felsorolt játékosított módszert). Ugyan a preferencia és a hatékonyság között szoros kapcsolatot nem tudtam kimutatni a 3. fejezetben végzett vizsgálat alapján, azonban az alkalmazhatóság érdekében fontosnak tartottam megvizsgálni, hogy hogyan viszonyulnak a felhasználók a programot követően a gamifikációs módszerekhez.

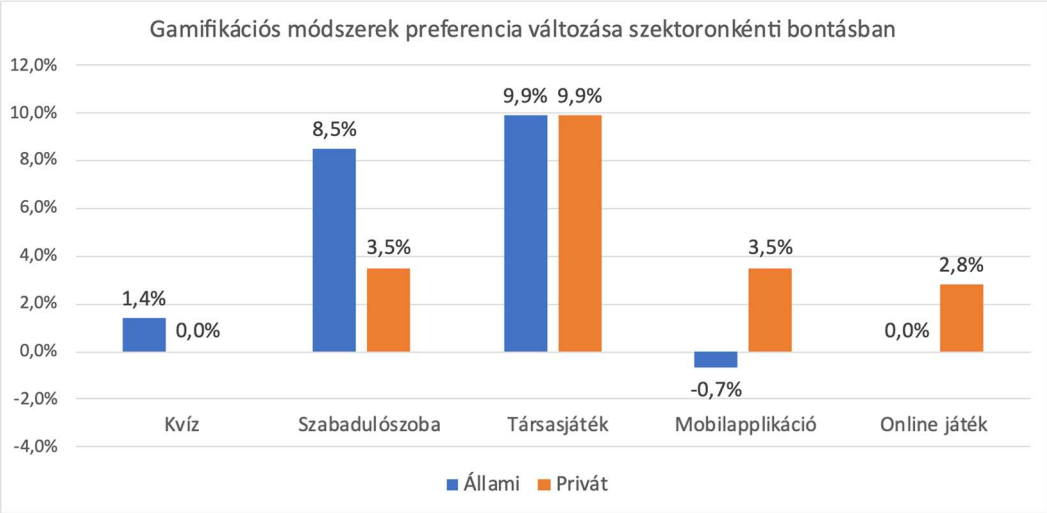
Az előző pontban tett megállapítások miatt feltételeztem, hogy ez az értékelés a gamifikációs módszerek irányába mutat majd elmozdulást.

A változást az alábbi pókháló diagramon szemléltetem, melyen jól látszódik, hogy a feltételezésem beigazolódott, a programon való részvételt követően látványos elmozdulás van a gamifikációs megoldások irányába. Ez leginkább az online oktatás és e-Learning rovására történik, és legszembetűnőbben a társasjáték felé mozdul (27. diagram).



27. diagram: A kutatásban vizsgált programelemek iránti preferencia változása (forrás: saját szerkesztés)

Csak a gamifikációs módszerek vonatkozásában megnéztem, hogy az egyes megoldások iránti érdeklődés milyen mértékben nőtt. Ahogyan a 28. diagramon is látszódik, leginkább a társasjáték, és az állami szférában az online játék keltette fel az érdeklődést (utóbbiról nem kaptak részletes tájékoztatást a résztvevők, így feltételezhető, hogy a társasjátékból indultak ki az értékelés során). Szintén általánosságban elmondható, hogy az állami szektor válaszadói nagyobb mértékben részesítették előnyben a gamifikációs lehetőségeket az egyes programokat követően.



28. diagram: A kutatásban vizsgált gamifikációs módszerek preferencia változása szektoronkénti bontásban (forrás: saját szerkesztés)

A szektor szerinti bontás mellett érdekes lehet a szervezeti méret szerinti preferencia vizsgálata is. Megnéztem ezért, hogy ahogyan nő a szervezet mérete, hogyan változik az egyes módszerek iránti preferencia, mind a kutatási program előtt, mind a programon való részvételt követően. Az eredményeket a 6. számú mellékletben feltüntetett kiegészítő diagramok szemléltetik.

Az adatok alapján elmondhatjuk, hogy a bemutatott gamifikációs módok preferencia növekedése az 5000 fő alatti szervezetek esetében közel azonos módon nőtt, tehát a szervezet mérete alapján is bárhol gondolkodhatunk a játékosított módszerek bevezetésében – az 5000 főt meghaladó szervezetek vonatkozásában pedig érdemes lehet valamilyen online gamifikációs megoldás megfontolása, mert ezek esetében továbbra is ezen módszerek dominálnak.

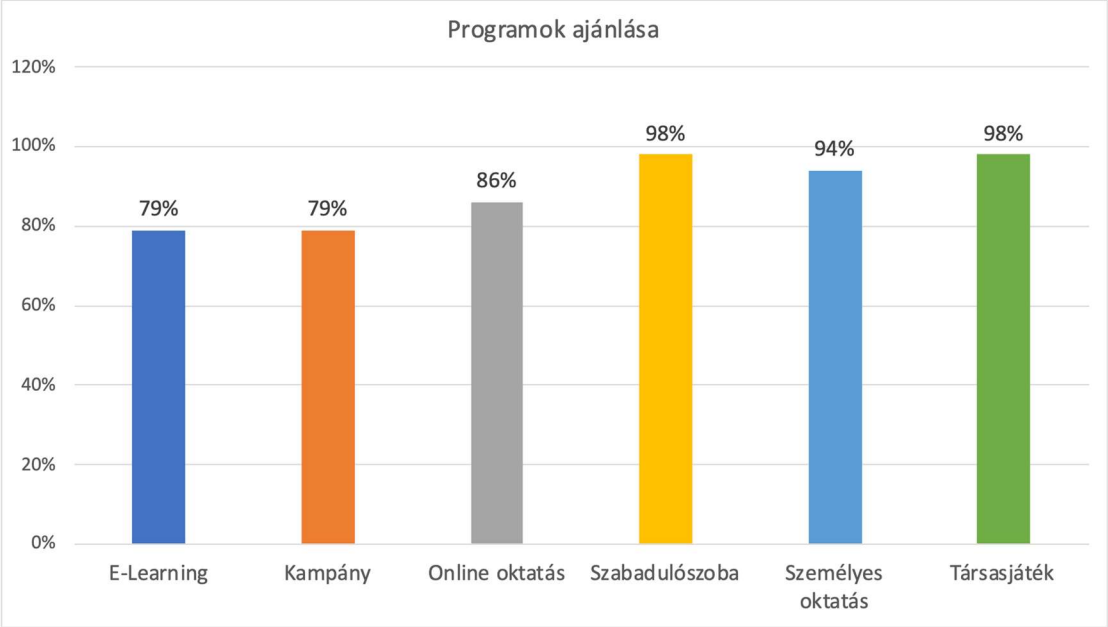
A gamifikációs lehetőségek alkalmazása előtt gyakran találkozok azzal a kérdéssel is, hogy milyen korosztály számára lehet vonzó megoldás, sokak tévhite szerint ugyanis csak a fiatalabb korosztály érdeklődhet leginkább. Az eredmények azt mutatják, hogy a kor előrehaladtával egyre kevésbé népszerű gamifikációs módszerek a programot követően minden korosztály esetében növekedtek, és a kor előrehaladtával a program során bemutatott módszerek esetében inkább stagnáló, vagy enyhében lefelé ívelő trendet mutatnak, a társasjáték pedig kiemelkedően előkelő helyre került az 50 év feletti munkavállalók preferencia listáján is. Ezen eredmények szintén a 6. számú melléklet kiegészítő diagramjai között tekinthetőek meg.

Nemek szerinti bontás tekintetében azt állapítottam meg, hogy mind a férfiak, mind a nők 13-13%-kal preferálták többen a gamifikációs megoldásokat a programot követően. Kizárólag az általam bemutatott két módszer vonatkozásában a pozitív irányba történő elmozdulás férfiak esetében 16%, nők esetében pedig 24% volt.

Fentiek alapján elmondható, hogy a felhasználók a programon való részvételt követően valóban inkább a gamifikációs lehetőségeket részesítenék előnyben, tehát a felhasználók értékelése alapján a játékosított módszerek alkalmazásának van igénye és létjogosultsága munkahelyi környezetben a biztonságtudatosság fejlesztése céljából.

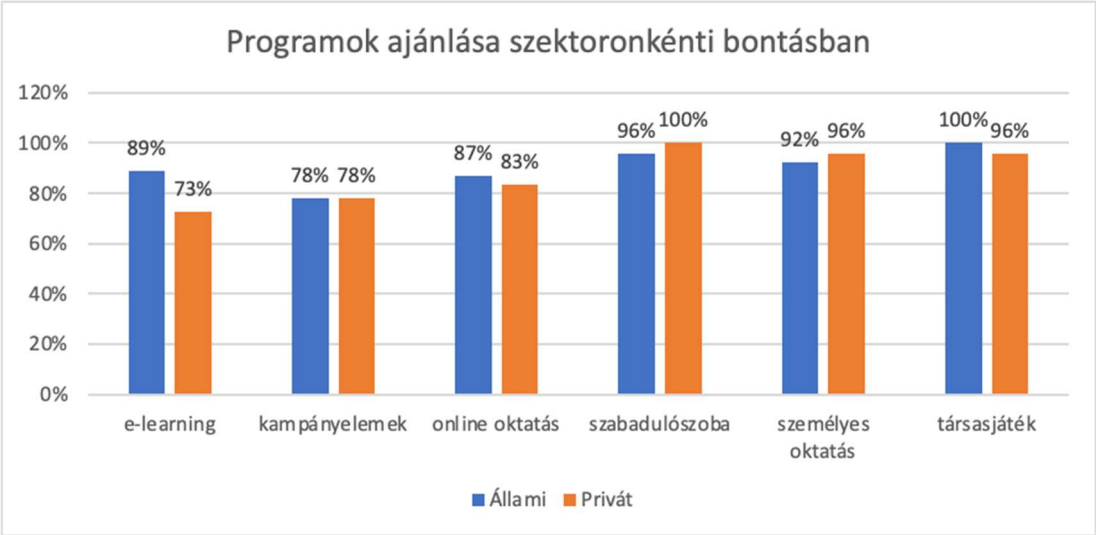
4.6. FELHASZNÁLÓI AJÁNLÁS ÉRTÉKELÉSE

Az előző fejezetben szintén hasznosnak véltem megnézni, hogy a felhasználók a programot, melyen részt vettek, ajánlanák-e más felhasználóknak, és ebben a gamifikációs módszerek milyen értéket érnek el. Az előző alpont értékelése szerint feltételeztem, hogy az élmény alapján ezek magas értéket érnek el. (Megjegyzés: az, hogy egy programot a résztvevő nem élvezett, nem jelenti azt, hogy nem is ajánlja másoknak. Azon felhasználók, akik a programot, melyen részt vettek, nem élvezték, 53,3%-uk mégis ajánlotta. Olyan felhasználó, aki pedig élvezetesnek jelölte, egyetlen sem volt, aki egyértelműen nem ajánlotta volna a módszert, melyen részt vett.) A 29. diagram egyértelműen mutatja, hogy leginkább a gamifikációs módszerek kapták a legmagasabb számú ajánlást, ezeket a résztvevők 98-98%-a ajánlaná.



29. diagram: A kutatásban vizsgált képzési módszerek ajánlása (forrás: saját szerkesztés)

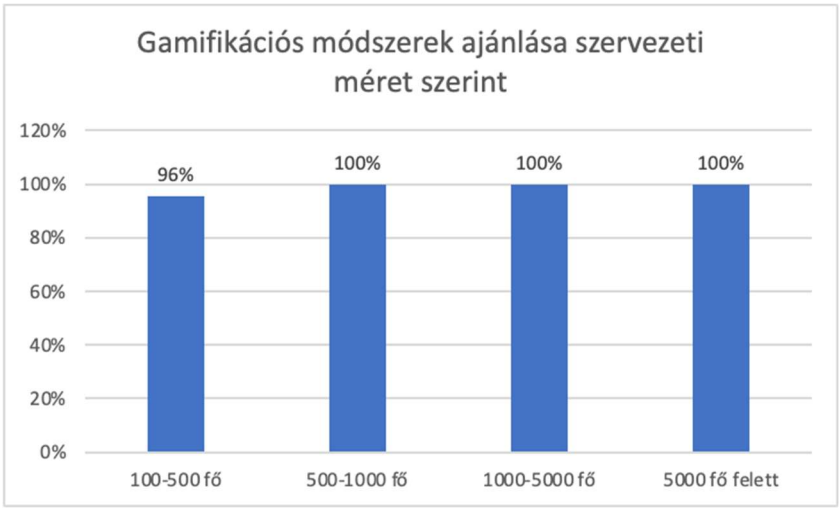
Szektoronkénti bontást is végeztem, melynek a következő eredménye született, ebből szintén látszódik, hogy mindkét vizsgált szektor alkalmazottai ugyanúgy a legmagasabb arányban ajánlják a gamifikációs módszereket. A szabadulószoba a privát szektorban, míg a társasjáték az állami szférában ért el 100%-os ajánlást, vagyis minden résztvevő ajánlotta (30. diagram).



30. diagram: A kutatásban vizsgált képzési módszerek ajánlása szektoronkénti bontásban (forrás: saját szerkesztés)

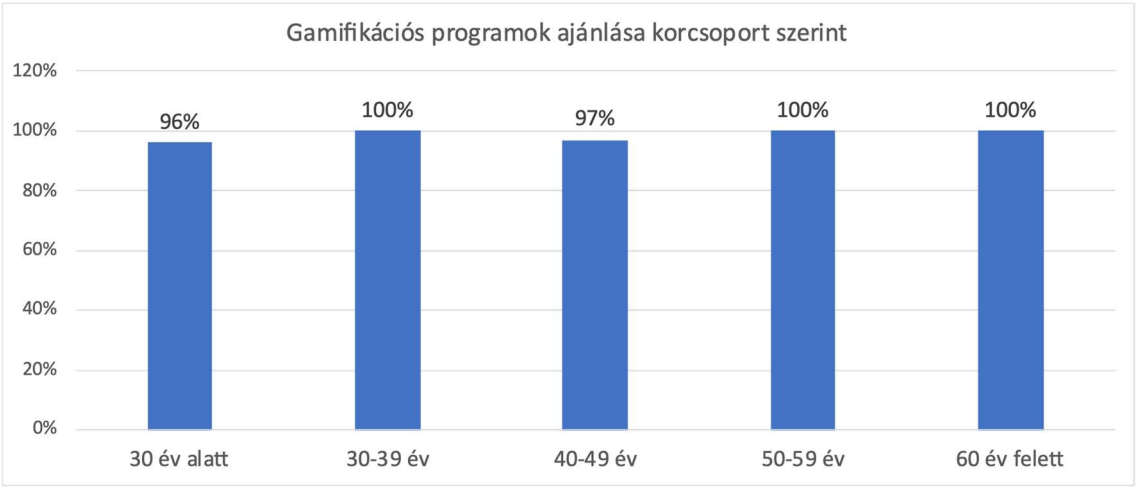
Ezt követően csak a gamifikációs és hagyományos oktatási módszerek vonatkozásában megvizsgáltam a szervezet méret szerinti, valamint a korosztály és nemek szerinti értékeléseket is.

Szervezeti méret alapján egyedül az 500 főt meg nem haladó szervezetek esetében volt néhány olyan résztvevő, aki nem ajánlotta az adott gamifikációs programot, melyen részt vett, a többi szervezet vonatkozásában azonban minden válaszadó pozitívan értékelte és ajánlotta azt (31. diagram).



31. diagram: A kutatásban vizsgált képzési módszerek ajánlása szervezeti méret szerinti bontásban (forrás: saját szerkesztés)

Korcsoportok tekintetében csak a 30 év alatti, illetve 40-49 éves korosztályban volt minimális számú résztvevő, akik nem ajánlanák a játékosított módszereket, vagy nem tudták eldönteni, hogy ajánlanák-e a módszert más felhasználóknak (32. diagram).



32. diagram: A kutatásban vizsgált képzési módszerek ajánlása korosztály szerinti bontásban (forrás: saját szerkesztés)

Végül nemek szerinti bontást is megnézve mind a férfiak, mind a nő 98-98%-os arányban ajánlanák más felhasználóknak a gamifikációs programban való részvételt.

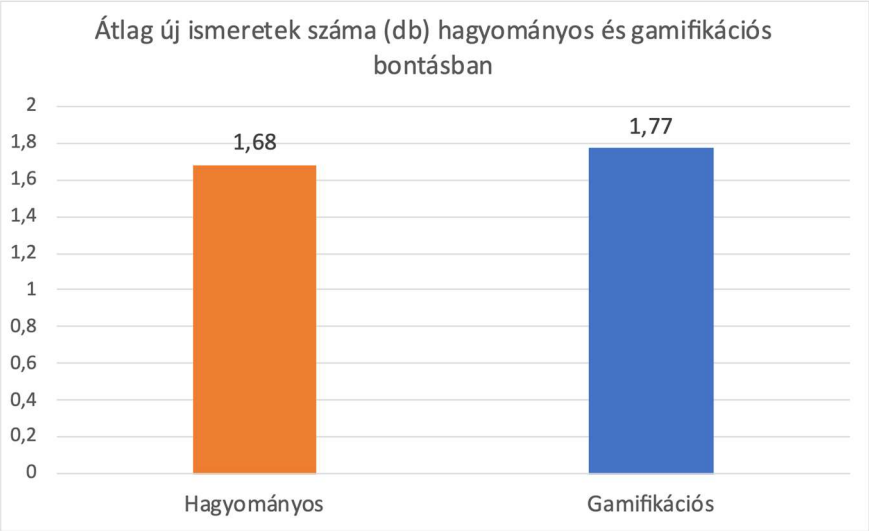
Fentiek alapján szintén elmondható, hogy a felhasználók szektortól, szervezeti mérettől, korosztálytól és nemtől függetlenül ajánlják a gamifikációs módszerek alkalmazását, így a játékosított programok bármely szervezet számára alkalmazható megoldást jelentenek.

4.7. A GAMIFIKÁCIÓS MÓDSZEREK ALKALMAZHATÓSÁGA A BIZTONSÁGTUDATOSSÁGI ISMERETEK SZÁMOSSÁGÁNAK NÖVELÉSÉBEN

Az előzőekben folytatott vizsgálatok során azt állapítottam meg, hogy a gamifikációs módszerek elnyerik a munkavállalók tetszését, a legmagasabb élmény-index-szel rendelkeznek, és kortól, nemtől, szervezeti mérettől és szektortól függetlenül alkalmazhatóak a felhasználók értékelése alapján. Ezek, valamint a 3. fejezetben tett megállapítások alapján alkalmazásuk javasolt a biztonságtudatossági képzések során.

Ebben az alfejezetben azt vizsgálom és igazolom, hogy az élvezetességhez hasonlóan ezen módszerek szintén hatékonyabbak, mint a hagyományos oktatási módszerek, azaz több, és ha igen, mennyivel több biztonságtudatossági ismeretet szereznek a gamifikációs módszerek résztvevői, mint a tradicionális programok válaszadói.

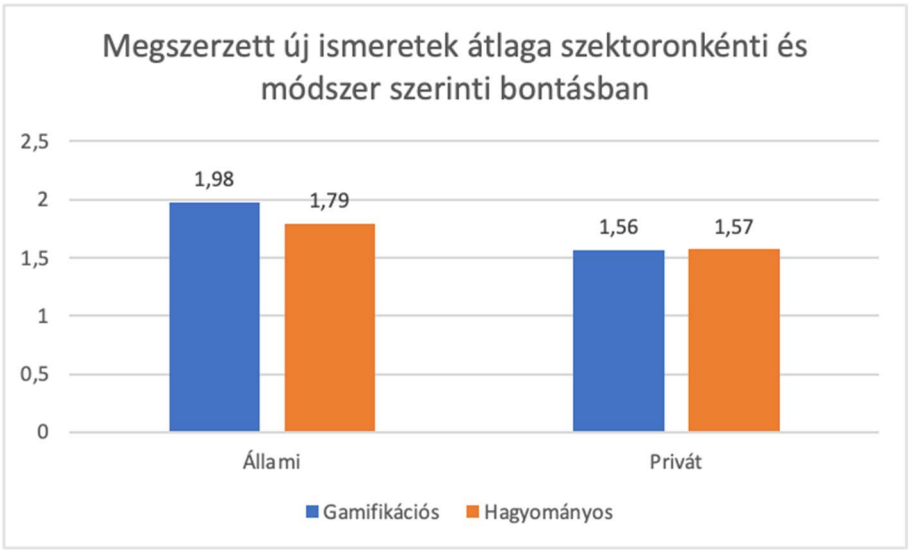
Az alábbi diagramokon szemléltetem, hogy összességében, illetve az állami, valamint a privát szférában átlagosan mennyi új ismeretre tettek szert a résztvevők közvetlenül az egyes programok során.



33. diagram: A kutatásban vizsgált képzési módszerek során szerzett új ismeretek átlagos száma (db) hagyományos és gamifikációs bontásban (forrás: saját szerkesztés)

Összességében a gamifikációs módszerek minimálisan, de több új ismerettel gazdagították a résztvevőket, mint a hagyományos tudatosító lehetőségek (33. diagram), azonban a privát szektorban 0,01 értékkel jobban teljesítettek a hagyományos módszerek.

Szintén említésre méltó, hogy a vizsgálat alapján az állami szektor munkavállalói szemmel láthatóan magasabb tudás-átlagot érnek el a játékosított módszerek alkalmazásával, mint a privát szektor résztvevői (34. diagram)

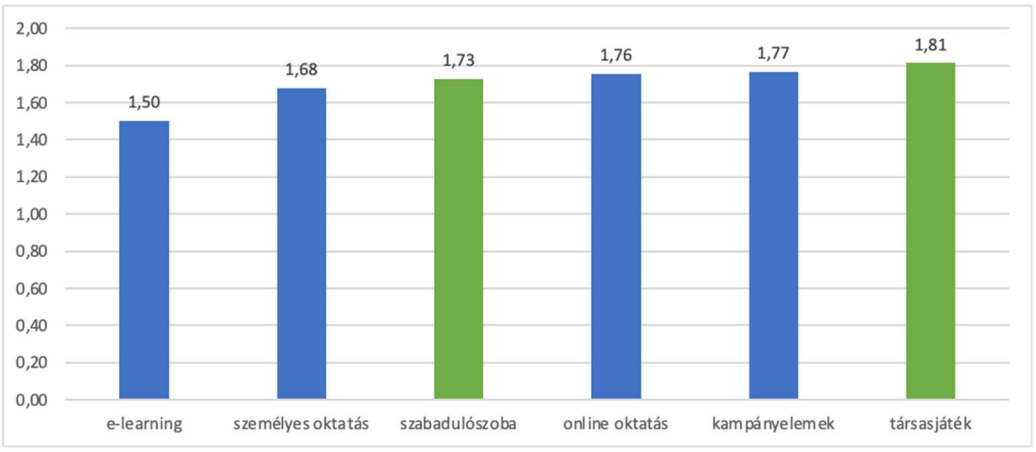


34. diagram: A kutatásban vizsgált hagyományos és gamifikációs módszerek során szerzett új ismeretek átlagos száma (db) szektor szerinti (forrás: saját szerkesztés)

(Ha az új ismeretek számát csak azon felhasználók körében átlagolom, akik ténylegesen tanultak is a programból, akkor elmondható, hogy közel azonos mértékű tudást szereztek a kétféle megközelítés résztvevői: hagyományos programok esetében azon felhasználók átlagos új ismerete, akik legalább 1 új ismeretet írni tudtak, 2,16 db, míg gamifikációs esetben ez 2,15

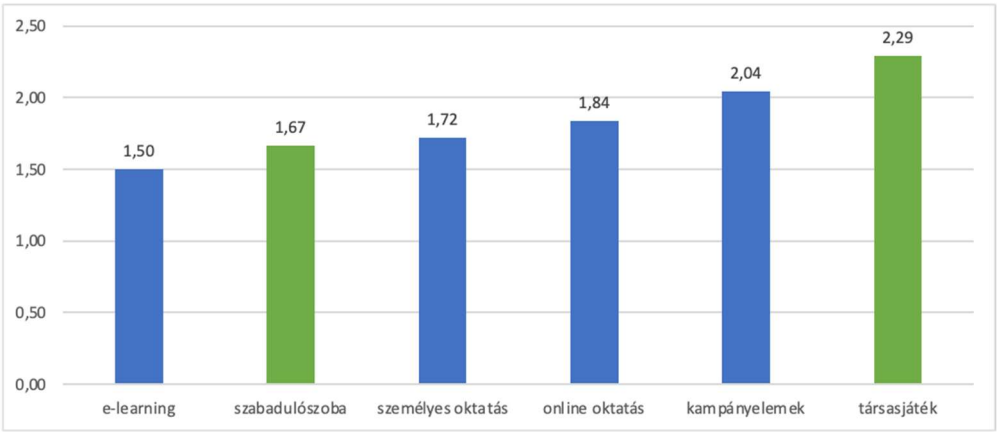
db átlag új ismeretet jelent. Tételesen leszűrve pedig az egyes programokat, egyik sem tudta elérni a 3 db új ismeretet.)

Ebben az esetben is kíváncsi voltam a rangsorra, hogy ebben a gamifikációs megoldásokon belül az általam vizsgált két módszer hogyan szerepelt, ezért a 35. diagramot készítettem el. Ezen jól látszódik, hogy összességében a társasjáték adta a legtöbb új ismeretet (1,81 db), míg a szabadulószoba a középmezőnyben végzett (1,73 db).



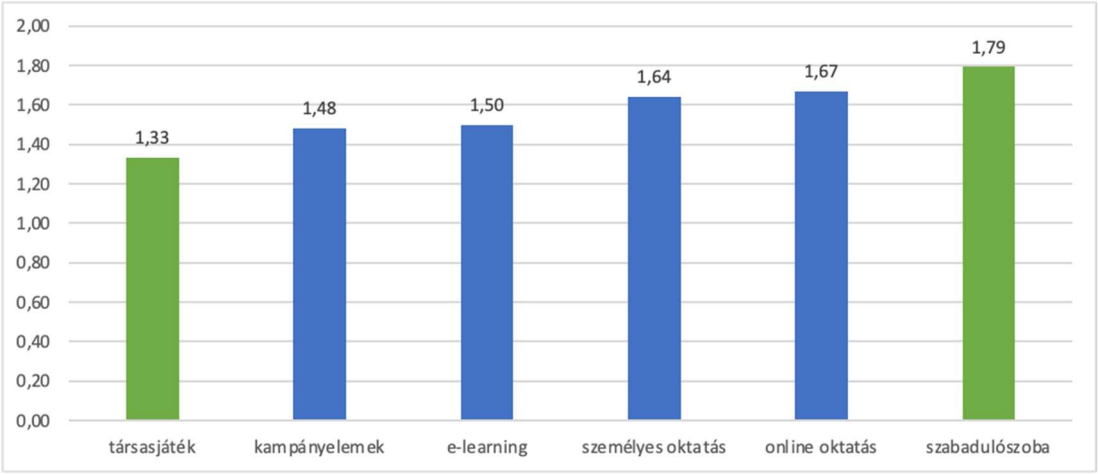
35. diagram: A kutatásba bevont különböző programok összesített eredmények alapján meghatározott rangsora a biztonságtudatossági ismeretek számosságának növelése szerint (átlagos új tudás, db) (forrás: saját szerkesztés)

Állami szférában a társasjáték előnye tovább nőtt az általgoshoz képest, itt átlag 2,29 db új ismeret átadását tulajdoníthattam neki. Ellenben a szabadulószoba alacsonyabb hatékonysággal (1,67 db ismeret) volt azonosítható ebben a szektorban (36. diagram).



36. diagram: A kutatásba bevont különböző programok összesített eredmények alapján meghatározott rangsora az állami szektorban a biztonságtudatossági ismeretek számosságának növelése szerint (átlagos új tudás, db) (forrás: saját szerkesztés)

A privát szektort vizsgálva az az érdekes helyzet alakult ki, hogy a sorrend teljesen megfordult: 1,79 db ismerettel a szabadulószoba lett a leghatékonyabb, és 1,33 db értéket ért el a társasjáték (37. diagram).



37. diagram: A kutatásba bevont különböző programok összesített eredmények alapján meghatározott rangsora a privát szektorban a biztonságtudatossági ismeretek számosságának növelése szerint (átlagos új tudás, db) (forrás: saját szerkesztés)

Megnéztem azt is, hogy a hagyományos, illetve gamifikációs programokban résztvevő felhasználók milyen arányban tudtak különböző mennyiségű új biztonságtudatossági ismeretet írni.

Ahogyan a 20. táblázat mutatja, nagyon hasonló értékek jöttek ki a mennyiség szempontjából, így feltételezhetően egyik megoldás sem befolyásolja jelentős mértékben a megszerzett ismeretek számát. Ennek igazolására Khi-négyzet próba végrehajtása lett volna alkalmas, azonban ez az adott mintán nem volt lehetséges (nem teljesült az a feltétel, hogy az összes cella maximum 20%-ában lehet az elvárt gyakoriság száma kevesebb, mint 5).

Összesítés	***1***	***2***	***3***	***4***	***5***	***6***	***7***
hagyományos	40,1%	27,2%	18,4%	8,8%	3,4%	1,4%	0,7%
gamifikációs	35,4%	**32,9%**	16,5%	**11,4%**	3,8%	0,0%	0,0%

20. táblázat: A hagyományos és gamifikációs programban résztvevő felhasználók aránya az újonnan szerzett információbiztonsági tudás száma szerint, kiemelve azon értékeket, melyek esetében a gamifikáció a hatékonyabb (forrás: saját szerkesztés)

Megbontottam azonban a táblázatot szektor szerint is, és az alábbi eredmények születtek:

Állami	***1***	***2***	***3***	***4***	***5***	***6***	***7***
hagyományos	**42,1%**	23,7%	15,8%	11,8%	3,9%	1,3%	1,3%
gamifikációs	28,6%	**38,1%**	16,7%	11,9%	4,8%	0,0%	0,0%

21. táblázat: A hagyományos és gamifikációs programban résztvevő, állami szektorban dolgozó felhasználók aránya az újonnan szerzett információbiztonsági tudás száma szerint, vastag szedéssel jelölve a kiemelt értékeket (forrás: saját szerkesztés)

Privát	*1*	*2*	*3*	*4*	*5*	*6*	*7*
hagyományos	38,0%	31,0%	21,1%	5,6%	2,8%	1,4%	0,0%
gamifikációs	**43,2%**	27,0%	16,2%	**10,8%**	2,7%	0,0%	0,0%

22. táblázat: A hagyományos és gamifikációs programban résztvevő, privát szektorban dolgozó felhasználók aránya az újonnan szerzett információbiztonsági tudás száma szerint, vastag szedéssel jelölve a kiemelt értékeket (forrás: saját szerkesztés)

A 21. és 22. táblázatból is látható, hogy a gamifikációs módszerek az állami szektorban 2 új ismeret átadásában hatékonyabbak (lásd. kiemelés), és több ismeretet körülbelül ugyanolyan hatékonysággal fejlesztenek, mint a hagyományos megoldások. A privát szektor esetében a játékosított megoldások ugyanúgy 1 ismeretet képesek leginkább fejleszteni, mint a hagyományos módszerek, és egyedül a 4 db ismeret átadásában bizonyulnak jelentős mértékben jobbnak (lásd. kiemelés), mint a hagyományos képzések (tehát vagy alacsony, vagy viszonylag jelentős mennyiségű új ismeretet képesek átadni).

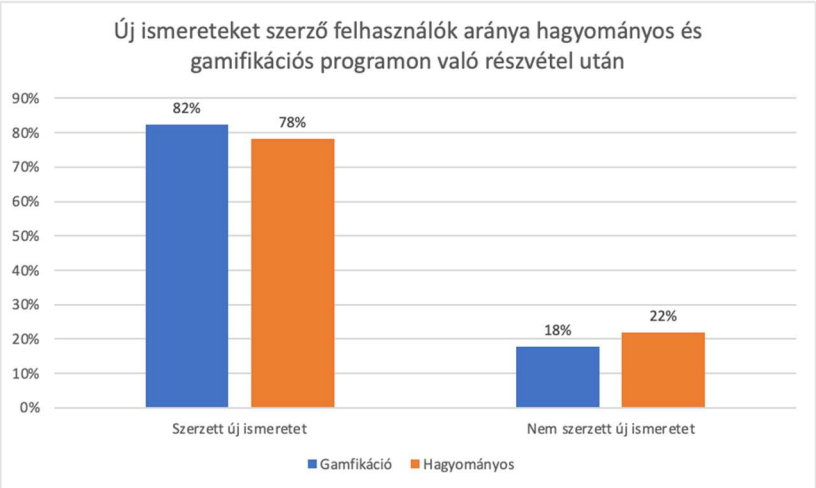
Mindkét esetben elmondhatjuk azonban, hogy a gamifikációs módszerek maximum 5 db új ismeret átadására voltak képesek, szemben a hagyományos lehetőségekkel (7 db új ismeret), ezért inkább speciális, célirányos oktatások esetében lehetnek előnyösebbek.

Fentiek alapján elmondható, hogy a gamifikációs módszerek közvetlenül a programban való részvételt követően összességében legalább olyan jól képesek a biztonságtudatossági ismeretek átadására azok számosságának növelése szempontjából, mint az egyéb hagyományos oktatási formák, így alkalmazhatóak a biztonságtudatossági képzések során.

4.8. A GAMIFIKÁCIÓS MÓDSZEREK ALKALMAZHATÓSÁGA A BIZTONSÁGTUDATOSABB FELHASZNÁLÓK SZÁMÁNAK NÖVELÉSÉBEN

Az ismeretek számának növelése mellett szintén érdekes az is, hogy az egyes módszerek hány felhasználót képesek elérni abban a tekintetben, hogy legalább 1 db új ismeretet szereznek a képzés során.

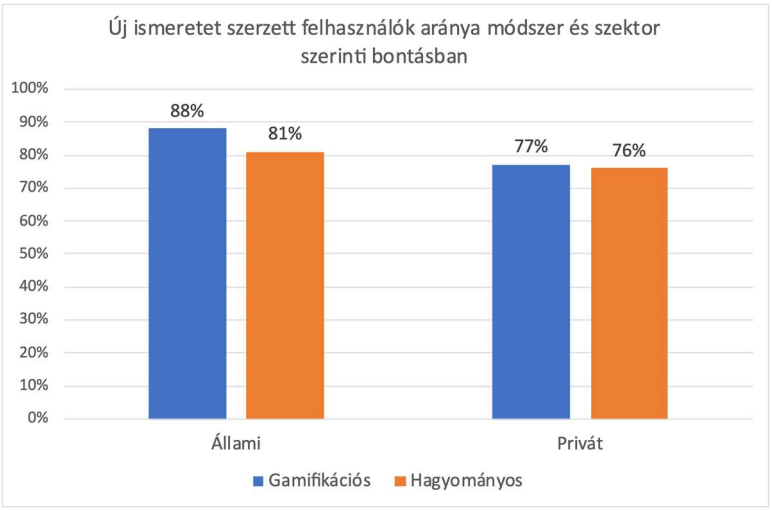
Megnéztem ezért azt is, hogy a gamifikációs és hagyományos módszereken résztvevők hány százaléka szerzett új ismeretet. Ahogyan a 38. diagram is mutatja, nagyon kicsi a különbség, a gamifikációs programon résztvevők 82%-a, míg a hagyományos oktatásban részesülő 78%-a távozott biztonságtudatosabban (legalábbis minimum 1 db új ismerettel).



38. diagram: A hagyományos és gamifikációs programban résztvevő, legalább 1 db új ismerettel rendelkező felhasználók aránya (forrás: saját szerkesztés)

Ezen értékekre végrehajtottam egy Khi-négyzet próbát is, hogy megnézzem a kapcsolatot aközött, hogy a felhasználó szerzett-e új biztonságtudatossági ismeretet, illetve, hogy milyen jellegű képzésen volt. Az eredmény 0,9419 lett, mely alapján elmondható, az, hogy a felhasználó milyen jellegű oktatáson volt, nagyon kis mértékben befolyásolja azt, hogy szerzett-e új ismeretet.

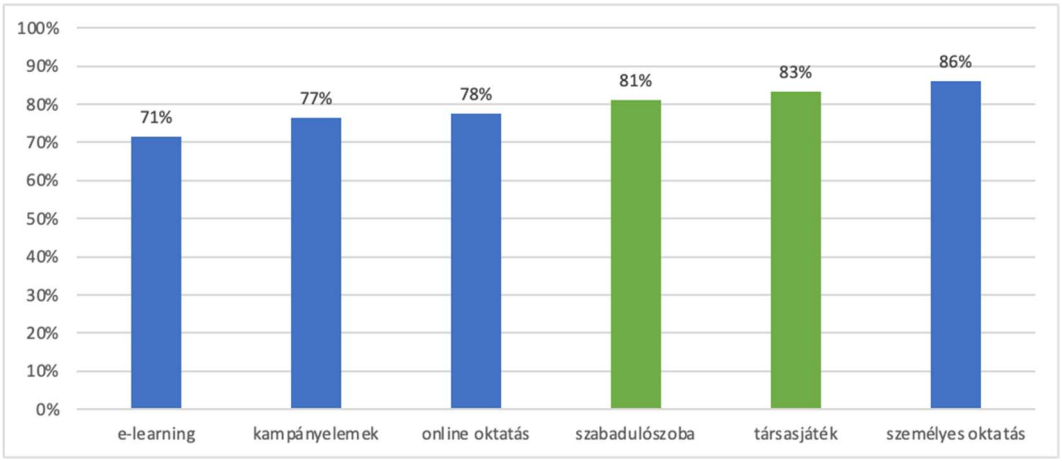
Ugyanezt a diagramot megbontottam aszerint, hogy az új tudást szerzett munkavállalók aránya hogyan alakult szektoronkénti bontásban. Itt az látszódik, hogy az állami szférában a gamifikációs módszerek valamivel nagyobb hatékonysággal (7%) növelték a legalább 1 új ismerettel gazdagodott felhasználók számát (39. diagram).



39. diagram: A hagyományos és gamifikációs programban résztvevő, legalább 1 db új ismerettel rendelkező felhasználók aránya szektor szerinti bontásban (forrás: saját szerkesztés)

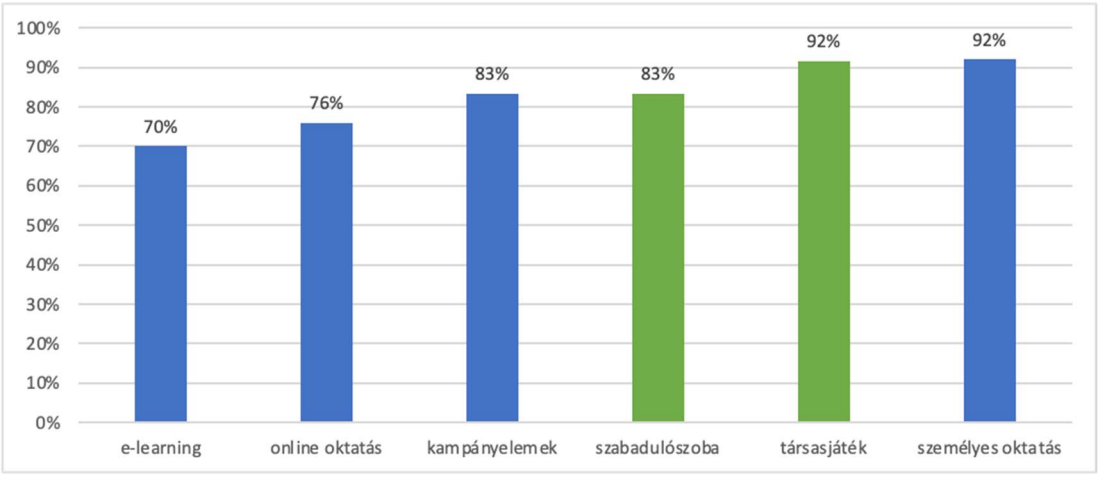
Itt is kibontottam az egyes módszereket, és néztem meg a két gamifikációs programelem eredményességét, rangsorban elfoglalt helyét. Ahogyan a lenti ábra is tükrözi, összességében a

személyes oktatás követő 2. (társasjáték), illetve 3. (szabadulószoba) szerepelnek, mindkettő 80% feletti értékkel (40. diagram).



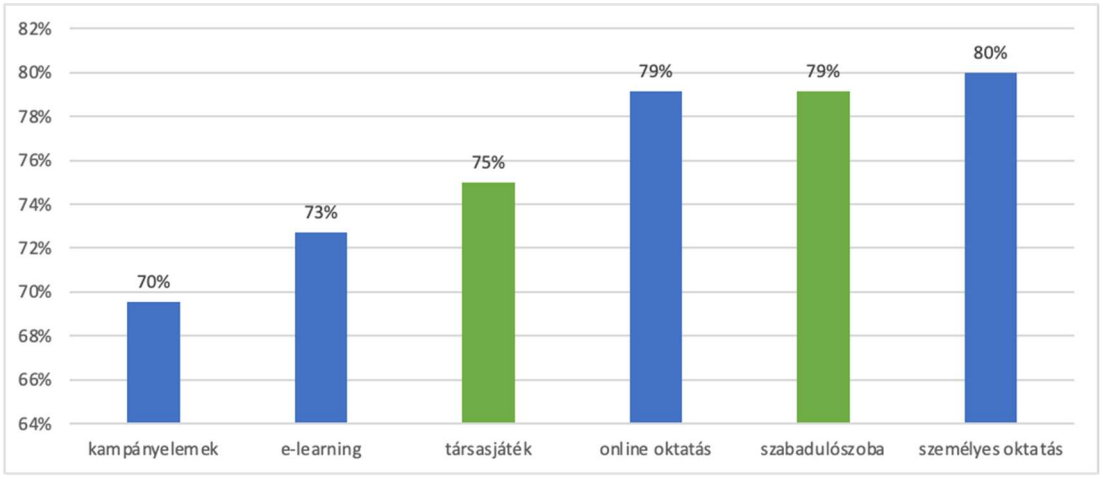
40. diagram: A kutatásba bevont különböző programok összesített eredmények alapján meghatározott rangsora a legalább 1 db új ismerettel rendelkező résztvevők aránya szerint (forrás: saját szerkesztés)

A diagramokból szokás szerint készítettem egy verziót az állami szervezetekre is, melyen a társasjáték 92%-kal holtversenyben az első helyre került a személyes oktatás mellé (41. diagram).



41. diagram: A kutatásba bevont különböző programok összesített eredmények alapján meghatározott rangsora az állami szektorban a legalább 1 db új ismerettel rendelkező résztvevők aránya szerint (forrás: saját szerkesztés)

A privát szférában ugyanez nem mondható el a társasjátékra, itt ugyanis 75%-os hatékonysággal működik csak a több biztonságtudatossági ismerettel rendelkező felhasználók számának növelésében, ezzel pusztán a kampányelemeket és az e-Learninget megelőzve. A szabadulószoba viszont az online oktatással holtversenyben a 2. helyen 1%-kal lemaradva szerepel a személyes oktatás mögött, tehát rendkívül sikeresnek mondható (42. diagram).



42. diagram: A kutatásba bevont különböző programok összesített eredmények alapján meghatározott rangsora a privát szektorban a legalább 1 db új ismerettel rendelkező résztvevők aránya szerint (forrás: saját szerkesztés)

Fentiek alapján elmondható, hogy a gamifikációs módszerek közvetlenül a programon való részvételt követően legalább olyan hatékonyan képesek a biztonságtudatossági ismeretek átadására, mint az egyéb hagyományos oktatási formák, illetve minimálisan több felhasználó ismereteit sikerül bővíteni a játékosítást alkalmazó megoldásokkal. Ezek tükrében a gamifikációs lehetőségek alkalmazhatóak a biztonságtudatossági képzések során, viszont kulcsfelhasználók bevonásával érdemes vizsgálni a különböző játékosított módszereket, és a szervezet számára legideálisabbat kiválasztani, mert ahogyan a felmérés eddigi eredményei is tükrözik, eltérő hatékonysággal működhetnek a különböző szervezeteknél.

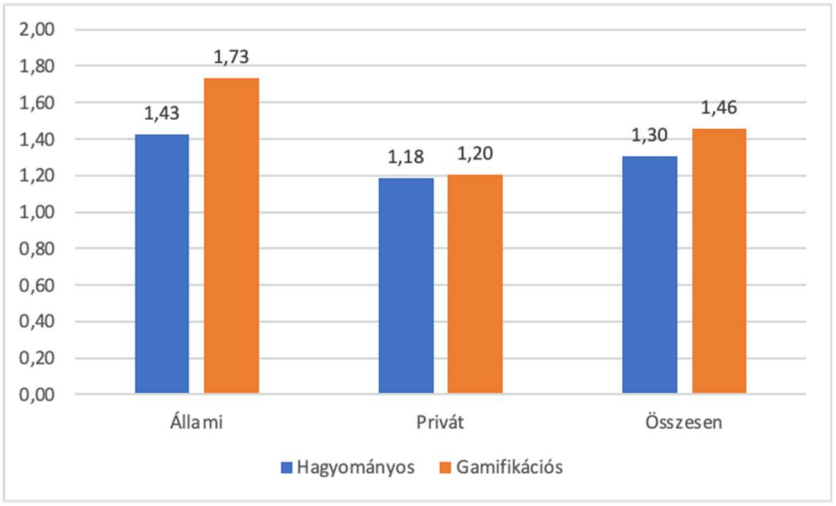
4.9. A GAMIFIKÁCIÓS MÓDSZEREK HATÉKONYSÁGÁNAK ÖSSZESÍTETT EREDMÉNYEI KÖZVELTENÜL A PROGRAMON VALÓ RÉSZVÉTELT KÖVETŐEN

A két különböző értékelési szempontot (legalább 1 új ismerettel bővült résztvevők száma, illetve átlagosan átadott új tudás) szerettem volna valamilyen módon ötvözni, és összességében megmondani, hogy melyik lehet a leghatékonyabb módszer. Ennek megállapítására összesített hatékonyság-indexként a két értékelés szerinti eredmény szorzatát választottam, melyeket a 23. táblázat foglal össze.

Az egyes programok eredményessége	*Átlagos szerzett ismeret (db)*	*Fejlesztett felhasználók aránya (%)*	Összesített eredmény (hatékonyság-index)
Gamifikációs	1,77	82%	1,46
Hagyományos	1,67	78%	1,30

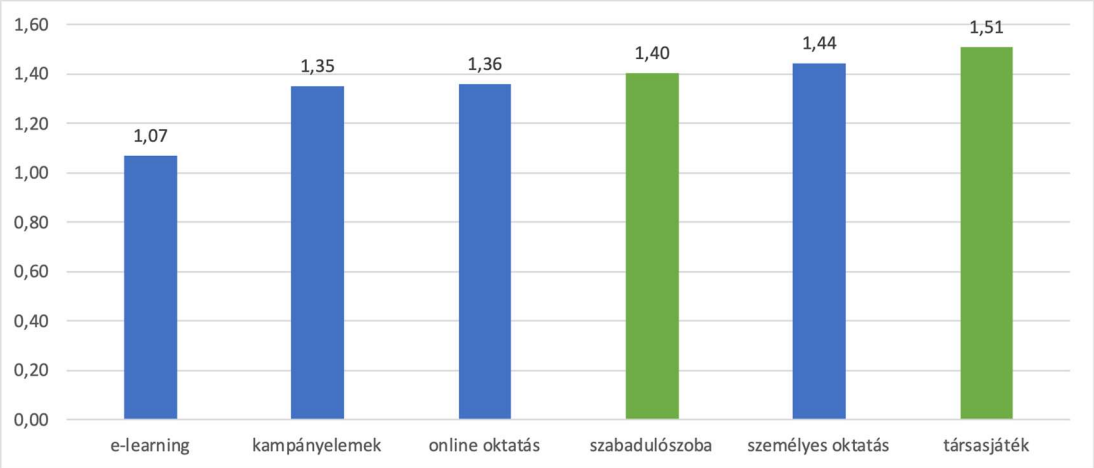
23. táblázat: A kutatásba bevont hagyományos és gamifikációs elemek értékelése átlagos szerzett ismeret, illetve a fejlesztett (legalább 1 db új ismerettel rendelkező) résztvevők aránya szerint (forrás: saját szerkesztés)

Az ezek alapján számított összesített eredmények mellett feltüntettem az alábbi diagramon a szektor szerinti megbontást is, melyből jól látható, hogy ezen számítás szerint a gamifikációs módszerek általánosságban kis mértékben hatékonyabbak, mint a hagyományos megoldások. Privát szféra esetében ez az érték (0,02) elhanyagolható, állami szektor esetében viszont már nagyobb különbség is mutatkozik (0,3) (43. diagram).



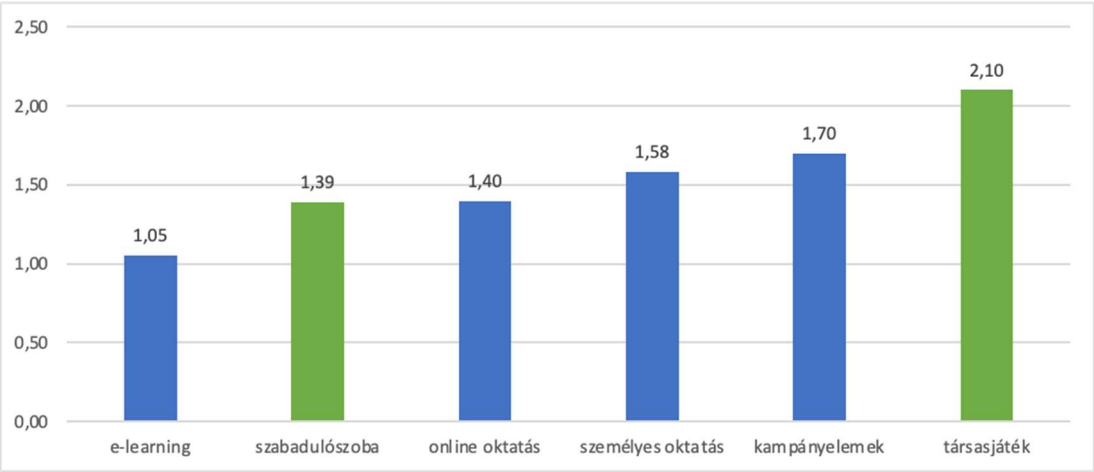
43. diagram: A kutatásban résztvevő hagyományos és gamifikációs módszerek összesített eredményei szektor szerinti bontásban (összesített hatékonyság-index) (forrás: saját szerkesztés)

Ugyanezen elven elkészítettem a számítást a különböző módszerekre is, és azt állapítottam meg, hogy eszerint az értékelés szerint összességében a társasjáték lehet a legjobb megoldás, majd a személyes oktatást követően a szabadulószoba alkalmas a legtöbb átlag ismeret átadására (44. diagram).



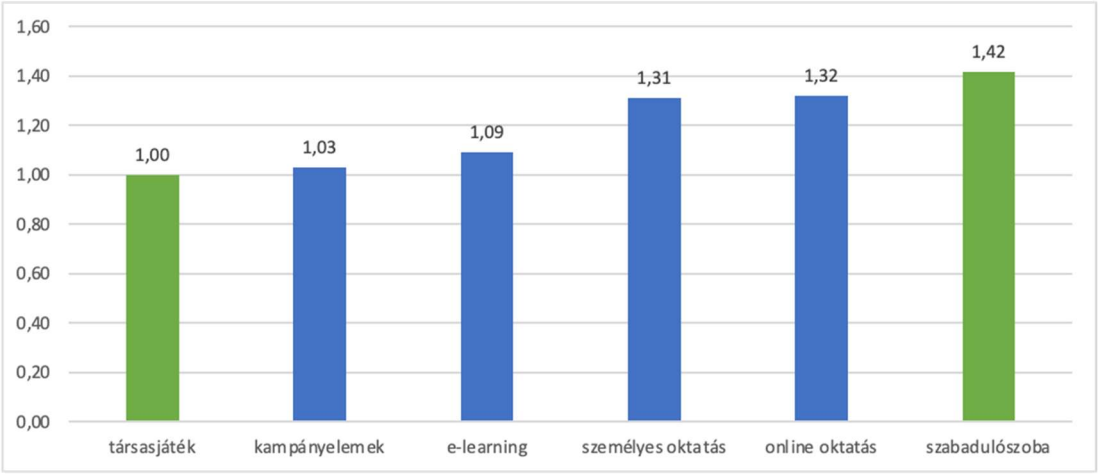
44. diagram: A kutatásban résztvevő biztonságtudatosság fejlesztő módszerek összesített eredményei (összesített hatékonyság-index) (forrás: saját szerkesztés)

Az állami szektorban viszont a szabadulószoba kevésbé hatékony ezen a téren, ugyanis összességében 1,39-es értékkel az utolsó előtti helyen szerepel és egyedül az e-Learning-nél bizonyul hatékonyabbnak, kimagasló értéket ér el viszont a társasjáték (45. diagram).



45. diagram: A kutatásban résztvevő biztonságtudatosság fejlesztő módszerek összesített eredményei az állami szektorban (összesített hatékonyság-index) (forrás: saját szerkesztés)

A privát szektorban ismét megfordultak az arányok, és összességében a szabadulószoba mondható ezen értékelés szerint a leghatékonyabbnak, míg a társasjáték a legkevésbé hatékony megoldásnak (46. diagram).



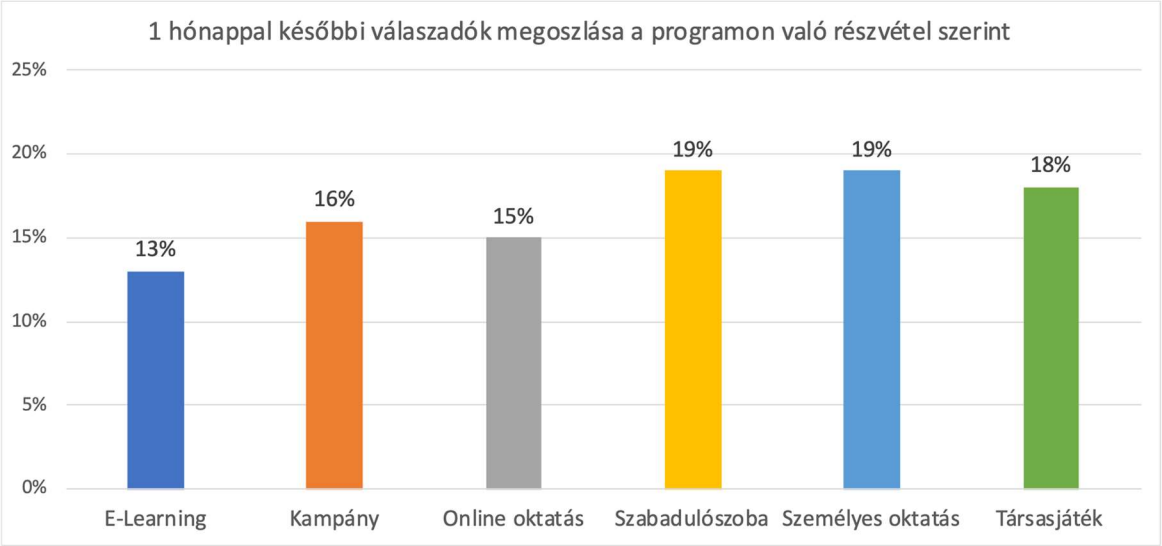
46. diagram: A kutatásban résztvevő biztonságtudatosság fejlesztő módszerek összesített eredményei a privát szektorban (összesített hatékonyság-index) (forrás: saját szerkesztés)

A fentiek ismét arra világítottak rá, hogy a gamifikációs módszerek közvetlenül a programban való részvételt követően összességében legalább olyan hatékonyan képesek a biztonságtudatossági ismeretek átadására, mint az egyéb hagyományos oktatási formák, illetve minimálisan több ismeretet képesek átadni a játékosítást alkalmazó megoldásokkal. Ezek tükrében a gamifikációs lehetőségek alkalmazhatóak a biztonságtudatossági képzések során, viszont érdemes kulcsfelhasználókkal vizsgálni a különböző játékosított módszereket, és a szervezet számára legideálisabbat kiválasztani, mert ahogyan a felmérés eddigi eredményei is tükrözik, eltérő hatékonysággal működhetnek a különböző szervezeteknél.

4.10. A GAMIFIKÁCIÓS MÓDSZEREK HATÉKONYSÁGÁNAK EREDMÉNYEI EGY HÓNAPPAL A PROGRAMON VALÓ RÉSZVÉTELT KÖVETŐEN

A kutatás utolsó lépéseként megvizsgáltam, hogy egy hónappal a programok megvalósítását követően a felhasználók mennyire emlékeznek a tanultakra, ezért egy utolsó kérdőívet (K3) is kitöltettem a résztvevőkkel. Ezt a felhasználók 68,3%-a töltötte ki. A válaszadók 48,9%-a az állami szférából, az 51,1%-a pedig a privát szektorból került ki.

Programon való részvétel szempontjából az utolsó kört is kitöltő felhasználók aránya a következőképpen nézett ki, tehát minden oktatási formában résztvevő csoport képviselve volt (47. diagram).



47. diagram: A kutatás utolsó (K3) kérdőívének válaszadói program szerinti bontásban (forrás: saját szerkesztés)

Ahogyan a diagram is tükrözi, a legtöbb utolsó körös válaszadó a személyes programok résztvevői közül került ki, ez azon feltételezésemet erősítette meg, hogy akikkel személyes kontaktus volt, jobban elköteleződtek a kutatás támogatása iránt (így feltételezhetően az információbiztonság iránt is). Tekintve, hogy mindkét gamifikációs program személyes jelenlétet igényelt, így arra vonatkozóan nem tudtam következtetést levonni, hogy a gamifikációs élmény növelte-e a kitöltési hajlandóságot.

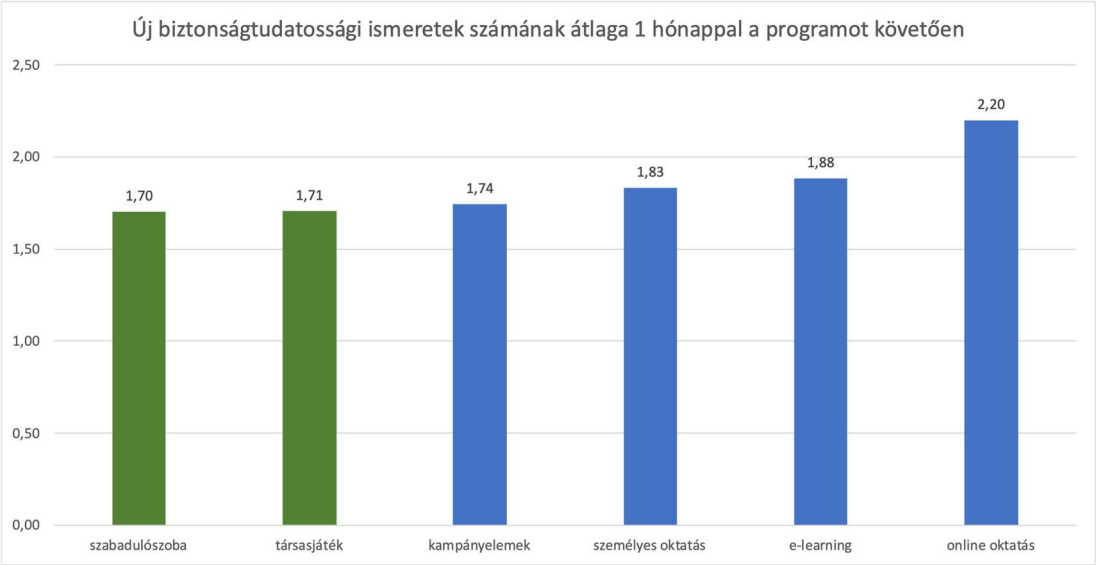
Ami a felhasználók biztonságtudatossági ismereteinek bővítését illeti, összességében a válaszadók 80,4%-a tudott legalább 1 új ismeretet írni az utolsó kérdőívben, mely nem szerepelt a legelső kérdőívre adott válaszai között – tehát a programnak köszönhetően fejlődött.

Ezt lebontva gamifikációs és hagyományos programelemekre megállapítottam, hogy közel azonos mértékben nőtt a több biztonságtudatossági ismerettel rendelkező felhasználók száma mind a gamifikációs (80,3%), mind a hagyományos (80,5%) programok résztvevői esetében – a különbség elhanyagolható mértékű a hagyományos képzések javára.

Természetesen itt is megnéztem, hogy hogyan alakult az átlagos új biztonságtudatossági ismeretek száma, és itt megállapítottam, hogy a gamifikációs módszerek átlag 1,7 db új ismeretet eredményeztek egy hónappal később, a hagyományos programok pedig átlagosan 1,92 db új ismeretet jelentettek, tehát a felhasználók összességében hosszú távon többet tanultak a hagyományos megoldásokból.

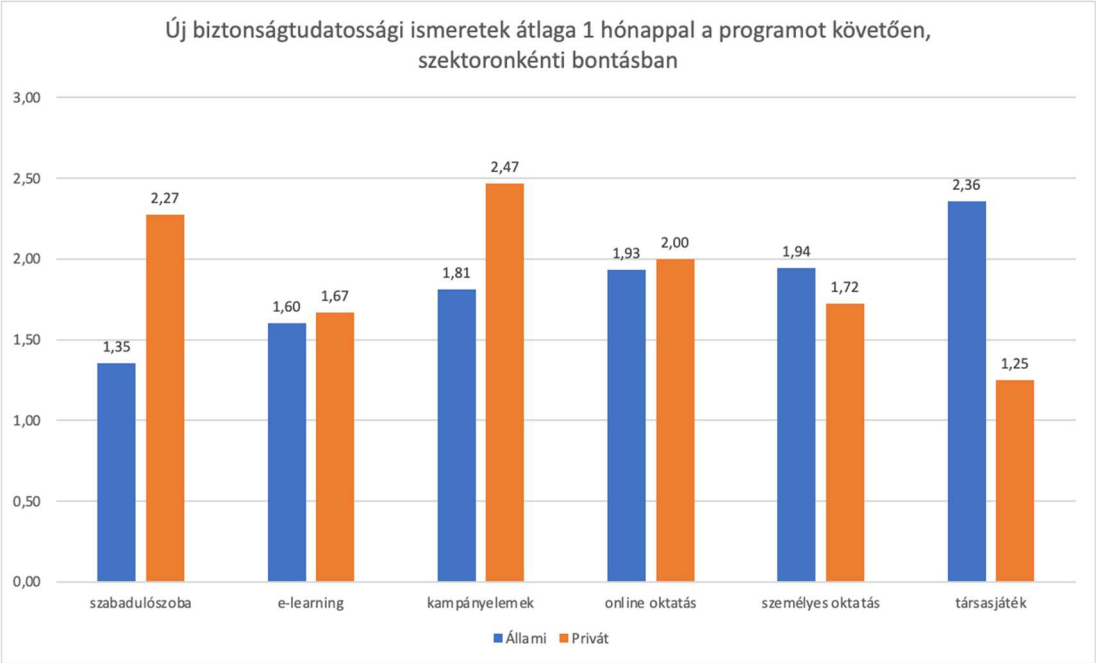
Az egyes programok hatékonysági rangsora az átadott új ismeretek száma szerint a 48. diagramon látható, mely alapján az online oktatás bizonyult a tudás bővítése szempontjából a legsikeresebb módszernek. Második helyre került az e-Learning, itt azonban a nagyon kis részvételi arány és a korábbi értékelés miatt felmerült bennem annak a gyanúja, hogy a

résztvevők elővették a korábbi e-Learning anyagot (a kampányelemeken kívül ez az egy anyag volt, amit meg tudtak tartani, le tudtak menteni) és felelevenítették a tudásukat (korábbi érték átlagosan 1,5 db új ismeret volt).



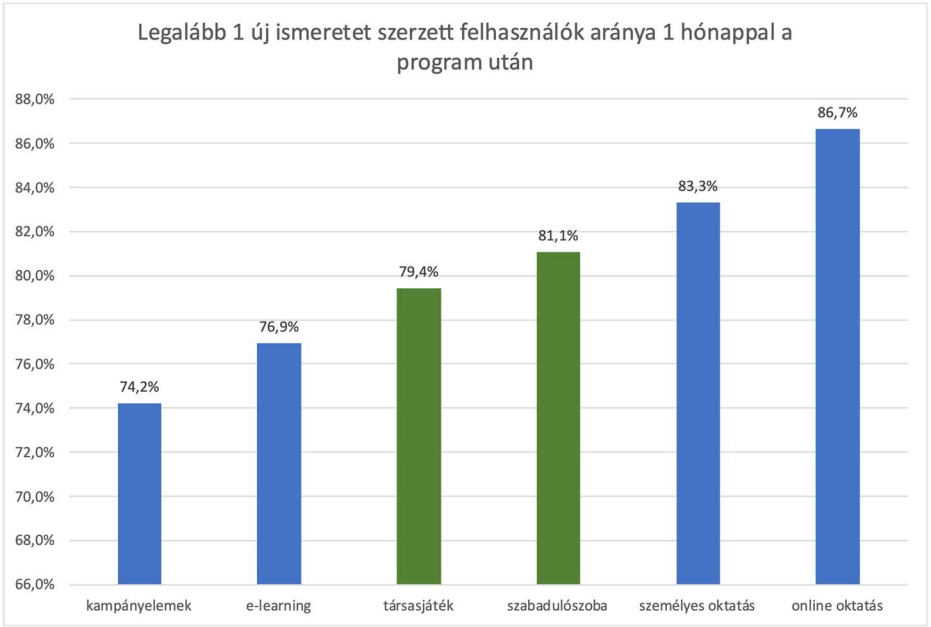
48. diagram: A kutatásba bevont különböző programok 1 hónappal későbbi eredmények alapján meghatározott rangsora az átlagosan szerzett új ismeretek száma (db) szerint (forrás: saját szerkesztés)

Szektoronkénti bontásban az egy hónappal későbbi eredmények alapján azt lehet elmondani, hogy állami szférában leginkább a társasjáték volt a leghatékonyabb megoldás hosszútávon (2,36 db), a privát szférában ez teljesen az ellentette a legalacsonyabb 1,25 db új ismeret értékkel. A privát szektorban a kampányelemek (2,47 db) és a szabadulószoba (2,27 db) domináltak. Érdekesség, hogy az összességében legjobb eredményt elérő e-Learning közel azonos, 1,6 db (állami) és 1,67 db (privát) értéket ért el (49. diagram).



49. diagram: A kutatásba bevont különböző programok 1 hónappal későbbi eredményei szektoronkénti bontásban az átlagosan szerzett új ismeretek száma (db) szerint (forrás: saját szerkesztés)

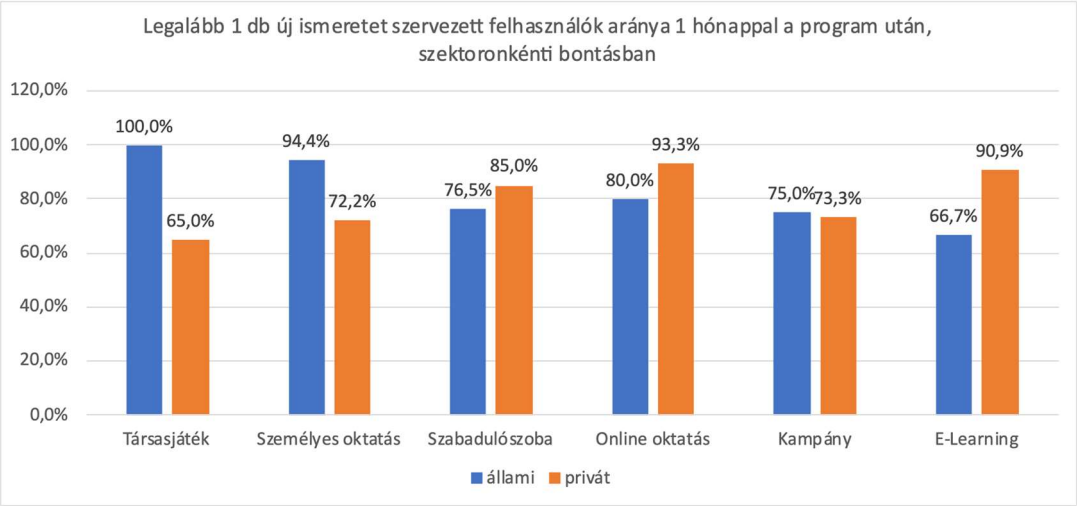
Ha csak azt nézem, hogy hogyan változott a legalább egy új ismerettel rendelkező felhasználók aránya, akkor a gamifikációs módszerek a középmezőnyben végeztek, és az online, valamint azt követően a személyes oktatások voltak a leghatékonyabbak, ezek által átadott ismeretek maradtak meg a legtöbb felhasználóban. Ezeket az értékeket az 50. diagram mutatja be.



50. diagram: A kutatásba bevont különböző programok rangsora az 1 hónappal későbbi eredmények alapján, a legalább 1 db új ismeretet szerzett felhasználók aránya szerint (forrás: saját szerkesztés)

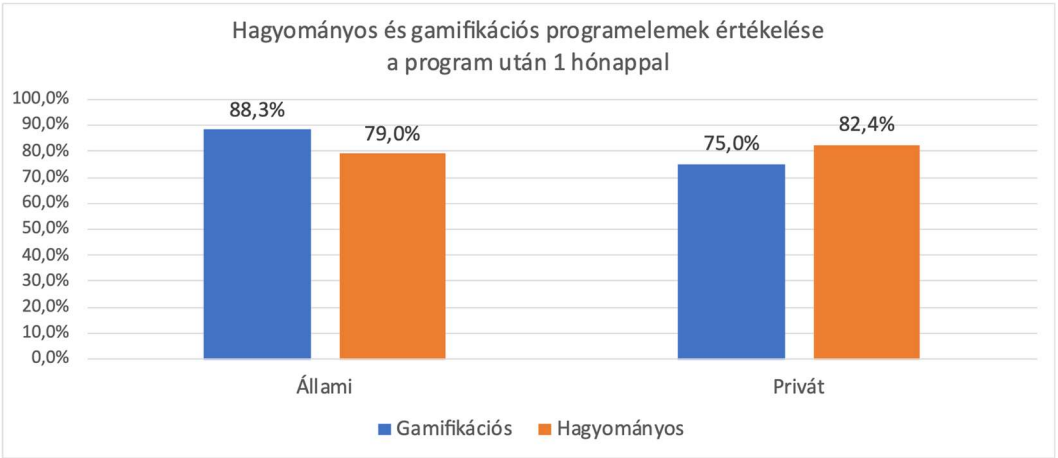
A szektor szerinti bontás itt is érdekes eredményeket rejt. Állami szférát tekintve a társasjáték bizonyult hosszú távon a legtöbb felhasználót fejlesztő megoldásnak, ebben az esetben ugyanis minden résztvevő tudott legalább egy új biztonságtudatossági ismeretet írni.

A privát szektor hosszútávon leghatékonyabb megoldásai az egyébként bevett gyakorlatként alkalmazott online oktatás (93,3%) és az e-Learning (90,9%) voltak. Ezek mellett a szabadulószoba előkelő 3. helyezést ért el (85,0%), a másik gamifikációs elem azonban az utolsó helyen végzett és csak a résztvevők 65,0%-át fejlesztette (51. diagram).



51. diagram: A kutatásba bevont különböző programok eredményei az 1 hónappal későbbi eredmények alapján, a legalább 1 db új ismeretet szerzett felhasználók aránya szerint, szektoronkénti bontásban (forrás: saját szerkesztés)

Összességében a privát szektorban a hagyományos programelemek 82,4%-os, a gamifikációs módok pedig 75%-os eredményt értek el, tehát a klasszikus módszerek ott hosszútávon hatékonyabbnak bizonyulnak, míg az állami szférában 79% – 88,3% aránnyal a gamifikációs megoldások hosszútávon is hatékonyak. Az eredményeket az 52. diagram szemlélteti.



52. diagram: A kutatásba bevont különböző programok eredményei az 1 hónappal későbbi eredmények alapján, a legalább 1 db új ismeretet szerzett felhasználók aránya szerint, szektoronkénti bontásban (forrás: saját szerkesztés)

A fentiek alapján elmondhatjuk, hogy hosszútávon általánosságban az előadás jellegű, akár online vagy személyesen tartott programok fejlesztik a legtöbb felhasználó biztonságtudatossági ismereteit, érdemes azonban alkalmazni gamifikációs lehetőségeket is, hiszen megbontva a módszereket az állami szférában a társasjáték, a privát szektorban pedig a szabadulószoba jelenthet hatékony kiegészítő megoldást.

4.11. A GAMIFIKÁCIÓS MÓDSZEREK HATÉKONYSÁGÁNAK ÖSSZESÍTETT EREDMÉNYEI EGY HÓNAPPAL A PROGRAMON VALÓ RÉSZVÉTELT KÖVETŐEN

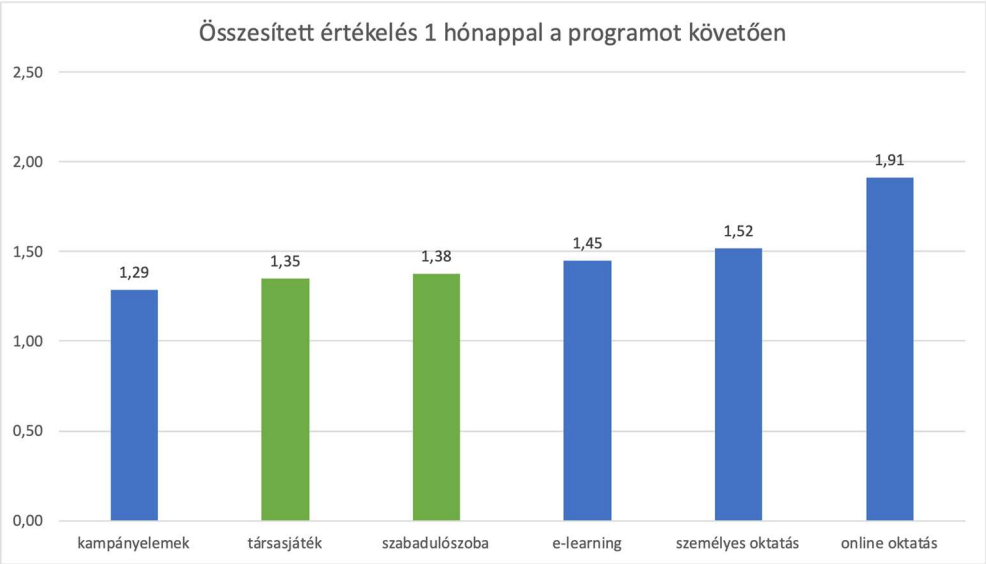
A teljesség kedvéért a két különböző értékelési szempontot (legalább 1 új ismerettel bővült résztvevők száma, illetve átlagosan átadott új tudás) ebben az esetben is szerettem volna valamilyen módon ötvözni, és összességében megmondani, hogy hosszútávon melyik lehet a leghatékonyabb módszer. Ennek megállapítására itt is a két értékelés szerinti eredmény szorzatát választottam, mely eredményeket a 24. táblázat foglalja össze.

Az egyes programok eredményessége	*Átlagos szerzett ismeret (db)*	*Fejlesztett felhasználók aránya (%)*	Összesített eredmény
Gamifikációs	1,70	80,3%	1,36
Hagyományos	1,92	80,5%	1,54

24. táblázat: A kutatásba bevont hagyományos és gamifikációs elemek értékelése átlagos szerzett ismeret, illetve a fejlesztett (legalább 1 db új ismerettel rendelkező) résztvevők aránya szerint, 1 hónappal későbbi eredmények alapján (forrás: saját szerkesztés)

Az eredmények azt tükrözik, hogy hosszú távon összességében a hagyományos biztonságtudatosság fejlesztési programok jelenthetnek hatékonyabb megoldást a gamifikációs megoldásokkal szemben.

Ugyanezen elven elkészítettem a számítást a különböző módszerekre is, és azt állapítottam meg, hogy eszerint az értékelés szerint összességében az online oktatás lehet a legjobb megoldás, ezt jelentős különbségekkel követi csak a többi módszer (53. diagram). (Az e-Learning értékelését az előző fejezetben írtak miatt itt is fenntartásokkal kezelem.)



53. diagram: A kutatásban résztvevő biztonságtudatosság fejlesztő módszerek összesített eredményei 1 hónappal a programot követően (összesített hatékonyság-index) (forrás: saját szerkesztés)

A fentiek alapján azt lehet elmondani, hogy hosszútávon összességében az online oktatás minősül a leghatékonyabb megoldásnak, az összes többi módszer jelentősen lemaradva (több, mint 25%-os különbség) követi. A kevésbé hatékony megoldások között viszont nincsenek ilyen jelentős különbségek, így ezek alapján a gamifikációs módszerek biztonságtudatosság fejlesztési képességét továbbra sem zárom ki.

4.12. KLASZTERELEMZÉS AZ ISMERETEK SZÁMÁNAK BŐVÍTÉSE SZEMPONTJÁBÓL TÖRTÉNŐ ÉRTÉKELÉSHEZ

Annak megállapítására, hogy mind rövid- (K2), mind hosszútávon (K3), valamint összességében melyik biztonságtudatosságot fejlesztő módszer mennyire hatékony, klaszterelemzést is végrehajtottam.

Ahogyan Sajtos és Mitev (2007) megfogalmazza, „*a klaszterezés hasonló dolgok csoportosítását jelenti, s gyakorlatilag az osztályozás szinonimája. A klaszteranalízis alapvető célja, hogy a megfigyelési egységeket viszonylag homogén csoportokba rendezze, az elemzésbe bevont változók alapján*”. (Sajtos és Mitev, 2007, p. 283.) Ezen meghatározás alapján a módszer megfelelően illeszthető a kutatásomban vizsgált problémára, melynek során egyrészt az egyes felhasználókat szeretném csoportba sorolni megszerzett ismereteik vonatkozásában, másrészt a vizsgált biztonságtudatosság fejlesztési módszereket, azok hatékonysága szempontjából.

A klaszterezés lépései Sajtos és Mitev (2007) alapján a következők (6. ábra):

6. ábra: Klaszterelemzés folyamata (forrás: saját szerkesztés Sajtos és Mitev, 2007 alapján)

A klaszterelemzés elvégzésének feltételei esetemben teljesültek, a vizsgált adatok között kiugró érték nem volt tapasztalható, az elemzés során pedig standardizált adatokkal dolgoztam. A standardizálás során az egyes változók értékét standard értékké alakítottam át a következő képlet szerint (Sajtos és Mitev, 2007):

$$z_i = (X_i + \underline{X}) / s_x$$

Klaszterezési módszer tekintetében a nem-hierarchikus K-közép eljárást választottam, melynek jellemzője, hogy akkor előnyös, ha a mintavételi egységek száma magas, nincsenek kiugró adatok, a kapott eredmények kevésbé függenek a távolságmértéktől, valamint attól, hogy van-e irreleváns változó az elemzésben. (Sajtos és Mitev, 2007)

Az első klaszterelemzés során azt vizsgáltam, hogy azok a felhasználók, akik mind a K2, mind a K3 kérdőívet kitöltötték, ismereteik számának növekedését tekintve milyen csoportba tartoznak, és az egyes csoportok jellemzően melyik képzési formában vettek részt. Ennek megfelelően ebben a vizsgálatban kizárólag azzal a 194 darab kérdőívvel dolgoztam, melyet a válaszadók mind a K2, mind pedig a K3 fázisban kitöltöttek.

Az első vizsgálat során K-közép elemzést végeztem 4 klaszterre. A klaszterek számát szakértői tapasztalatok, valamint az előző fejezetekben végzett általános statisztikai eredmények alapján határoztam meg, feltételezve, hogy az eredmények a „Nem tanult”, „Rövid távon tanult”, „Hosszútávon tanult”, valamint a „Rövid és hosszútávon tanult” kategóriákat reprezentálják.

A vizsgált változók a K2 kérdőívben megadott új ismeretek száma, valamint a K3 kérdőívben megadott új ismeretek száma volt, melyre a következő 4 klasztert határozta meg az SPSS (25. táblázat):

	1	**2**	**3**	**4**
Új ismeretek száma (K2)	2,22460	-0,77564	0,64725	-0,07256
Új ismeretek száma (K3)	1,30982	-0,39688	-0,41057	1,66601

25. táblázat: Klaszter középpontok (forrás: saját szerkesztés SPSS adatok alapján)

A vizsgálat eredménye igazolta a 4 klaszterre vonatkozó feltételezésemet, és a klaszterek a vártak szerint a következőképpen alakultak, az egyes program-típuson résztvevő felhasználókat a következő klaszterekbe soroltam:

- 1 = A felhasználó rövid és hosszú távon is átlag feletti új ismereteket szerzett, tehát a módszer összességében hatékony. (Klaszter elnevezés: Rövid és hosszú távon tanult.)
- 2 = A felhasználó sem rövid, sem hosszú távon nem szerzett az átlag szintet elérő új ismeretet, tehát a módszer nem hatékony. (Klaszter elnevezés: Nem tanult.)
- 3 = A felhasználó rövid távon szerzett átlag feletti ismereteket, hosszú távon nem érte el az átlagot, tehát a módszer rövid távon hatékony. (Klaszter elnevezés: Rövid távon tanult.)
- 4 = A felhasználó rövid távon átlagos ismereteket szerzett, hosszú távon viszont átlag feletti új ismeretre tett szert, tehát a módszer hosszú távon hatékony. (Klaszter elnevezés: Hosszú távon tanult.)

Az egyes klaszterekbe eső felhasználók száma a következőképpen alakult (26. táblázat):

Klaszter	Elemszám (db)
Rövid és hosszútávon tanult (1)	13
Nem tanult (2)	89
Rövid távon tanult (3)	65
Hosszú távon tanult (4)	27
Összesen	**194**

26. táblázat: Klaszterek elemszáma (forrás: saját szerkesztés SPSS adatok alapján)

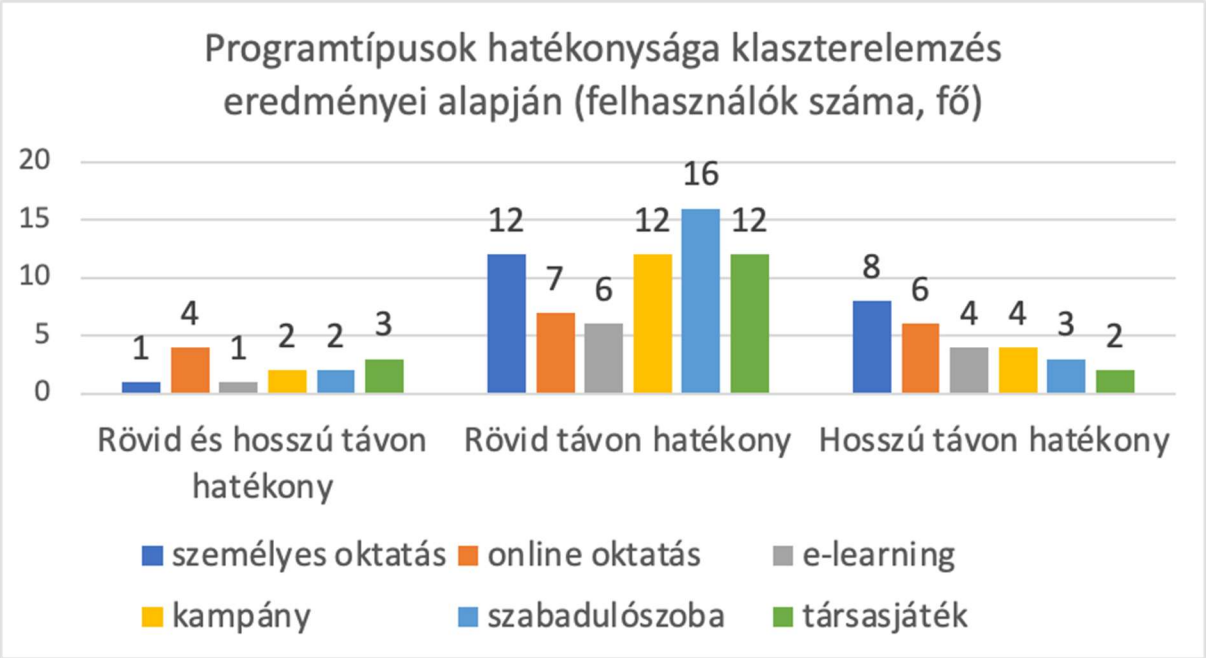
A 27. táblázatban feltüntetett, kapcsolódó ANOVA tábla alapján a klaszterhez való tartozásban a közvetlenül a program utáni új ismeretek számának van a legnagyobb szerepe (F érték magasabb):

	Cluster		Error		F	Sig.
	Mean Square	df	Mean Square	df		
Új ismeret (K2) (db)	48,418	3	0,251	190	192,667	<0,001
Új ismeret (K3) (db)	40,740	3	0,373	190	109,362	<0,001

27. táblázat: ANOVA tábla (forrás: saját szerkesztés SPSS adatok alapján)

A szignifikancia mindkét változó esetén kisebb, mint 0,05, ezért a nullhipotézis elutasítható, a csoportok közötti különbség szignifikáns.

Ezt követően a klaszter-besorolásokat hozzárendeltem az egyes felhasználókhoz, majd megvizsgáltam, hogy az egyes klaszterekbe sorolt felhasználók közül hányan vettek részt az egyes programokon. Az eredményekből az 55. diagramot alkottam, melyen nem szerepeltettem a „Nem tanult” klaszterbe sorolt felhasználók értékeit (tehát a nem hatékonynak minősített módszereken résztvevők számát).



54. diagram: Programtípusok hatékonysága klaszterelemzés eredményei alapján (felhasználók száma, fő) (forrás: saját szerkesztés)

Az eredményből az a következtetés vonható le, hogy rövid- és hosszútávú biztonságtudatossági fejlesztésekre az online oktatás a legalkalmasabb, melyet a társasjáték követ, de figyelembe kell venni, hogy nincsen jelentős különbség az eredmények között, illetve a felhasználók csupán 6,7%-a tartozik ebbe a csoportba.

Az elemzés alapján rövid távon a szabadulószoba a leghatékonyabb, majd a társasjáték, a személyes oktatás és a kampány követi – tehát olyan módszerek, melyek személyes jelenlétet igényelnek.

Hosszú távon a személyes oktatás, majd az online oktatás bizonyultak a legjobbnak, a gamifikációs módszerek pedig a legkevésbé hatékonyabbnak ezen a téren.

Az elemzés megerősítette, hogy a gamifikációs módszerek elsősorban rövid távon, figyelemfelkeltés céljából a leghatékonyabbak.

4.13.KLASZTERELEMZÉS AZ ÖSSZESÍTETT ÉRTÉKELÉSRE

Végezetül az előző ponthoz hasonlóan megvizsgáltam szintén K-közép módszerrel azt is, hogy mind K2 és K3 kérdőívek során, mind új ismeretek számának és biztonságtudatosabb felhasználók számának függvényében melyik vizsgált biztonságtudatosságot módszer összességében milyen hatékonyságú.

Ugyan az előzetes hierarchikus klaszterelemzés, melyet a kis minta miatt végeztem, 2 klasztert javasolt, ennek ellenére K-közép módszerrel a 28. táblázatban bemutatott 3 klasztert alkottam:

	1	**2**	**3**
Új ismeretek száma (K2)	0,44610	0,37175	-2,00745
Tanult felhasználók száma (K2)	0,37463	0,37463	-1,87317
Új ismeretek száma (K3)	-0,82687	0,73983	-0,56575
Tanult felhasználók száma (K3)	-1,08799	0,87039	-0,43519

28. táblázat: Klaszter középpontok (forrás: saját szerkesztés SPSS adatok alapján)

A klaszterek számának becslése során ismételten a korábbi szakértői tapasztalatokra, valamint az általános statisztikai eredményekre támaszkodtam. Ezek alapján az egyes program-típusok összesített eredményeit a következő klaszterekbe soroltam:

- 1 = A felhasználók biztonságtudatossági ismereteit, valamint a biztonságtudatosabb felhasználók számát rövid távon átlag felett növeli, hosszú távon viszont nem éri el az átlagos eredményt. (Klaszter elnevezés: Rövid távon hatékony.)
- 2 = A felhasználók biztonságtudatossági ismereteit, valamint a biztonságtudatosabb felhasználók számát rövid és hosszú távon is átlag felett növeli. (Klaszter elnevezés: Abszolút hatékony.)
- 3 = A felhasználók biztonságtudatossági ismereteit, valamint a biztonságtudatosabb felhasználók számát rövid és hosszú távon sem növeli az átlagos mértékben. (Klaszter elnevezés: Nem hatékony.)

Ahogyan a 29. számú, a módszereket klaszterekbe soroló táblázat is mutatja, az elemzés alapján egyedül az e-Learning nem bizonyult hatékony megoldásnak, abszolút hatékonynak pedig a személyes oktatás, az online oktatás, valamint a szabadulószoba került minősítésre.

Oktatási mód	Klaszter	Távolság
Személyes oktatás	2	0,649
Online oktatás	2	1,061
E-Learning	3	0,000
Kampány	1	0,632
Szabadulószoba	2	0,665
Társasjáték	1	0,632

29. táblázat: Oktatási módszerek klaszterbe sorolása (forrás: saját szerkesztés SPSS adatok alapján)

A 30. táblázatban látható, kapcsolódó ANOVA tábla alapján láthatjuk, hogy a klaszterhez való tartozásban a közvetlenül a program utáni új ismeretek számának van a legnagyobb szerepe (F érték a legmagasabb).

	Cluster		Error		F	Sig.
	Mean Square	df	Mean Square	df		
Új ismeret (K2) (db)	2,421	2	0,053	3	46,105	0,006
Tanult felhasználók (K2) (db)	2,105	2	0,263	3	8.000	0,063
Új ismeret (K3) (db)	1,665	2	0,557	3	2,990	0,193
Tanult felhasználók (K3) (db)	2,415	2	0,057	3	42,500	0,006

tábla:

30. táblázat: ANOVA tábla (forrás: saját szerkesztés SPSS adatok alapján)

A „Tanult felhasználók (K2)" és az „Új ismeret (K3)" változók esetében a szignifikancia szint meghaladja a 0,05 értéket, mely alapján a nullhipotézis nem utasítható el, azaz nincsen elegendő bizonyíték szignifikáns különbségek megállapítására.

Ezen elemzés is azt támasztja alá, hogy a gamifikációs módszerek összességében, mind a biztonságtudatosabb felhasználók számának a növelése, mind a biztonságtudatossági ismeretek számának bővítése során is képesek a biztonságtudatosság fejlesztésére.

4.14. A GAMIFIKÁCIÓS MÓDSZEREK HATÉKONYSÁGA A KÜLÖNBÖZŐ BIZTONSÁGTUDATOSSÁGI ISMERETEK ÁTADÁSA SZEMPONTJÁBÓL

Hipotézisemhez részlegesen kapcsolódik, de ennek a blokknak a végén azt is megnéztem, hogy a gamifikációs módszerek az általam korábban a vizsgálatba bevont 10 biztonságtudatossági ismeret közül melyiket, illetve milyen hatékonysággal képesek fejleszteni.

Ehhez készítettem egy olyan táblázatot, melyben kiszámoltam, hogy az egyes módszerek résztvevőinek hány százaléka írta az adott biztonságtudatossági ismeretet új ismeretként. A táblázatban automatikus formázással és ikonkészlettel jelöltem, hogy az adott programelem az eredmények alapján mennyire képes az adott ismeret fejlesztésére, ehhez a következő általános

beállítást hagytam meg: ha a válaszadók aránya a felső harmadba tartozott (67%-os beállítás a feltételes formázáson), akkor hatékonynak (zöld pötty), ha az alsó harmadba (33%-os beállítás a feltételes formázáson), akkor pedig nem hatékonynak minősítettem (piros pötty). A két érték között átlagosnak minősítettem (sárga pötty).

Első körben a második, közvetlenül a program után kitöltött kérdőív (K2) eredményei alapján készítettem el a 31. táblázatban látható értékelést. Ebből már számszerűen is jól látszódik, hogy a gamifikációs módszerek összességében 5 ismeret esetében bizonyultak hatékonynak, és csak 2 esetben lehetett egyértelműen azt mondani, hogy nem jó megoldások a tudatosításra (tiszta képernyő, adathalászat). Ezzel szemben a hagyományos módszerek csak 3 esetben bizonyultak hatékonynak, 4 ismeret esetében pedig nem minősültek annak.

Módszer és tudatossági elem	*Gamifikációs*		*Hagyományos*	
Tiszta asztal	🟢	24,0%	🟡	17,6%
Tiszta képernyő	🔴	4,2%	🔴	6,4%
Kulcsok, kártyák	🟢	27,1%	🔴	11,7%
Hardver	🟢	26,0%	🔴	9,6%
Jelszó	🟡	19,8%	🟢	22,3%
Iratmegsemmisítés	🟢	20,8%	🟢	29,3%
Adathalászat	🔴	3,1%	🟡	14,4%
Vírusvédelem	🟢	20,8%	🟡	16,0%
Közösségi média	🟡	13,5%	🟢	25,5%
Telefon és okos eszközök	🟡	15,6%	🔴	7,4%

31. táblázat: A kutatásba bevont hagyományos és gamifikációs módszerek hatékonysága az egyes vizsgált biztonságtudatossági ismeretek fejlesztésében közvetlenül a programot követően (forrás: saját szerkesztés)

Ami a kifejezetten fejlesztendő ismereteket illeti, ezen értékelés alapján elmondhatjuk, hogy az iratmegsemmisítést összességében mind a hagyományos, mind a gamifikációs módszerek hatékonyan fejlesztik, közösségi média esetében a hagyományos, míg a telefon és okos eszközök esetében pedig a játékosított megoldások értek el inkább jó eredményt.

A fentiek alapján elmondhatjuk, hogy rövid távon a gamifikációs módszerek valóban hatékonyabban képesek átadni a legtöbb ismeretet, összességében kevésbé hatékonyak viszont a korábban azonosított, 3 db kiemelten hiányos ismeret fejlesztésére.

Ugyanezt a táblázatot megbontottam konkrét oktatási módszerek szerint is, ennek az eredménye a következő lett (32. táblázat):

Módszer és tudatossági elem	Személyes oktatás	Online oktatás	E-Learning	Kampány-elemek	Szabaduló-szoba	Társasjáték
Tiszta asztal	22,0%	18,4%	7,1%	21,3%	18,8%	29,2%
Tiszta képernyő	2,0%	8,2%	4,8%	10,6%	0,0%	8,3%
Kulcsok, kártyák	16,0%	8,2%	16,7%	6,4%	22,9%	31,3%
Hardver	16,0%	12,2%	2,4%	6,4%	25,0%	27,1%
Jelszó	22,0%	24,5%	16,7%	25,5%	29,2%	10,4%
Iratmegsemmisítés	24,0%	32,7%	26,2%	34,0%	27,1%	14,6%
Adathalászat	10,0%	16,3%	16,7%	14,9%	0,0%	6,3%
Vírusvédelem	14,0%	20,4%	14,3%	14,9%	2,1%	39,6%
Közösségi média	30,0%	24,5%	26,2%	21,3%	18,8%	8,3%
Telefon és okos eszközök	2,0%	2,0%	11,9%	14,9%	29,2%	2,1%

32. táblázat: A kutatásba bevont biztonságtudatosság fejlesztési módszerek hatékonysága az egyes vizsgált biztonságtudatossági ismeretek fejlesztésében, közvetlenül a programot követően (forrás: saját szerkesztés)

Itt jól látszódik, hogy a szabadulószoba körülbelül ugyanolyan hatékonysági arányban szerepel, és a negatívumok között csak azon 3 ismeret emelkedik ki, melyet valóban kevésbé hangsúlyoz a játék: ezek a tiszta képernyő politika, az adathalászat és a vírusvédelem. Kiválóan fejlesztette viszont a leghiányosabb ismeretek kétharmadát.

Társasjáték esetében szélsőségesebbek az értékek, és azt mondhatjuk, hogy vagy nagyon hatékonyan, vagy nagyon kis mértékben fejleszti az egyes ismereteket: negatívan, vagy semlegesként szerepel az általánosan azonosított, leginkább hiányos 3 ismeret vonatkozásában. Az összes többi vizsgált hagyományos módszernél látjuk viszont, hogy maximum 1 zöld pöttyel, tehát kiemelkedő hatékonysággal rendelkeznek, az e-Learning pedig egyik ismeret esetében sem ért el ilyen eredményt.

Végül ezen szempontok alapján megnéztem az egy hónappal későbbi eredményeket is azon mintán, akik az utolsó kérdőívet is kitöltötték (194 válaszadó).

Itt összességében elmondható, hogy a gamifikációs elemek a korábban vizsgáltaknak megfelelően rosszabbul szerepeltek, és nem voltak képesek olyan hatékonyan előidézni a tanultakat, egyedül a tiszta asztal politika és a kulcsok, kártyák biztonságtudatos kezelése maradt meg kiemelkedően, a tiszta képernyő politika és az adathalászattal kapcsolatos ismeretek kivételével az összes többit csupán közepesen hatékonyan fejlesztették.

Hagyományos módszerek esetében elmondható, hogy hatékonyabbak voltak az ismeretek hosszútávú megjegyzése szempontjából, mert kifejezetten jó értéket értek el a tiszta asztal politika, jelszavak, iratmegsemmisítés és adathalászattal kapcsolatos ismeretek terén, és csak a hardver eszközökkel, valamint telefon és okos eszközökkel kapcsolatos ismereteket nem fejlesztették (33. táblázat).

Módszer és tudatossági elem	*Gamifikációs*	*Hagyományos*
Tiszta asztal	17%	24%
Tiszta képernyő	0%	3%
Kulcsok, kártyák	25%	10%
Hardver	10%	-7%
Jelszó	12%	26%
Iratmegsemmisítés	12%	24%
Adathalászat	-12%	20%
Vírusvédelem	2%	12%
Közösségi média	6%	12%
Okos eszközök	12%	-5%

33. táblázat: A kutatásba bevont hagyományos és gamifikációs módszerek hatékonysága az egyes vizsgált biztonságtudatossági ismeretek fejlesztésében, 1 hónappal a programot követően (forrás: saját szerkesztés)

Ebben az esetben is néztem egy bontást oktatási módszerek szerint. Az alábbi táblázat alapján jól látható, hogy az előadás jellegű oktatások, akár személyesen, de akár online kerültek megtartásra, a hosszútávú fejlesztés céljából a leghatékonyabbnak bizonyultak. Gamifikációs módszerek esetében pedig elmondható, hogy a szabadulószoba valamivel jobban teljesített az egy hónappal későbbi felmérés során, mint a társasjáték (34. táblázat).

Módszer és tudatossági elem	*Személyes oktatás*	*Online oktatás*	*E-Learning*	*Kampány-elemek*	*Szabaduló-szoba*	*Társasjáték*
Tiszta asztal	31%	31%	19%	15%	27%	8%
Tiszta képernyő	-15%	8%	-12%	31%	0%	0%
Kulcsok, kártyák	35%	-4%	4%	4%	15%	35%
Hardver	-31%	15%	0%	-12%	15%	4%
Jelszó	12%	35%	23%	35%	31%	-8%
Iratmegsemmisítés	35%	38%	8%	15%	15%	8%
Adathalászat	8%	42%	23%	8%	0%	-23%
Vírusvédelem	15%	23%	15%	-8%	-12%	15%
Közösségi média	23%	0%	23%	0%	8%	4%
Okos eszközök	0%	-8%	8%	-19%	19%	4%

34. táblázat: A kutatásba bevont biztonságtudatosság fejlesztési módszerek hatékonysága az egyes vizsgált biztonságtudatossági ismeretek fejlesztésében, 1 hónappal a programot követően (forrás: saját szerkesztés)

Fentiek alapján elmondható, hogy hosszútávon a hagyományos módszerek, azon belül is az előadás jellegű oktatások képesek a leginkább a biztonságtudatosság fokozására, a legtöbb vizsgált ismeret átadására, illetve ezek bizonyultak a leghatékonyabbnak a hiányos ismeretek bővítésében. A gamifikációs programelemek egy hónappal később

leginkább átlagos értéket értek el, a 3 kiemelten hiányzó ismeret vonatkozásában is egységesen átlag-eredményt produkáltak.

4.15.LEVONT KÖVETKEZTETÉSEK

Ebben a fejezetben elsődlegesen azt vizsgáltam meg, hogy a gamifikációs biztonságtudatosság-fejlesztő megoldások, mint legélvezetesebbnek bizonyuló programelemek, milyen hatékonysággal képesek a felhasználók biztonságtudatosságának fokozására.
A következőket állapítottam meg, és az alábbi következtetéseket vontam le:

- A vizsgált szervezetek munkavállalói által adott válaszok alapján a gamifikációs módszerek hazánkban még nem terjedtek el a biztonságtudatosságot fejlesztő módszerek között, viszont tekintve, hogy a vizsgáltak alapján a leginkább élvezetesebb programok, melyek hatékonyságra gyakorolt pozitív hatását a 3. fejezetben igazoltam, érdemes megfontolni alkalmazásukat a hazai szervezetek körében is.
- Vizsgálataim 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.
- Szintén alátámasztottam, hogy a felhasználók a programon való részvételt követően valóban inkább a gamifikációs lehetőségeket részesítenék előnyben, miszerint a játékosított módszerek alkalmazásának van igénye és létjogosultsága munkahelyi környezetben a biztonságtudatosság fejlesztése céljából.
- A válaszadók szektortól, szervezeti mérettől, korosztálytól és nemtől függetlenül ajánlják a gamifikációs módszerek alkalmazását, még azon résztvevők is, akik egyébként negatívan értékelték a programot felhasználói élmény szempontjából, így a játékosított programok bármely szervezet számára alkalmazható megoldást jelentenek.
- A felmérésem alapján a gamifikációs módszerek közvetlenül a programban való részvételt követően összességében legalább olyan jól képesek a biztonságtudatossági ismeretek átadására, azok számosságának növelése

szempontjából, mint az egyéb hagyományos oktatási formák, így alkalmazhatóak a biztonságtudatossági képzések során.

- Emellett azt is igazoltam, hogy a gamifikációs módszerek közvetlenül a programon való részvételt követően legalább olyan hatékonyan képesek a biztonságtudatossági ismeretek átadására, mint az egyéb hagyományos oktatási formák, illetve minimálisan több felhasználó ismereteit sikerül bővíteni a játékosítást alkalmazó megoldásokkal.
- Tekintve az eredmények során azonosított jelentős különbségeket az egyes gamifikációs módszerek között (állami szektorban a társasjáték, privát szférában pedig a szabadulószoba bizonyul hatékonyabbnak), kulcsfelhasználók bevonásával érdemes vizsgálni a különböző játékosított módszereket, és a szervezet számára legideálisabbat kiválasztani.
- Az általam alkalmazott számítási mód szerint a gamifikációs módszerek közvetlenül a programban való részvételt követően összességében legalább olyan hatékonyan képesek a biztonságtudatossági ismeretek átadására, azok számosságának növelésére, mint az egyéb hagyományos oktatási formák, illetve minimálisan több ismeretet képesek átadni a játékosítást alkalmazó megoldásokkal. A gamifikációs módszerek rövid távon való hatékony alkalmazhatóságát az általam készített klaszter elemzés is alátámasztotta.
- A vizsgálatom viszont hosszútávon azt bizonyította, hogy általánosságban az előadás jellegű, akár online vagy személyesen tartott programok fejlesztik a legtöbb felhasználó biztonságtudatossági ismereteit, kiegészítésként érdemes azonban alkalmazni gamifikációs lehetőségeket is, hiszen megbontva a módszereket az állami szférában a társasjáték, a privát szektorban pedig a szabadulószoba jelenthet hatékony kiegészítő megoldást. Ezen eredményeket az általam készített klaszter elemzés is alátámasztotta.
- A különböző távlatokon elért vizsgálati eredmények alapján érdemes megfontolni a biztonságtudatossági programok tervezése esetén a vegyes programelemek alkalmazását, és mind rövid, mind hosszútávon fejlesztő megoldásokat alkalmazni.
- Javasolt 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.

- Szintén továbbfejlesztési lehetőség lehet annak vizsgálata is, hogy a gyakorlatban ténylegesen hogyan alkalmazzák a tanultakat a felhasználók, az elméleti tudás hosszútávú felidézése és a gyakorlati alkalmazás között milyen összefüggés figyelhető meg.

Vizsgálatom igazolta azt a hipotézist, 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.

5. A BIZTONSÁGTUDATOSSÁGI SZABADULÓSZOBA ALKALMAZHATÓSÁGA A BIZTONSÁGTUDATOSSÁG FEJLESZTÉSÉRE

Az előző fejezetben igazoltam, hogy a gamifikációs módszereknek van létjogosultsága a biztonságtudatossági fejlesztések között és legalább ugyanolyan hatékonysággal képesek fejleszteni a munkavállalók biztonságtudatosságát, mint a hagyományos módszerek.
A disszertáció 3. fejezetében bemutatott kutatás egyik eleme az általam 2014-ben kifejlesztett biztonságtudatossági szabadulószoba volt, jelen fejezetben kifejezetten ennek alkalmazhatóságát, illetve hatékonyságát vizsgálom a felhasználók biztonságtudatossági fejlesztésének tükrében.

5.1. KAPCSOLÓDÓ 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 hipotézis igazolására szintén az első hipotézishez készített kutatást használtam fel, melynek során hat különböző, biztonságtudatosságot fejlesztő módszert, köztük az általam 2014-ben fejlesztett biztonságtudatossági szabadulószoba hatékonyságát vizsgáltam abból a szempontból, hogy melyiknek milyen hatása van a biztonságtudatossági ismeretek bővülésére (*átlagos új ismeretszám*), vagy a biztonságtudatos felhasználók számának növelésére (*legalább egy új ismeretet szerző résztvevő felhasználók aránya*).
A hipotézishez kapcsolódó új fejlesztés a saját fejlesztésű biztonságtudatossági szabadulószoba módszertanának kialakítása. (2014)

5.2. A BIZTONSÁGTUDATOSSÁGI SZABADULÓSZOBA CÉLJA

A biztonságtudatossági szabaduló szoba lényege, hogy a felhasználók interaktív, játékos feladat formájában teszteljék biztonságtudatosságukat, illetve bővítsék ismereteiket az információbiztonság terén. A hagyományos játékkal szemben itt azonban a hangsúly nem a szobából való kijutáson, hanem épp az ellenkezőjén, a „támadóként" vagy segítő szándékú kollégaként való bejutáson van – méghozzá nem csak az irodába, hanem a számítógépbe is. A

játék során egy fiktív felhasználó irodája kerül szimulálásra és a főbb biztonságtudatossági hiányosságok kerülnek bemutatásra, melyeket a résztvevőknek azonosítaniuk kell ahhoz, hogy sikeresen eljussanak a megoldáshoz, mely a számítógépbe való bejelentkezést követően egy bizalmas dokumentum megnyitása lesz.

A saját fejlesztésű biztonságtudatossági szabaduló szoba ötletét a Magyarországon népszerű szabaduló szobák alkották. A fejlesztés idejében (2014) nem állt rendelkezésemre olyan forrás, szakirodalom, mely hasonló megoldás kialakítását mutatta be, így a saját módszertant a hagyományos szabadulószobák alapján alkottam meg.

Ugyan vannak olyan kezdeményezések, mint például a Beguin és szerzőtársai (2019) által definiált védekező szcenáriójú szabadulószobák, ahol a játékosoknak hibákat, sebezhetőségeket kell javítaniuk, hogy pontokat szerezzenek, ezt a lehetőséget én nem tartottam annyira izgalmasnak. Ehelyett egy olyan megoldásban gondolkodtam, miszerint két különböző csapat játszana ugyanazon szobában, az egyikük a klasszikus „támadó" csapat lenne, a másikuk pedig az ő játékuk előtt alakítaná ki szabadulószobát, tehát gyakori biztonságtudatossági hiányosságokat kellene összeszedniük és implementálniuk, melyet a következő csapat „normál módon" felfed. Ennek lehetőségét azonban egyelőre elvetettem, később viszont érdekes fejlesztés lehet.

Az általam fejlesztett biztonságtudatossági szabadulószobában a feladatok teljes mértékben szervezetre szabhatóak, nem csak a szoba kialakításában, illetve az alkalmazott design-elemekben, hanem a végrehajtandó feladatokban is, előtérbe lehet helyezni a korábbi felmérések során azonosított problémákat, hiányos ismereteket. Ez a szakirodalom feltárás során azonosított szabadulószobák esetében is általános jellemző.

A biztonságtudatossági szabadulószobában végrehajtandó feladatok mindegyike valamely információbiztonsági ismerethez kötődik és tipikus hiányosságokra világít rá, fontos szabályokra hívja fel a figyelmet, például miért ne rejtsük a kulcsunkat a virágcserépe, miért ne írjuk fel post-it-ekre a jelszavunkat, egyáltalán miért ne válasszunk egyszerű jelszót, de kitekinthetünk a közösségi média, mobilalkalmazások, sőt akár az adathalászat világába is.

Az első és legfontosabb különbség egy hagyományos és egy biztonságtudatossági szabadulószoba között természetesen a forgatókönyv, illetve a céltéma jellege. A klasszikus szabadulószobákban ez bármi lehet, valóság és fikció széles skálája megjelenik, be lehetünk zárva például egy kalóz barlangjába, tudós irodájába, de akár egy erőműbe is. Ezek a forgatókönyvek ugyan érdekesek, de általában nem reálisak, így nem célszerű ezekre építeni biztonságtudatossági elemeket. Ezt publikációjukban Schneider és Zanwar (2020) is megerősítik. Biztonságtudatossági szabadulószoba esetében sokkal hitelesebb, ha a szoba egy

titkárnő, menedzser, IT üzemeltető, programozó, vagy bármilyen más érdekes szerepkört betöltő “kolléga” irodája, igazodva a szervezethez. Például, amennyiben egy vállalatnál az IT üzemeltetési terület munkatársai számára szeretnénk ilyen programot rendezni, a legérdekfeszítőbb és hasznosabb az lesz, ha egy fiktív rendszergazda „kolléga” irodája lesz a színtere, és ahhoz kapcsolódik a kerettörténet is. Minél hasonlóbb a környezet és a szituáció, annál élethűbb és emlékezetesebb lesz a játék – és természetesen a tapasztalat.

Információbiztonsági tanácsadóként specialitásom a Social Engineering auditok és biztonságtudatossági képzések megvalósítása, az ezek során szerzett tapasztalatok remekül beépíthetőek a biztonságtudatossági szabadulószoba forgatókönyvekbe. Ezek keretein belül egyrészt jól lehet azonosítani a tipikus biztonságtudatossági hiányosságokat, jellemző rossz szokásokat, másrészt az oktatásokon feltett kérdések, biztonságtudatossági kampányokra, programokra tett visszajelzések is megalapozták egy érdekes és szokatlan program létrehozásának szükségességét, sokan jelezték ugyanis, hogy a hagyományos megközelítés már nem elég. Tapasztalataim szerint a felhasználók akkor érzik át az információbiztonság fontosságát, ha már megtörtént a baj (például incidens áldozatává válnak), illetve látják egy kockázat bekövetkezését – ennek szimulálására pedig a biztonságtudatossági szabadulószoba játékos környezete is alkalmas. Ezen meglátásomat a szakirodalom feltárás során Hill és szerzőtársai (2020) is megerősítették, és előnyként tüntették fel, hogy a gamifikációs módszerek, így a szabadulószobák is lehetővé teszik a felhasználók számára a lehetőségek kipróbálását, olyan környezetet teremtenek, ahol következmények nélkül játszanak le különböző szcenáriókat, forgatókönyveket, és próbálhatnak ki különböző megoldásokat egy játékon belüli környezetben.

Az alábbi alfejezetekben bemutatom, hogy hogyan került kidolgozásra az általam fejlesztett biztonságtudatossági szabadulószoba módszertana, illetve hogyan lehet megvalósítani az ilyen jellegű programokat.

5.3. A SAJÁT FEJLESZTÉSŰ SZABADULÓSZOBA BEMUTATÁSA

A klasszikus szabadulószobák már 2014-ben is nagyon népszerűek voltak Magyarországon, ez adta a biztonságtudatossági szabadulószoba fejlesztésének alapötletét. Hiszen, ha olyan sokan hajlandóak viszonylag magas összeget kifizetni egy órás csapatjátékért, a munkahelyeken vagy csapatépítők során ingyenesen biztosított biztonságtudatossági változat a munkavállalók és munkáltatók számára is érdekes lehet. Emellett ahogyan a szakirodalom feltárás során is

bemutattam, a játékosítás vállalati környezetben is egyre népszerűbbé vált napjainkra, sőt megjelentek már kifejezetten biztonságtudatossági játékok, szabadulószobák is.
Mindezen okokból kifolyólag döntöttem úgy, hogy megvizsgálom annak lehetőségét, lehet-e egy biztonságtudatossági ismeretek mérésére-fejlesztésére szolgáló adaptációt készíteni a játékból.

5.3.1. A JÁTÉK KIALAKÍTÁSA

Első lépésként természetesen megvizsgáltam, hogy a klasszikus szabadulószobák hogyan működnek, és azt egy biztonságtudatossági változatban hogyan lehetne megvalósítani. Ehhez elsősorban hagyományos szabadulószobákat látogattam különböző témákban (kincskereső, kalóz, gyilkos, tudós, szerelmespár, atomerőmű, stb.) és megvizsgáltam, hogy mi szükséges egyáltalán egy szabadulószoba kialakításához, illetve milyen különbségekkel kell szembenézni egy biztonságtudatossági szabadulószoba tervezése esetén.
A vizsgálati szempontok és eredmények, valamint az azok átalakításából származó, biztonságtudatossági szabadulószobával kapcsolatos elvárások az alábbi alpontokban kerülnek bemutatásra.

5.3.1.1. A játék célja

A biztonságtudatossági szabadulószoba edukációs céllal került létrehozásra, annak érdekében, hogy a felhasználók megtapasztalják a biztonságtudatos magatartás szükségét, azonosítsák a legfontosabb biztonságtudatossági ismereteket és a gyakorlatban is alkalmazzák a tanultakat.
Klasszikus szabadulószobák esetén a cél a szórakozás, a tényleges kijutás egy zárt szobából, kulcs vagy kód megtalálásával. A játékosok akkor teljesítik a küldetést, ha a megadott időkereten belül ténylegesen el tudják hagyni a szobát. Emellett később kialakultak olyan verziók is, melyek során például egy visszaszámláló órát kell megállítani, vagy valamit megtalálni.
A klasszikus kijutást egy biztonságtudatossági szabadulószoba esetén életszerűtlennek tartottam, helyette a fókuszt a szervezetnél leginkább védendő értékek, nevezetesen fájlok megvédésére, illetve ezen védelem hiányának felfedezésére helyeztem, így a biztonságtudatossági szabadulószobából esetemben egy megszerzendő fájl megnyitása jelenti a „szabadulást”, az időnyomást pedig egy hamarosan kezdődő megbeszélés kerettörténete adja.

5.3.1.2. A játékosok szerepe

Hagyományos szabadulószobák esetében nagyon vegyes, tematika függő, hogy éppen kinek a bőrébe bújnak a résztvevők. A lehetőségeket én a következő 4 kategóriába soroltam:

- **menekülők**: akiknek azért fontos a kijutás, mert az életüket veszélyezteti valami, például robban a helyiség, amennyiben nem jutnak ki. Ők nem más érdekeit nézik, és sem támadó, sem segítő szerepben nem lépnek fel.
- **támadók**: akiknek saját érdeke motiválja a kijutást, de nem menekülés céllal, hanem például, hogy megszerezzenek valamit, ellopjanak valamit, és a tett helyszínéről kell távozniuk, sőt nem is feltétlenül kell távozniuk, az is lehet, hogy pont a bejutás vagy megérkezés a cél.
- **segítők**: akiknek más érdeke motiválja a kijutást, de nem kimenekítés céllal, hanem például tipikusan nyomozás végrehajtása, bizonyítékok gyűjtése miatt.
- **általános**: végül megállapítottam egy olyan kategóriát is, melyekben a játékosoknak célja ugyan a kijutás vagy bejutás, de nem jellemző a fenti három motiváció egyike sem, a cél megtalálni valamilyen jutalmat, például a játék végén kínált süteményt vagy ajándékot.

Biztonságtudatossági szabadulószoba esetében kizártam azt, hogy a játékosok életét veszélyeztesse valami, meneküljenek, és azért legyen szükségük egy adott fájl megszerzésére. Az általános megközelítést szintén nem tartottam olyan izgalmasnak (bár lehetne olyan megoldás, melynek motivációs nyereménye valamilyen apró, biztonságtudatossághoz kapcsolódó ajándék, jelszókódoló, kameratakaró lehetne). Első körben a legéletszerűbb megoldásnak a támadói szemszög bizonyult. Ez később kiegészítésre, finomításra került „segítő” szerep bevezetésével, attól függően, hogy az adott szervezetnél preferálták-e, hogy a munkavállalók egy potenciális támadót személyesítsenek meg, vagy helyette olyan munkavállalókká váljanak, akik szigorúan információbiztonsági vezetői engedéllyel, egy fél órán belül kezdődő fontos megbeszélésük miatt tárják fel fiktív kollégájuk biztonságtudatossági hiányosságait, a fájl tartalmának megismerése végett és a kolléga védelme érdekében.

Személyes tapasztalatok alapján elmondhatom, hogy az utóbbi időben mind a résztvevői, mind a munkáltatói oldal a segítő szerepet preferálta.

5.3.1.3. A játék célközönsége

A klasszikus szabadulószobák több korosztályt is megcéloznak, vannak gyermekeknek készült verziók, de elsősorban mégis felnőtteknek szóló, vagy felnőttek számára is élvezhető forgatókönyvvel készülnek. A pontos célközönség erősen tematika függő.

A biztonságtudatossági szabadulószoba, lévén munkahelyi környezetbe készült, mint oktatóeszköz, elsősorban felnőtteket, azon belül is főként irodai munkavállalókat céloz meg.

Ettől függetlenül a tapasztalatok alapján a játékok hasznosak és élvezetesek alacsonyabb korosztály, illetve nem irodai munkát végző résztvevők számára is.

5.3.1.4. Játékosok száma

A hagyományos szabadulószobák általában 2-6 fő részvételére optimalizáltak. Ez egyrészt a feladatok számosságából és jellegéből is adódik (például lehet olyan ügyességi feladat, melynek megoldásához legalább 2 fő részvétele szükséges), másrészt a helyszín méretéből fakadóan maximalizálni kell a létszámot. A biztonságtudatossági szabadulószoba résztvevőinek számát én is ezekhez igazítottam, viszont teljesen más szempontok miatt. Gyakorlatilag a biztonságtudatossági szabadulószoba egyedül is megoldható feladat lenne, viszont az időkeret és a feladatok számossága követeli meg a legalább 2 fő részvételét. A létszám maximumát itt nem elsődlegesen a helyszín befogadó képessége (főleg, ha több „iroda" is egybenyitható) határozta meg, hanem hogy minden játékos kivegye a részét a „tanulásból", illetve ne akadályozzák egymást a feladatok végrehajtása során. Így a keretek ebben az esetben is 2-6 fő közé tehetőek, a gyakorlatban a program meghirdetésnél azonban 3-5 főre javaslom, és a forgatókönyveket is ehhez optimalizálom.

Később felmerült igények alapján munkahelyi környezetben az egyidejű játékosszám növelésére és több felhasználó egyidejű fogadására a párhuzamosítás lehetőségével szoktam élni, melynek köszönhetően több játékoscsoport dolgozhat párhuzamosan, egy idősávban ugyanolyan vagy különböző forgatókönyvű szobákban, egymással versenyezve, vagy akár két szoba összevezetésével (például igazgató és titkárnője akkor nyernek, ha mindkét szobában megszerzik a „szabaduláshoz" szükséges információt).

5.3.1.5. A játék időkerete

A klasszikus szabadulószobák időkerete általában minimum 60 perc, ettől tematika függvényében inkább csak fölfelé szoktak eltérni.

Figyelembe véve a munkahelyi környezetet, a biztonságtudatossági szabadulószobában a játékidőt csökkentettem, hogy jobban beleilleszthető legyen a munkanapba, illetve olyan szempontból is reálisabb legyen, hogy rávilágítson, egy támadó számára viszonylag rövid idő is elég lehet a kártokozásra, információszerzésre. Átlagosan 30 perces játékok kerültek kialakításra, de természetesen szervezeti igények alapján ez módosítható volt 15-60 perc között bármilyen időkeretre a forgatókönyv és feladatszám módosításával.

5.3.1.6. Helyszín kialakítása

A klasszikus szabadulószobák állandó, fix helyen működnek, az adott témakörhöz kialakított, részletesen berendezett szobákkal. Egy szabadulószoba akár több helyiségből állhat, például

egy titkos átjáró felfedezésével, másik ajtó kulcsának megtalálásával. Később megjelentek mobil kezdeményezések is, melyek csapatépítőkre, családi napokra, egyéb rendezvényekre kitelepíthetőek.

Bár többen jelezték, hogy hasznos lenne a klasszikus mintára egy mindig üzemelő, fix helyen működtetett biztonságtudatossági szabadulószoba, ennek megvalósítását alacsonyabb prioritásra helyeztem az erőforrás igénye miatt (kellően általános forgatókönyv, terembérlet, munkaidőn kívüli rendelkezésre állás, stb.), és a fő célra fókuszáltam, vagyis a munkavállalók oktatására az új eszközzel. Ebből kifolyólag a megoldás a célcsoportok munkahelyén, munkaidőben kerül alkalmazásra, és tekintve a változó szervezeti környezetet, helyszínéül általában tárgyaló vagy üres iroda ad otthont, minimálisan szükséges pluszban biztosított elemekkel (például zárható fiókos szekrény), illetve a forgatókönyv szerint szükséges kellékekkel, melyet vagy én, mint szervező, vagy előzetes egyeztetés alapján a munkáltató biztosít (például vállalati laptop, telefon, stb.). Több szoba egymásra építésének lehetőségét párhuzamos, illetve összevezetett játékokhoz használtam fel (lásd. 5.2.1.4 pont), az egyes biztonságtudatossági szabadulószobák forgatókönyvének összetettsége nem indokolja külön helyiségek bevezetését.

Az alábbi képen egy általam berendezett biztonságtudatossági szabadulószoba látható, mely egyben demonstrálja azt is, hogy egy ilyen jellegű program viszonylag kis hely- és erőforrás ráfordítással megvalósítható – az 1. képen a munkahelyi erőforrás pusztán a szoba, az asztal és a forgószék.

1. kép: Egy berendezett biztonságtudatossági szabadulószoba (forrás: saját fénykép)

5.3.1.7. Feladatok típusa

A klasszikus szabadulószobákban főképp logikai, rejtvény, ügyességi feladatokkal találkozunk, nem lexikális tudásra vagy speciális ismeretre alapozó feladványok szerepelnek a forgatókönyvükben.

A biztonságtudatossági szabadulószoba esetében az oktatási célok miatt kizárólag általános, vagy forgatókönyv függvényében a szervezetnél elvárt biztonságtudatossági ismeretekre alapozó, azok hiányát felfedő, élethű feladatok szerepelnek, melyekhez azonban külön előzetes oktatás nem szükséges (de előnyt jelenthet). Mindezek értelmében nem tekintem „igazi" és hatékony biztonságtudatossági szabadulószobának az olyan verziókat, melyek a klasszikus szabadulószobák elemeit nagymértékben ötvözik információbiztonsági tematikával (például ügyességi feladatként kell kihalászni egy pendrive-ot, keresztrejtvényt kell megoldani információbiztonsági ismeretekről, stb.).

5.3.1.8. Játékosok felügyelete, instruktori feladatok

A hagyományos szabadulószobák jellemzője, hogy az instruktorok a játék elején elmondanak minden szükséges ismeretet, majd ezt követően kívülről, kamerán keresztül figyelik a játékosokat, és elakadás esetén segítséget nyújtanak hangszórókon keresztül. Az is előfordul, hogy a játékosoknak van kérdezési lehetősége, általában előre meghatározott kérdés-számmal. Biztonságtudatossági szabadulószoba esetében én a személyesen, a résztvevőkkel egy játéktérben való tartózkodást preferálom az alábbi okokból kifolyólag:

- egyrészt a változó környezetből adódó technikai nehézségek ezáltal elkerülhetőek (pl. kamerák telepítése, nincs Internet, stb.),
- másrészt így könnyebben felügyelhetőek a kamerán nehezen ellenőrizhető dolgok, például PIN-kód beírás, szükségtelen vagy tiltott alkalmazások használata,
- végül így elkerülhető, illetve enyhíthető az egyébként is gyakori tévhit, mely szerint „az információbiztonsági terület megfigyel minket".

A gyakorlati tapasztalatok azt mutatják, hogy a játékosokat nem zavarja az instruktor bent tartózkodása, bizonyos esetben a személyes felügyelet még megnyugtató is (például felhasználói ellenérzés a folytatott cselekedettel szemben, a fiktív munkatárs holmijai között való turkálás, stb.), ráadásul elmondható, hogy a játékokat követően az információbiztonsági terület ismertsége, valamint a bizalom jelentős mértékben nőtt a munkavállalókban.

A biztonságtudatossági szabadulószobával kapcsolatos instruktori feladatok fontos különbsége, hogy nem szükséges, sőt nem javasolt minden szabály, ismeret átadása. Ez egyrészt rontja az élményt (tudják, hogy találni kell például egy telefont), másrészt a tapasztalat alapján úgyis

elfelejtik a kapcsolódó előírást, mire oda jutnak, hogy alkalmazni kell (például, hogy 5 sikertelen kód megadási kísérlet után 1 percre kizárják magukat). Azon eszközökhöz kapcsolódó szabályok, melyek az adott eszköz megtalálását követően lesznek relevánsak, elég, ha a felügyelet során, a megfelelő időben kerülnek átadásra (például telefon PIN kódjával kapcsolatos korlátozások).

5.3.1.9. Számítógép használat

A klasszikus szabadulószobák esetében a vizsgált időszakban (2013-2014) kevésbé jellemző a számítógép használat, nem szükséges elem, ugyan később ez is megjelent az újabb forgatókönyvek eszköztárában.

A biztonságtudatossági szabadulószoba elengedhetetlen része a számítógép, sőt mobileszköz használat, így jelentős különbséget jelent a hagyományos szabadulószobákhoz képest, a feladatok 50%-a biztos, hogy ezen eszközökhöz kell, hogy kapcsolódjon. Ezen feladatok tervezése során komoly kérdés volt, hogy az alkalmazott eszközöket mennyire kell „felhasználó-biztossá" tenni, vagyis úgy kialakítani, beállítani, hogy a játékosok ne tudjanak velük visszaélni, ne tudják azt elrontani, illetve ne kösse le fölöslegesen a figyelmüket. Arra a megállapításra jutottam, hogy mivel fontosabb több, szervezetre szabható forgatókönyvű szabadulószoba kialakítása, mint egy „dobozos" szabadulószoba megalkotása, az említett kockázatokat csak két módon csökkentettem:

- egyrészt a szükségtelen funkciók, alkalmazások eltávolításával vagy elrejtésével (pl. beállítások menü),
- másrészt az instruktori feladatokba építettem a helyes használat ellenőrzését (mind játék közben, mind pedig azt követően).

További kockázatcsökkentés céljából saját tapasztalat alapján érdemes a játékok során minden informatikai eszközből egy tartalékot biztosítani (laptop esetében plusz egy felhasználói fiókot előre létrehozni ugyanazon forgatókönyvhöz).

5.3.1.10. Értékelés, jutalom

A klasszikus szabadulószobák végén a résztvevők kiszabadulást követően összeállnak egy csoportképre, melyen az időeredményüket tudják kezükben tartani egy felíró táblán, vagy számlapokból kirakva. A fényképek később a szabadulószoba szolgáltatójának honlapján vagy közösségi média felületein kerülnek publikálásra, természetesen előzetes hozzájárulás esetén.

A biztonságtudatossági szabadulószobánál ugyanezen módszert követve szintén alkalmazható az időeredménnyel való fénykép készítése, illetve annak e-mail-ben vagy intranetes felületen való publikálása. Bár a játékosok sok esetben szeretnek magukról fotót készíteni a

szabadulószobában talált eszközökkel (mobiltelefon szelfi, laptop kamera), ezáltal jó ötlet lehetne, hogy a cél egy olyan fájl megnyitása legyen, mely automatikusan mutatja az elért időeredményt, és fényképet is készít a megnyitás pillanatában a csoportról - a tapasztalat viszont azt mutatja, hogy nem feltétlenül növelné annyira a felhasználói élményt, a csoportkép készítése során is több felvétel készítését kérik leginkább.

Emellett, ahogyan a hagyományos szabadulószobák némelyikének a végén is kaphatnak a sikeres teljesítők jutalmat, úgy erre a biztonságtudatossági szabadulószobánál is van lehetőségünk, például kameratakaró, jelszókódoló, egyéb apró ajándék osztásával. A tapasztalat azt mutatja, hogy bár a fényképeknek is nagyon örülnek a résztvevők, erre is lenne azonban igény.

Ami lényeges különbség még a klasszikus módszerektől az, hogy a biztonságtudatossági szabadulószoba után – amennyiben külön időkeret biztosítható – lehet értékelni a játék megoldását, az instruktor összefoglalja, hogy milyen tapasztalatai vannak, és közösen át lehet beszélni, hogy melyek voltak a legfontosabb biztonságtudatossági ismeretek. A tapasztalatok szintén azt mutatják, hogy a felhasználók erre is nyitottak, szívesen beszélgetnek a játékot követően, és osztják meg saját hibáikat, vagy akár jó gyakorlataikat.

5.3.1.11. Továbbfejlesztés – időbüntetés

A biztonságtudatossági szabadulószoba feladatait 2016-ban továbbfejlesztettem, és megjelentek olyan elemek is, melyek során a játékosoknak nem csak biztonságtudatossági hiányosságokat kellett azonosítaniuk, hanem nekik is biztonságtudatosan kellett végezniük tevékenységüket a játék során. Ennek keretein belül bekerültek olyan elemek a játékba, mint elhagyott adathordozó csatlakoztatásának a veszélyei, e-mail-ben érkező adathalász megkeresések és kártékony kód terjesztési módszerek. Amennyiben a játékosok megnyitják ezeket a gyanús tartalmakat, 5 perc időbüntetésben részesülnek „vírusirtás” címen, mely érték természetesen csak a végeredményükhöz kerül hozzáadásra a játék végén.

5.3.2. A JÁTÉK SORÁN FEJLESZTENDŐ ISMERETEK, TÉMAKÖRÖK

Az előző pontban bemutattam, hogy a hagyományos szabadulószobák mintájára hogyan lehetett egy biztonságtudatossági adaptációt készíteni. Ebben a pontban azt gyűjtöttem össze, hogy milyen ismeretek fejlesztésére alkalmazható a játék.

Tekintve, hogy a biztonságtudatossági szabadulószoba forgatókönyve optimális esetben mindig szervezetre szabott, így gyakorlatilag bármilyen információbiztonsági ismeretet beépíthetünk. A leggyakoribb elemeket az alábbi három kategóriában mutatom be, de természetesen ezek irányadó jellegűek, nem tartalmazzák az összes lehetséges ismeretet és kontrollt.

5.3.2.1. Általános ismeretek

A biztonságtudatossági szabadulószoba jellemzően, de nem kizárólagosan az alábbi ismeretek átadására fókuszál:

- fizikai biztonság, kulcsok és belépőkártyák helyes kezelése
- tiszta asztal, tiszta képernyő politika betartása
- mobil eszközök fizikai biztonsága (notebook, mobiltelefon, adathordozók)
- helyes jelszó és PIN kód választás, tárolás
- alkalmazások biztonságtudatos használata (mind notebook-on, mind okostelefonon)
- titkosított adathordozók, titkosítási lehetőségek
- információmegosztás a közösségi médiában
- dokumentumok biztonságos megsemmisítése (mind papír alapon, mind elektronikusan)
- nyomtatás felügyelete
- adathalászat és kártékony kód terjesztés (elsősorban időbüntetéses verziók esetén)

A program előnye, hogy a fenti ismeretek tetszőleges súllyal szerepelhetnek, nagyobb hangsúlyt fektetve a legfontosabb átadandó ismeretekre az 5.2.2.2 és az 5.2.2.3 alpontokban rögzítettek szerint.

5.3.2.2. Szervezetspecifikus szabályok, eszközök

A biztonságtudatossági szabadulószoba lehetővé teszi, hogy rávilágítsunk új, vagy kérdéses szervezetspecifikus szabályokra, valamint bemutassunk újonnan bevezetett, vagy kevesek által ismert, az információbiztonsághoz kapcsolódó eszközöket. Így például a játékba be lehet építeni egy vonatkozó szabályzat vagy eljárás alkalmazását (a feladat megoldásához el kell olvasni a rendelkezésre bocsátott kivonatot), a 2016-2019 közötti felmérésben is bemutatott, szervezeti szinten bevezetett titkosított pendrive használatát, vagy ugyanezen elven a vállalati jelszószéf használatát is lehet promotálni, illetve tanítani a résztvevőknek.

5.3.2.3. Szervezetspecifikus problémák és kockázatok

Ahogyan az 5.1 alfejezet bevezetőjében is írtam, illetve a későbbi alpontokban részletesen is kifejtem, a biztonságtudatossági szabadulószobába saját, általános Social Engineering auditok tapasztalatai, oktatások kérdései épülnek be elsődlegesen. Ezeket a felméréseket szervezeti szinten is meg lehet valósítani, illetve ezáltal a szervezetspecifikus biztonságtudatossági hiányosságokat, gyakori problémákat és kapcsolódó humán kockázatokat is hatékonyan be lehet mutatni és fejleszteni a játék során, rávilágítva a problémákra és ösztönözve a felhasználókat a helytelen magatartás vagy rossz gyakorlat mellőzésére. Ilyen előzetes felmérések lehetnek a teljes vagy részleges Social Engineering auditok, helyszíni bejárások és

hulladék átvizsgálások, felhasználói kérdőívek vagy kulcsfelhasználókkal folytatott interjúk, valamint akár biztonsági eseményekből levont következtetések.

5.3.3. A BIZTONSÁGTUDATOSSÁGI SZABADULÓSZOBA PROGRAM MEGVALÓSÍTÁSA SZERVEZETI KÖRNYEZETBEN (MÓDSZERTAN)

A biztonságtudatossági szabadulószoba program szervezeten belüli lebonyolításának lépéseit a 7. ábra szemlélteti, mely a 2019-ben publikált (Oroszi, 2019) négy lépéses megközelítés kiegészített változata:

7. ábra: A biztonságtudatossági szabadulószoba kialakításának és lebonyolításának lépései (forrás: saját szerkesztés)

Az alábbiakban ezen lépések mentén mutatom be a biztonságtudatossági szabadulószoba program megszervezését és lebonyolítását.

5.3.3.1. Felmérés

Amennyiben szabadulószobát tervezünk megvalósítani, ha van lehetőségünk, első lépésként próbáljuk meg azonosítani a munkatársak jelenlegi információbiztonsági ismereteit, hiányosságait, rossz szokásait, hogy az 5.2.2.3 pont szerint példaként be tudjuk építeni a játékba és a résztvevők magukra ismerjenek (például, ha az a szokás, hogy a jelszavakat a naptár végében vezetik a kollégák, a játék fiktív munkatársa is ott tegye, így megtapasztalható lesz, hogy erre sajnos könnyen rá lehet jönni). A felmérést megtehetjük Social Engineering audit

vagy bejárás keretein belül, de ha erre nincsen időnk vagy lehetőségünk, felhasználói kérdőívet töltethetünk ki, esetleg interjút is készíthetünk néhány kiválasztott kollégával, kulcsfelhasználókkal, hogy szerintük melyek a leggyakoribb és legjellemzőbb rossz szokások a munkatársak körében. (Kulcsfelhasználónak érdemes olyan munkatársakat kiválasztani, akik bár nem információbiztonsági területen dolgoznak, de nyitottak, érzékenyebbek a témára és egyfajta példaképek lehetnek a többi munkatárs szemében.)

Emellett azonosíthatjuk a szervezetnél előírt, felhasználókra vonatkozó szabályokat, új vagy kevésbé ismert eszközöket, biztonsági eseményeket és incidenseket, vagy a biztonsági területhez érkezett leggyakoribb megkereséseket.

Amennyiben erre nincsen lehetőségünk, általános forgatókönyvvel dolgozhatunk.

5.3.3.2. Forgatókönyv

Az opcionális felméréseket követően el kell készíteni a szabadulószoba forgatókönyvét. Természetesen alkalmazhatunk általános forgatókönyvet, általános rossz példákkal (feladatokkal) is, azonban a program akkor a legizgalmasabb és hatékonyabb, ha a résztvevők környezetére épül, hiszen általános esetben lehet, hogy nem is minden feladat lesz releváns (például egyáltalán nem használnak jelszószéf megoldást a vállalatnál, holott a játékban szerepel). Feladatok számosságát tekintve 6-8 biztonságtudatossági ismeret feltárásában érdemes gondolkodnunk egy 30 perces játék esetén, ezeket a következőhöz hasonló táblázatban érdemes felvázolni (35. táblázat):

Sorszám	Feladat	Felhasználás	Fejlesztett ismeret
1.	*Szekrény kulcsának megtalálása a virágcserépben.*	*Szekrény kinyitása.*	*Kulcsok kezelése*
2.	*Szekrényben notesz, melyben fel vannak írva különböző jelszavak.*	*Számítógépbe való bejelentkezés.*	*Jelszóhasználat*
...	...	...	...

35. táblázat: Biztonságtudatossági szabadulószoba forgatókönyv segédlet (forrás: saját szerkesztés)

Természetesen a felvázolt sorszám nem azt jelenti, hogy a játékosok csak ebben a sorrendben tudják megoldani a feladatot, gyakran előfordul, hogy későbbi lépések hamarabb megoldásra kerülnek, de ebben az esetben előre tudtak dolgozni.

Ha megvan a forgatókönyvünk, kitalált karakterünk és a hiányosságokat bemutató feladatok váza, akkor érdemes még annyiban is vállalatra szabni, hogy azonosítjuk, milyen eszközöket

használnak a szervezetnél és azokat építjük be, hiszen a különböző operációs rendszerek, szokatlan alkalmazások zavaróak, sőt akár akadályozóak is lehetnek a játék során (például, ha a szervezetnél Windows környezetben dolgoznak a felhasználók, egy Macbook nem lesz a legjobb választás a programhoz).
Ezen a téren amire érdemes figyelni:

- operációs rendszer
- mobil eszközök (iOS vagy Android)
- titkosítási megoldások
- jelszószéf megoldás
- támogatott böngésző

Ezt követően lehet létrehozni a fiktív felhasználót és előkészíteni a környezetét a virtuális térben is, például létrehozni a fiókját a választott közösségi oldalon is. Fontos, hogy ha mindennel elkészültünk néhány kulcsfelhasználót kérjünk meg a játék tesztelésére, hogy elegendő-e a keretnek szánt idő, illetve megfelelő nehézségűek-e a feladatok, kell-e esetleg valamelyik lépésen változtatni, kiegészítő segítséggel készülni.
Amennyiben az "éles" játékra nagyon sok jelentkező van, és viszonylag kevés az időnk a program végrehajtására (például 1 munkanapon kellene több, mint 100 játékos számára biztosítani a lehetőséget), alkalmazhatunk párhuzamosítást ugyanazon vagy különböző forgatókönyvvel. Ebben az esetben egy időben két, akár egymás melletti helyszínen is játszhatnak a csapatok, sőt meg lehet azt is valósítani, hogy az egyik játék megoldása szükséges a másik csoport számára is (például a titkárnő irodájában a megszerzendő fájl tartalmazza a főnök gépén tárolt titkosított dokumentum jelszavát). Az egyforma forgatókönyvű párhuzamosításnak pedig előnye lehet, hogy a csapatok így egyidőben is tudnak versenyezni egymással. Természetesen ebben az esetben duplikálni kell az eszközöket, és nem árt, ha két instruktorunk is van.

5.3.3.3. Tesztelés

A forgatókönyv véglegesítése előtt elengedhetetlen annak szakértői tesztelése, mely nem azonos a kulcsfelhasználói teszteléssel, mely javasolt ugyan, de szükség esetén elhagyható. A szakértői teszt kiterjed mind a logikai felépítésre, mind az elkészített felhasználók, eszközök, információk elérhetőségének és megfelelő működésének vizsgálatára. Itt kell figyelembe venni azt is, hogy minden olyan funkció letiltásra, és minden olyan információ eltávolításra kerüljön, mely a játékosokat félrevezeti, vagy a feladat kijátszását segíti.

A forgatókönyv működésének tesztelését követően érdemes a kulcsfelhasználókkal is előzetesen kipróbáltatni a játékot, és észrevételeiket beépíteni a forgatókönyvbe (például, ha valamilyen feladat túl nehéz, vagy nagyobb mértékű segítséget igényel). Ezen teszt szintén nagyon hasznos az időkeret tarthatóságának ellenőrzésére is.

5.3.3.4. Regisztráció

Miután megvan a végleges forgatókönyvünk és előkészített eszközeink, elkezdődhet a regisztrációs folyamat. A regisztrációs ívet feltehetjük virtuálisan egy online felületre, intranetre, de helyszíni regisztrációt is alkalmazhatunk papír alapon. Nagyon fontos, hogy bármelyiket is válasszuk, előzetesen (legalább két héttel az esemény előtt) kommunikáljuk ki a programot a munkatársak felé, hogy időben be tudják tervezni azt a napi munkavégzésbe. Az előzetesen regisztráló felhasználóknak célszerű naptárbejegyzés (meghívó) küldése, illetve az esemény előtti emlékeztető e-mail küldése.

5.3.3.5. Instrukciók

Javasolt, hogy a forgatókönyvet és játékszabályokat csak közvetlenül a játék elején ossza meg az instruktor a résztvevőkkel, ne kommunikáljuk ki előzetesen. Így egyrészt a lelkesebb résztvevőknek nincsen lehetősége „előre dolgozni”, másrészt így nem fogják elfelejteni a játék során.

Az instruktor által átadandó játékszabályok:

- Mondjuk el, mit tartalmaz a játéktér, mi tartozik a fiktív irodához (jellemzően az íróasztal, a szék, a fiókos szekrény, a szemetes és minden, ami ezeken, illetve ezekben található). Célszerű arra is felhívni a figyelmet, hogy ezen területekre saját dolgokat, például mobiltelefont ne pakoljanak résztvevők, mert a tapasztalatok alapján ezek is könnyen áldozatává válnak a játéknak.
- Mondjuk el, milyen eszközök állnak rendelkezésre, pl. WiFi, Internet rendelkezésre áll, lehet használni. A tapasztalat alapján ezt a játék közben is el kell ismételni.
- Mondjuk el, hogy mi a megnyitandó fájl neve, formátuma, milyen eszközön kereshetjük.
- Mondjuk el, hogy privát eszközöket, például saját okostelefont lehet-e használni (általában igen, nem tiltott).
- Hívjuk fel a figyelmet arra, hogy csak biztonságtudatossági elemek hiányát kell felfedezni, egyéb trükköket nem kell alkalmazni (például felhasználó-váltás, stb.)
- Hívjuk fel a figyelmet arra, hogy van-e pontvesztési lehetőség, például biztonságtudatosnak kell-e lenniük a játékosoknak is.

- Kérjük meg a játékosokat, hogy ne változtassák meg a dokumentumok, fájlok tartalmát, valamint a beállításokat, illetve csak az erre kijelölt papíron jegyzeteljenek.

A speciális biztonsági szabályokra (például "Forgot password" funkció törli a Kingston titkosított pendrive tartalmát, 10 sikertelen kísérlet után zárolásra kerül a fiók, stb.) a tapasztalatok alapján érdemes inkább csak akkor felhívni a figyelmet, ha már megtalálták a kapcsolódó eszközt. Így egyrészt nem adunk plusz segítséget (például, hogy akkor biztos, hogy találni kell egy titkosított pendrive-ot), illetve nem is felejtik el a játékosok, míg oda jutnak. Szintén hasznos lehet, ha a speciális szabályokat egy „Információbiztonsági szabályzat" dokumentumban rögzítjük és helyezzük el a játéktérben, melyet a játékosok használhatnak.

5.3.3.6. Felügyelet és segítség

A játék során az instruktor feladata, hogy észlelje, ha valamelyik résztvevő megszegi a szabályokat, illetve természetesen elakadás esetén segítsen az időkeret tartása érdekében. A felügyelet történhet akár webkamerán keresztül is, mint a klasszikus szabadulószobákban, azonban a tapasztalat szerint nem zavaró az sem, ha személyesen maradunk bent a játéktérben. A segítségnél fontos arra figyelni, hogy inkább rávezető kérdéseket tegyünk fel instruktorként – a túl konkrét és túl gyors információátadás rontja a játék élvezhetőségét.

Ami a segítség gyakoriságát illeti, nagyon fontos, hogy az instruktor tisztában legyen a forgatókönyv menetével és jól meg tudja becsülni a hátralevő feladatok időigényét. Nem szabad elfeledkezni a nem lépéssorrendben megoldott feladatokról, azaz attól, hogy az első lépést még nem oldották meg a játékosok, még szerepelhetnek időarányosan jól a többi feladattal. Az eddigi tapasztalatok alapján nem lehet olyan ökölszabályt mondani, hogy milyen időközönként nyújtsunk segítséget, vagy egyáltalán mikor adjuk az első segítséget.

Természetesen instruktori feladat az is, ha a játékosok valamit elrontanak, helyreállítsuk azt (például kitörölnek információt, kijelentkeznek a közösségi média fiókból, stb.), így érdemes mindenből tartalék eszközzel is rendelkezni.

5.3.3.7. Fotó és eredmények

A feladat megoldása közben, illetve után a hagyományos játékokhoz hasonlóan célszerű csoportképet készíteni az eredményt mutató táblákkal, melyet a résztvevőkkel elektronikus úton oszthatunk meg, és melyek a következő rendezvényhez remek promóciós anyagként is szolgálnak. Ha van lehetőségünk, a résztvevőket egy kis ajándékkal (például kameratakaró, kulcstartó, jegyzettömb, kitűző, stb.) jutalmazhatjuk, vagy nyomtathatunk számukra oklevelet, mely tartalmazhatja a csoportképet és a teljesítési időt. Bár ezek csupán apróságok, mégis nagymértékben motiválhatják az embert a részvételre és a pozitív tapasztalatok egymás közötti

megosztására, nem is beszélve arról, hogy mindig emlékeztetni fogják az illetőt arra, hogy mit tanult a biztonságtudatossági szabadulószobában.

Az egyes játékoscsoportok között az instruktor feladata a rendrakás és annak ellenőrzése, hogy minden a normál állapotban maradt-e, vagy módosítottak-e valamit szándékosan vagy véletlenül a résztvevők. Természetesen plusz pontként be lehet építeni a játékba a munkakörnyezet megóvását is.

A játék tapasztalatait és eredményeit érdemes megosztani egyrészt rögtön a játék után az egyes csoportokkal, közösen átbeszélve a főbb üzeneteket, illetve érdemes valamilyen megosztható anyagot is készíteni az összesített eredményekből (például Intranet felületen).

5.4. A BIZTONSÁGTUDATOSSÁGI SZABADULÓSZOBA HATÉKONYSÁGÁNAK ÉRTÉKELÉSE

Az előző pontokban bemutattam, hogy szervezeti környezetben ki lehet alakítani biztonságtudatossági szabadulószobát. Ebben az alfejezetben azt igazolom, hogy a szabadulószoba ténylegesen alkalmazható a munkatársak információbiztonsági oktatására, valamint hatékonyan képes növelni a biztonságtudatossági ismeretek, illetve a több biztonságtudatossági ismerettel rendelkező felhasználók számát.

Ennek igazolására két kutatást használok fel, és azok eredményeit elemzem, az egyik a 2016-2019-ben készült felmérés, a másik pedig a jelen disszertációhoz folytatott kutatás.

5.4.1. A KAPCSOLÓDÓ 2016-2019 KÖZÖTT FOLYTATOTT KUTATÁS BEMUTATÁSA ÉS EREDMÉNYEI

Biztonságtudatossági szabadulószoba témában két kutatást folytattam, ezek egyike a 2019-ben a Cyber Science konferencián publikált (Oroszi, 2019), 2016-2019 között megvalósított, kifejezetten a biztonságtudatossági szabadulószobához kapcsolódó kérdőívezés volt, a másik pedig a 2021-2023 között zajló, jelen disszertációhoz készült felmérés, melyet a 3. fejezetben mutattam be.

Az általam fejlesztett biztonságtudatossági szabadulószobával kapcsolatban először 2016-ban kezdtem el felmérést végezni, melynek során azon konferenciákon, melyen megjelentem a szabadulószoba programmal, illetve azon szervezeteknél, ahol a megbízó hozzájárult, a résztvevőkkel egy rövid kérdőívet töltettem ki a játékot követően. Ezen felmérésnek kifejezetten az volt a célja, hogy megvizsgáljam, hogy a résztvevők hogyan értékelik a programot mind hasznosság, megszerzett ismeretek, mind élmény szempontjából.

A kérdőív a következő kérdéseket tartalmazta a statisztikai adatokon túl:

- Mi nyújtotta a legnagyobb segítséget a feladatok megoldásához?
- A felsorolt biztonságtudatossági hiányosságokból melyeket szokta a résztvevő is elkövetni?
- A résztvevő figyel-e arra, hogy a közösségi oldalon milyen adatokat oszt meg nyilvánosan?
- Mennyire tartotta biztonságtudatosnak a résztvevő a szoba „lakóját”?
- Melyik volt a legnehezebb feladat a játék során?
- Jelszó választáskor a résztvevő figyel-e arra, hogy ne szerepeljenek a jelszavában személyhez köthető adatok?
- Összességében milyen érzést keltett a résztvevőben a játék?

Ezen felmérés során 230 db értékelhető kérdőív született. A résztvevők statisztikai adatai a következők voltak:

- a játékos neme, életkora (a kitöltők csak a „25 év alatti” = fiatal munkavállalók, „25-50 év között” = általános munkavállalók, „50 évnél több” = nyugdíjazás előtt álló munkavállalók kategóriáját jelölhették meg),
- a jelenlegi munkahelyen eltöltött évek száma („1 évnél kevesebb” = új munkavállalók, „1-5 év” = általános munkavállalók), „5-10 év” = tapasztalt alkalmazottak vagy „több mint 10 év” = nagyon tapasztalt alkalmazottak),
- részvétel a biztonságtudatossági képzésen (igen/nem),
- az utolsó biztonságtudatossági képzés jellege (e-Learning/tantermi oktatás) és
- az utolsó ilyen jellegű képzés időpontja (1 éven belül/1-2 évvel ezelőtt/2-5 évvel ezelőtt/több mint 5 éve).

A résztvevők 38%-a nő, 62%-a férfi volt, 74%-uk 25-50 éves korosztályba tartozó, 19%-uk 25 év alatti, 6%-uk 50 év feletti munkavállaló, 1%-uk pedig nem nyilatkozott a koráról.

A játékosok 78%-a vett részt korábban biztonságtudatossági képzésen, és a válaszok alapján már akkor az e-Learning volt a leginkább alkalmazott módszer, és pusztán a munkavállalók 3%-a emlékezett tantermi előadáson való részvételre. A válaszadók 20%-a egy éve, 13%-a pedig 1-2 évvel ezelőtt vett részt utoljára tudatossági képzésen.

Az alap statisztikát áttekintve érdekesség, hogy előfeltételezésemmel ellentétben több férfi vett részt a játékokon, mint nő, és emellett pozitívum, hogy túlnyomórészt nem a pályakezdők, gyakornokok (25 év alatti résztvevők) favorizálták a játékot, hanem minden korosztály képviseltette magát.

Ezen felmérés gyakorlati tapasztalatai és visszajelzései alapján akkor a leghatékonyabb a biztonságtudatossági szabadulószoba, ha valamilyen eseményre, csapatépítőre, családi napra vagy (belső) konferenciára szervezzük, hiszen akkor a munkatársak jobban időt tudnak szakítani a részvételre, kevésbé akadályozza a munkát, napi rutint. Egyéb esetben fontos, hogy küldjünk emlékeztetőt a regisztráltaknak, például naptárbejegyzés formájában, hogy ne jöjjön közbe más megbeszélés, illetve ne felejtődjön el a program.

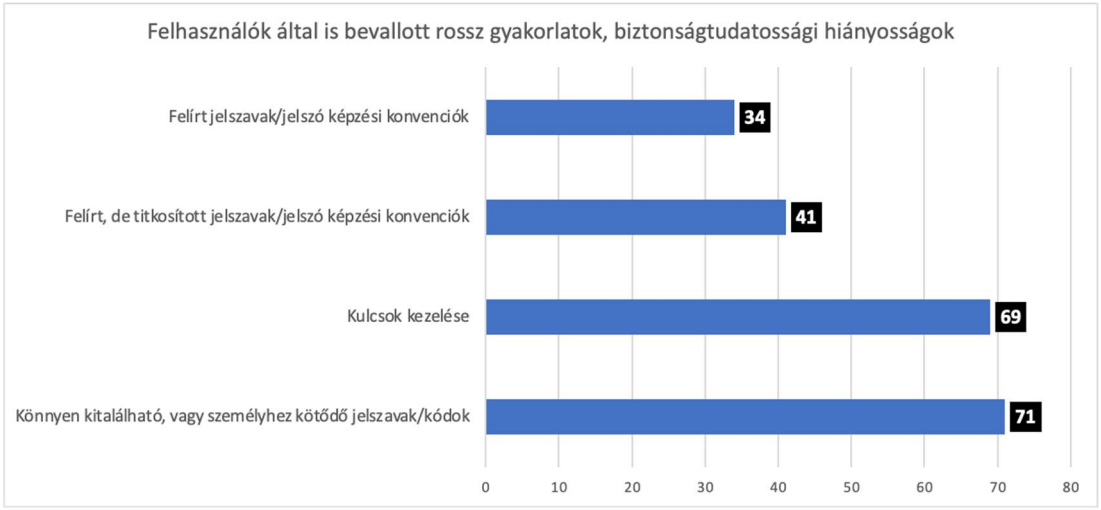
A felméréshez kapcsolódó visszajelzések nagyon pozitívak voltak a játékosoktól, többen kérdezték, hogy mikor lesz a következő alkalom (és ahol már több turnus is megszervezésre került, valóban sok ismert arc tért vissza a második fordulóra). Több különböző feladatot biztosító csapatépítőn is megjegyezték, hogy "*ez volt az az állomás, ahonnan mindenki mosolyogva távozott*", hiszen ez nem a szokványos "unalmas" csapatfeladat volt. Volt olyan szervezet, ahol biztonságtudatossági oktatáson való részvételt lehetett kiváltani a játékkal, és aki csak a kötelező jelleg miatt jött azzal a céllal, hogy passzív marad, az is becsatlakozott a feladatokba és segített a többieknek. Már ekkor is többször is megjegyezték, hogy voltak eszközök, melyek ugyan a vállalatnál rendelkezésre álltak, de eddig nem tudtak róla, vagy nem tudták használni (például titkosított pendrive), így a hiányosságok feltárása mellett ez is hasznos ismeret volt. Tapasztalt és bevallott jelenség volt, hogy többen magukra ismertek, és megdöbbentek, amikor egy játékostárs az általuk is alkalmazott hiányosságot felfedezte – ők jelezték, hogy ezen szokásokon változtatnak (például PIN kódként személyes információ használata, rejtekhelyek az irodában, stb.).

Többen ódzkodtak a mások (még ha csak fiktív személy is) holmijai közötti turkálástól, ők bevallották, hogy nem gondolnák, hogy bárki is hozzá merne ily módon nyúlni a dolgaikhoz – jó tapasztalat volt látni más kollégákon, hogy ez bizony nem kizárt, egy potenciális támadó az épületbe bejutva ugyanúgy megteheti ezt, mint a résztvevők a játék során. A hulladék átvizsgálás lehetősége szintén egy érdekes része volt a játéknak, többen is megkérdezték, hogy tényleg van-e értelme feltúrni a szemetest.

A külföldön szervezett játékok azt is alátámasztották, hogy mennyire is fontos felmérni előzetesen a résztvevői kört (szervezet, kultúra), volt ugyanis olyan feladatelem, mely hazánkban teljesen szokványos hiányosság, más országban viszont egyáltalán nem elterjedt (például telefon PIN kódjaként születési év használata). De szintén érdekes volt, hogy míg Magyarországon az elsődleges közösségi oldalnak a Facebook számított, máshol ezt a LinkedIn megelőzte, és elsősorban onnan próbáltak meg információt gyűjteni a résztvevők.

A 2016-os felmérésben kíváncsi voltam arra, hogy a résztvevők mely rossz szokásokat gyakorolják/gyakorolták saját bevallásuk szerint (több válasz is jelölhető volt). Ahogyan

feltételeztem, a kulcsok és a gyenge jelszóválasztás voltak a leginkább elkövetett, bevallott hibák, ahogyan az 55. diagram szemlélteti.



55. diagram: Mely hibákat követik el a felhasználók is a való életben? (db) (forrás: saját szerkesztés)

A válaszadás során a felhasználók önbevallás alapján töltötték ki a kérdőívet, így természetesen nem garantálható, hogy az eredmény tükrözi a valóságot, azonban mégis hasznos kiindulási pontot jelent, ha a felhasználók által is ismert hibákat akarjuk azonosítani.

Végül azt is megkérdeztem a kérdőívben, milyen benyomást keltett a játék, mennyire ment át az üzenete, elérte-e a célját. A válaszadók 66%-a hasznosnak vélte és leszűrte, miért fontosak a bemutatott biztonsági előírások, tudatossági elemek, és csupán elhanyagolandó töredékük (1%) jelezte, hogy nem gondolja, hogy ilyen a való életben is előfordulhat (56. diagram).

56. diagram: Milyen érzésekkel távoztak a résztvevők a biztonságtudatossági szabadulószobából? (forrás: saját szerkesztés)

Már ezen 2016-os kérdőíves felmérés is igazolta azon hipotézisemet, hogy a biztonságtudatossági szabadulószoba, mint gamifikációs elem használható a munkavállalók biztonságtudatossági képzésének eszközeként, mert összességében 90%-ban pozitív értékelést

kapott, azon belül is a válaszadók 66%-a az értékelés alapján nem csak tetszését fejezte ki, de véleménye szerint tanult is belőle.

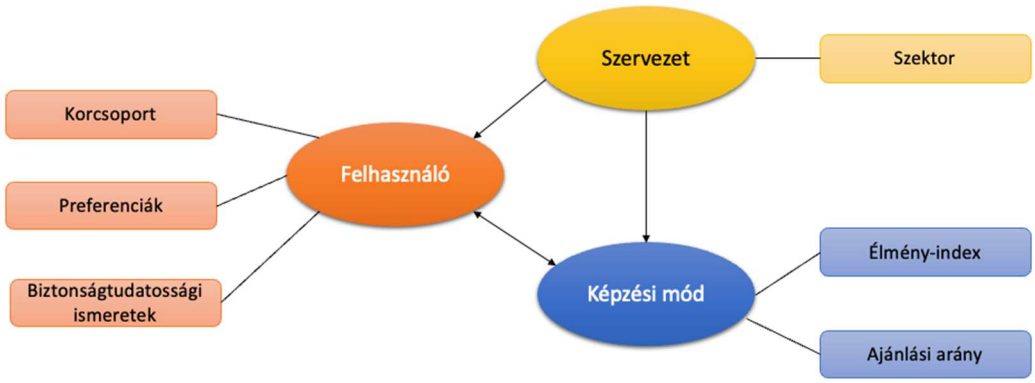
A felmérés rávilágított arra is, hogy a megtapasztalt felhasználói hibákra és hiányosságra jobban felfigyelnek a munkavállalók, és az önbevallás alapján tudták azonosítani azokat.

Ezen felmérés azonban nem alapozta meg azt, hogy a felhasználók ténylegesen tanulnak a programból, így a következő, jelen disszertáció keretein belül készült kutatással igazolom azt, hogy a biztonságtudatossági szabadulószoba nem csak a munkavállalók tetszését nyeri el, hanem képes is a felhasználók biztonságtudatossági ismereteinek növelésére.

5.5. A DISSZERTÁCIÓHOZ KÉSZÜLT KUTATÁS FELHASZNÁLT ADATAI ÉS EREDMÉNYEI

A biztonságtudatossági szabadulószoba alkalmazhatóságának vizsgálata során második forrásként szintén a 3. fejezetben bemutatott kutatás eredményeire támaszkodtam.

A vizsgálat során elsődlegesen a 8. ábrán szemléltetett adatokkal dolgoztam:



8. ábra: A kutatásban használt adatok a hipotézis vizsgálata során (forrás: saját szerkesztés)

Az adatok gyűjtése és a kérdőívek kitöltési aránya felhasználói, illetve szervezeti ismérvek vonatkozásában megegyezik a 3. fejezetben bemutatottakkal.

Az egyes képzési módokra vonatkozó kitöltési statisztikákat a 36. táblázat szemlélteti:

Program-típus	**K1 kérdőív (db)**	**K2 kérdőív (db)**	**K3 kérdőív (db)**
E-Learning	42	42	26
Kampány	47	47	31
Online oktatás	49	49	30
Szabadulószoba	48	48	37
Személyes oktatás	50	50	36
Társasjáték	48	48	34
Összesen:	**284**	**284**	**194**

36. táblázat: Kitöltési statisztikák (forrás: saját szerkesztés)

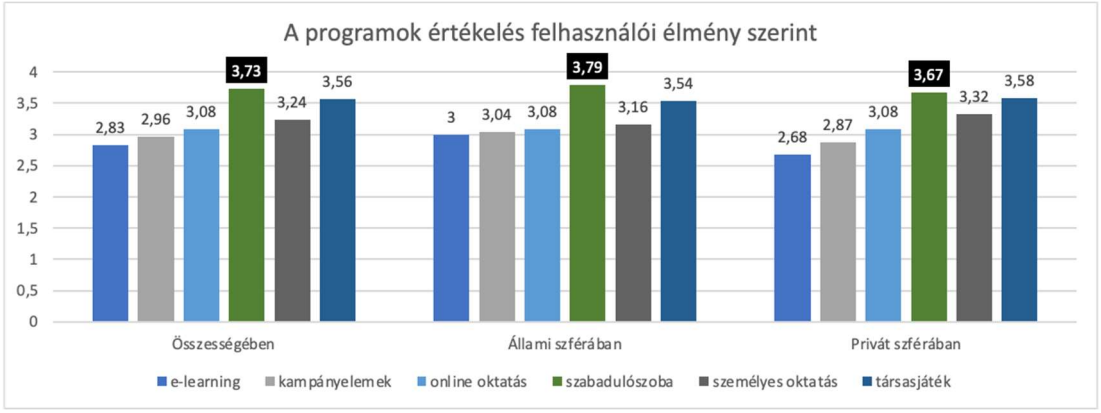
Ahogyan a gamifikációs programelemek értékelésénél, úgy a szabadulószoba esetében is az alábbi feltételekhez kötöttem a módszer eredményes alkalmazását:

- A felhasználók élvezetesnek tartják a programot.
- A felhasználók preferálják a programot.
- A felhasználók ajánlják a programot.
- A programot követően a résztvevők legalább egy új ismeretet tudnak írni a második kérdőíven (K2).
- A programot követően jelentős mértékben bővülnek a résztvevők biztonságtudatossági ismeretei (K2)
- A programot követően nagymértékben fejlődnek a korábban általánosságban hiányosságként azonosított ismeretek (iratmegsemmisítés, közösségi média, telefon és okos eszközök biztonságtudatos használata).
- A programot követően a résztvevők egy hónappal később (K3) is írnak olyan ismeretet, melyet az első kérdőívben nem rögzítettek, tehát a tudás tartósan megmaradt.
- A személyes tapasztalatok megerősítik a program alkalmazhatóságát.

Fentiek értékelését az alábbiakban mutatom be.

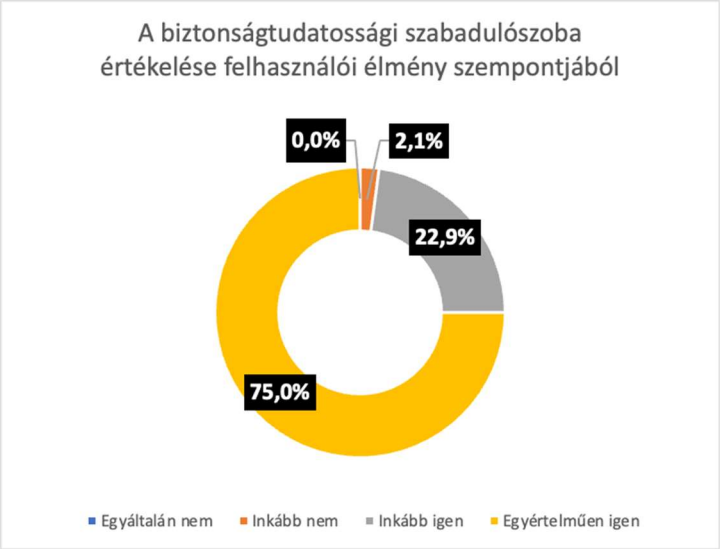
5.5.1. A BIZTONSÁGTUDATOSSÁGI SZABADULÓSZOBA ÉRTÉKELÉSE FELHASZNÁLÓI ÉLMÉNY ALAPJÁN

A disszertáció 3.6 pontjában folytatott vizsgálat alapján megállapítottam, hogy a szabadulószoba mind az állami, mind a privát szférában a leginkább élvezetesnek ítélt programelem, melyet az 57. diagram is szemléltet.



57. diagram: A biztonságtudatossági szabadulószoba értékelése felhasználói élmény alapján (élmény-index) (forrás: saját szerkesztés)

Részletes értékelés tekintetében a résztvevők 75%-a „*Egyértelműen élvezetes*”-nek értékelte, melyet az 58. diagram is tükröz.



58. diagram: A biztonságtudatossági szabadulószoba részletes értékelése felhasználói élmény alapján (forrás: saját szerkesztés)

Az eredmények alapján elmondható, hogy a felhasználói élmény alapján a biztonságtudatossági szabadulószoba alkalmazható megoldás munkahelyi környezetben.

5.5.2. A BIZTONSÁGTUDATOSSÁGI SZABADULÓSZOBA ÉRTÉKELÉSE PREFERENCIA ALAPJÁN

A disszertáció 4.4 pontjában folytatott vizsgálat alapján megállapítottam, hogy a szabadulószoba a program előtt a 10 vizsgált módszer közül az 5. legpreferáltabb módszer volt a biztonságtudatossági fejlesztési módszerek között, tehát a középmezőnyben végzett. A programot követő mérés alapján azonban a legpreferáltabb oktatási módszerré vált.

Az eredmények alapján elmondható, hogy a felhasználói preferencia változása alapján a biztonságtudatossági szabadulószoba alkalmazható megoldás munkahelyi környezetben.

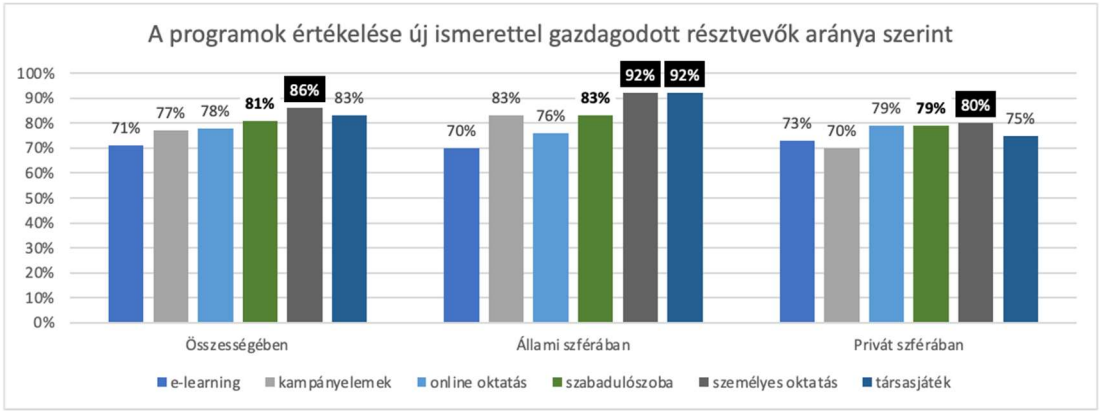
5.5.3. A BIZTONSÁGTUDATOSSÁGI SZABADULÓSZOBA ÉRTÉKELÉSE FELHASZNÁLÓI AJÁNLÁS ALAPJÁN

A disszertáció 4.5 pontjában folytatott vizsgálat alapján megállapítottam, hogy a felhasználók 98%-a ajánlja a programot. Állami szektorban 96%-kal a leginkább ajánlott megoldás, privát szférában pedig 100%-os ajánlási aránnyal a leginkább ajánlott megoldás.

Az eredmények alapján elmondható, hogy a felhasználói ajánlás alapján a biztonságtudatossági szabadulószoba alkalmazható megoldás munkahelyi környezetben.

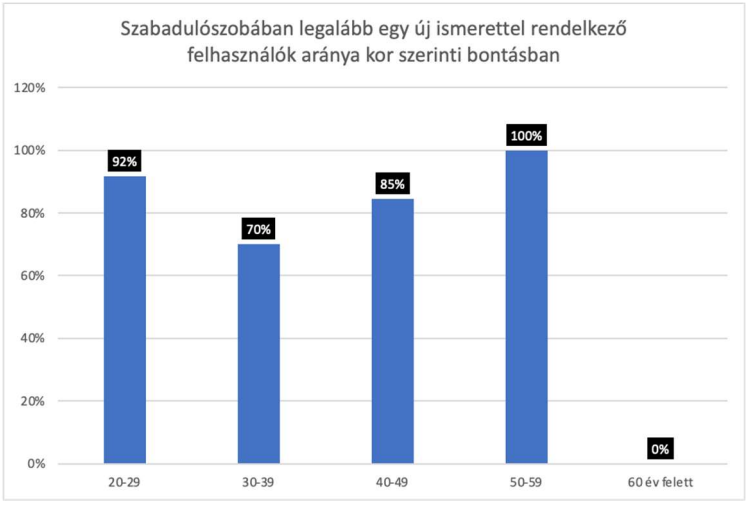
5.5.4. A MÓDSZER HATÉKONYSÁGÁNAK ÉRTÉKELÉSE A BIZTONSÁGTUDATOSABB FELHASZNÁLÓK SZÁMÁNAK NÖVELÉSÉBEN

Hatékonyság szempontjából megnéztem, hogy a szabadulószoba program hány százalékát fejlesztette a résztvevőinek, azaz a résztvevők hány százaléka írt a programot követő kérdőíven (K2) legalább egy új ismeretet. Ahogyan az 59. diagram is szemlélteti, ezen a téren összességében 3. helyen végzett a személyes oktatás és a társasjáték után, állami szférában szintén ezek után a 2., privát szférában pedig a személyes oktatást követő 2. helyet foglalta el az online oktatással holtversenyben.



59. diagram: A biztonságtudatossági szabadulószoba hatékonyságának értékelése a legalább 1 db új ismerettel rendelkező résztvevők aránya szerint (forrás: saját szerkesztés)

Kor szerinti bontásban a 60. diagram alapján leginkább az 50-59 éves korcsoport (100%), valamint a 30 év alattiak (92%) profitáltak belőle. (60 év feletti résztvevője nem volt a programnak.



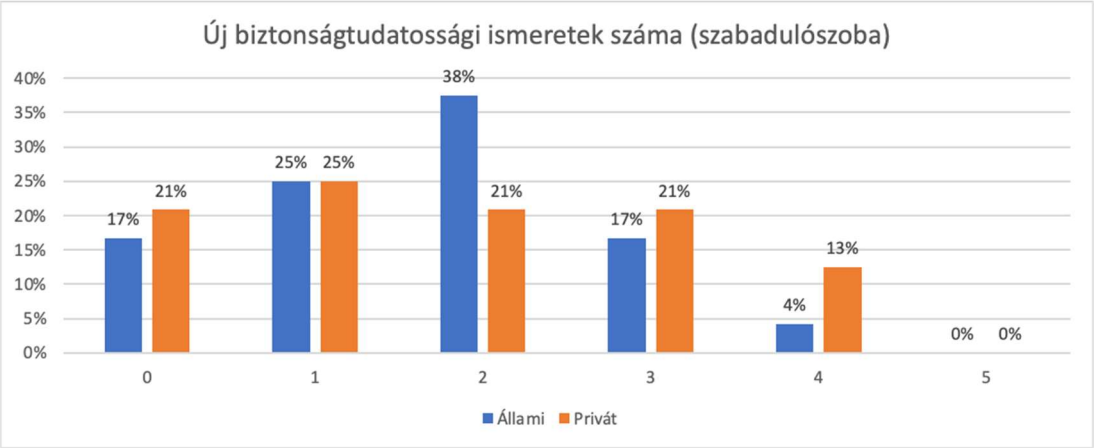
60. diagram: A biztonságtudatossági szabadulószobában résztvevő, legalább 1 db új ismerettel rendelkező felhasználók aránya korosztály szerint (forrás: saját szerkesztés)

Az eredmények alapján elmondható, hogy a legalább egy új biztonságtudatossági ismeretet szerző felhasználók aránya alapján a biztonságtudatossági szabadulószoba a 3. legjobb biztonságtudatosságot fejlesztő megoldás, ezáltal képes a biztonságtudatosság fejlesztésére, a több biztonságtudatossági ismerettel rendelkező felhasználók számának növelésére munkahelyi környezetben.

5.5.5. A MÓDSZER HATÉKONYSÁGÁNAK ÉRTÉKELÉSE A BIZTONSÁGTUDATOSSÁGI ISMERETEK SZÁMÁNAK NÖVELÉSÉBEN

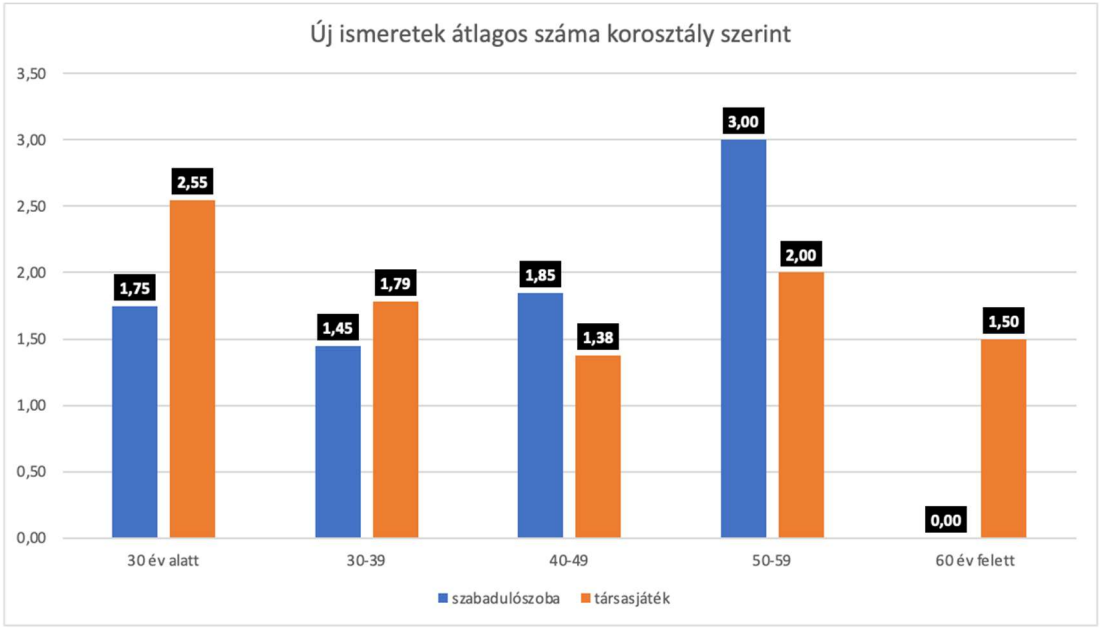
A szabadulószoba programon résztvevők összesen 83 db új ismeretet írtak, ez azt jelenti, hogy minden résztvevő átlagosan 1,73 db ismerettel írt többet a programot követően. Szektor szerinti bontásban ez állami szféra esetében 1,67 db, privát szféra esetében pedig 1,79 db új tudatossági elemet jelent. Ez alapján összességében a 4. leghatékonyabb megoldásnak tekinthető a társasjáték, kampányelemek és az online oktatást követően, állami szférában az 5., míg privát szférában az 1. helyet foglalja el.

A 61. diagram azt szemlélteti, hogy résztvevő felhasználók hány százaléka írt adott mennyiségű új biztonságtudatossági ismeretet szektor szerinti bontásban, mely jól tükrözi a privát szférában való dominanciáját.



61. diagram: A biztonságtudatossági szabadulószobában résztvevő felhasználók aránya új ismeretek szerzésének bontásában, szektor szerinti megkülönböztetéssel (forrás: saját szerkesztés)

A korosztály szerinti csoportosítást nézve az alábbi diagram alapján megállapítható, hogy az átlagosan legtöbb (3 db) ismeretet az 50-59 éves korosztály szerezte a szabadulószoba program során (62. diagram).

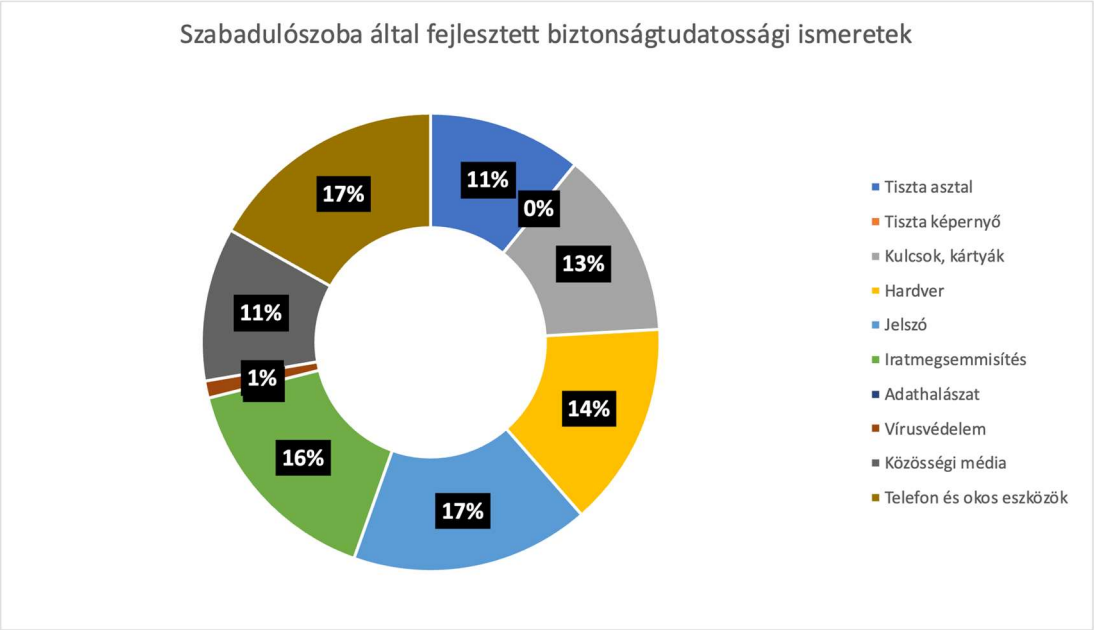


62. diagram: A biztonságtudatossági szabadulószobában és társasjátékon résztvevő felhasználók által szerzett új ismeretek átlaga (db) korosztály szerinti bontásban (forrás: saját szerkesztés)

Az eredmények alapján elmondható, hogy a biztonságtudatossági ismeretek számának növelése alapján a biztonságtudatossági szabadulószobának 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.

5.5.6. A MÓDSZER HATÉKONYSÁGÁNAK ÉRTÉKELÉSE A LEGINKÁBB HIÁNYOSNAK BIZONYULT BIZTONSÁGTUDATOSSÁGI ISMERETEK SZÁMÁNAK NÖVELÉSÉBEN

Az értékelésem egyik szempontja volt az is, hogy a korábban legjellemzőbb hiányosságként azonosított ismeretek milyen mértékben fejlődtek. Az alábbi diagram alapján elmondható, hogy mind a telefon és okos eszközök biztonságtudatos használatát (17%), mind az iratmegsemmisítést (16%), mind pedig a közösségi média biztonságtudatos használatát (11%) hatékonyan adta át a program (63. diagram).



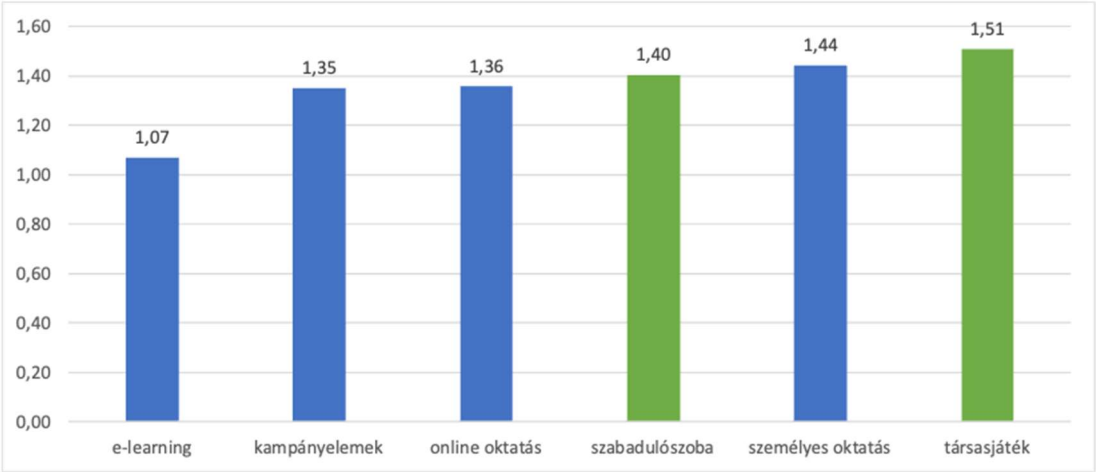
63. diagram: A biztonságtudatossági szabadulószoba által fejlesztett új ismeretek (forrás: saját szerkesztés)

A fentiek alapján elmondható, hogy a szabadulószoba programot követően nagymértékben fejlődnek a korábban általánosságban hiányosságként azonosított ismeretek (iratmegsemmisítés, közösségi média, telefon és okos eszközök biztonságtudatos használata).

5.5.7. HATÉKONYSÁG ÖSSZESÍTETT ÉRTÉKELÉSE KÖZVETLENÜL A PROGRAMON VALÓ RÉSZVÉTELT KÖVETŐEN

A biztonságtudatossági programok hatékonyságát a fentiek szerint abból a szempontból külön értékeltem, hogy hány felhasználó biztonságtudatossági ismereteit növelték, illetve milyen mértékben növelték átlagosan az ismereteket. Szerettem volna azonban azt is valamilyen módon értékelni, hogy összességében mit lehet mondani, melyik bizonyul a leghatékonyabb oktatási módszernek. Ennek megállapítására az egyes módszerek átlagos új ismereteinek a számának, valamint a legalább egy új ismeretet szerzett felhasználók arányának a szorzatát vettem alapul.

Az eredmények alapján összességében a következő sorrend alakult ki (64. diagram):



64. diagram: A biztonságtudatossági szabadulószoba hatékonysága az összesített rangsor szerint (összesített hatékonyság-index) (forrás: saját szerkesztés)

Fentiek alapján elmondhatjuk, hogy a biztonságtudatossági szabadulószoba összességében a 3. legjobb biztonságtudatosságot fejlesztő megoldás, ezáltal képes a biztonságtudatosság fejlesztésére munkahelyi környezetben.

5.5.8. HATÉKONYSÁG ÖSSZESÍTETT ÉRTÉKELÉSE 1 HÓNAPPAL A PROGRAMON VALÓ RÉSZVÉTELT KÖVETŐEN

A biztonságtudatosság fejlesztési programok természetesen akkor hatékonyak, ha a felhasználók nem csak a programot követően, hanem később is emlékeznek a tartalmukra, illetve alkalmazni is tudják azokat.

Azt ugyan nem tudtam tesztelni, hogy a tanultakat ténylegesen elsajátították-e készség szinten, és alkalmazzák-e a mindennapokban, a 4. fejezetben viszont értékeltem a kutatásban résztvevők 1 hónappal a program után kitöltött kérdőíveit is.

A szabadulószoba ennek alapján összességében a résztvevők 81,1%-át fejlesztette legalább egy tudatossági elemmel, és állami és privát szektor bontásban ennek arányában nincs jelentős különbség.

Ismeretek számát tekintve egy hónappal később átlag 1,7 db új ismeretet írtak az ezen résztvevő válaszadók, mely ugyan nem a hatékonyabb tudatosító eszközök közé sorolja a megoldást (utolsó helyen végzett a társasjátékkal holtversenyben), a privát szférában azonban 2,27 átlag új ismerettel az élvonalban van.

A korábbiak alapján elmondhatjuk, hogy a biztonságtudatossági szabadulószoba tartósan is képes fejleszteni a felhasználók biztonságtudatossági ismereteit és legalább az 1 új ismerettel rendelkező felhasználók számát hatékonyan képes növelni.

5.6. SZEMÉLYES TAPASZTALATOK AZ ALKALMAZÁS SORÁN

Az általam végrehajtott biztonságtudatossági szabadulószoba programok a fentieken túl az alábbi tapasztalatokkal járultak hozzá az értékeléshez:

- Bár a játékok meghirdetése nem mindenhol, és nem mindig történik zökkenőmentesen, ezáltal előfordul, hogy kedvezőtlen az előjelentkezési arány, azonban a program napján a játékoscsoportok további résztvevőket toboroznak, „híre megy” az eseménynek.
- Több szervezet információbiztonsági munkatársa is megjegyzete, hogy nagyon pozitív visszhangja volt a biztonságtudatossági szabadulószoba programnak, és a munkavállalóknak kifejezetten tetszett a megoldás.
- Vannak olyan szervezetek is, akik már minden évben beépítik a szabadulószoba lehetőségét a biztonságtudatossági programjukba.
- Érdemes a programot akár nyitott helyszínen, például aulában is megrendezni, mert így azon munkavállalók is értesülhetnek róla, akik esetleg más forrásból nem kapták meg az információt.
- Több játékoscsoport már rögtön a programot követően megkérdezte, hogy mikor lesz a következő alkalom, és több résztvevő külön is megkeresett a várható következő lehetőséggel kapcsolatban.
- Olyan játékoscsoport is előfordult, aki a párhuzamosan vezetett, különböző forgatókönyvű szabadulószobára is benevezett egy másik idősávban.
- A játékokra és rám, mint instruktorra, vannak felhasználók, akik úgy is emlékeznek, hogy teljesen külsősként vezettem a játékot.
- A játékba az is aktívan bevonódik, aki egyébként csak megfigyelő szerepet szeretne betölteni.
- Kifejezetten gyakran előfordul, hogy egy-egy, biztonságtudatossági szabadulószoba program résztvevő szervezet munkavállalói megjegyzik, hogy milyen tapasztalatokra tettek szert a játék során, és alkalmaznak is a mindennapokban (például „azóta sem dugom be az ismeretlen pendrive-ot”, vagy „azóta én is a szervezet által engedélyezett jelszószéfet használom”, stb.).
- A büntetőpontos verziókban, ahol nem kellően biztonságtudatos csoportok megnyithatnak szimulált kártékony kódot tartalmazó fájlokat, nagyon jól szembetűnik a játék adta „kipróbálom” élmény pozitívuma: az időbüntetésben részesülő csoportok több, mint fele elmondja, hogy szerinte vírusos a talált pendrive, vagy a furcsa melléklet,

de mivel ez egy játék, és baj úgysem lehet, megnyitja. (Ennek kapcsán nagyon jól lehet az értékelés során reflektálni a hamis biztonságtudat érzésére.)

- A kutatás utolsó (K3) kérdőívének szabadulószobában résztvevő válaszadói meglepő pontossággal írták le, hogy milyen feladatok voltak a szabadulószobában, és azok mentén rögzítettek biztonságtudatossági ismereteket.

Fentiek alapján elmondhatom, hogy a biztonságtudatossági szabadulószoba nagymértékben elnyerte a felhasználók tetszését, és megfelelő kommunikáció támogatásával szívesen részt vesznek a programokban. Emellett a visszajelzések azt is alátámasztják, hogy a résztvevők tényleg tanulnak a programokból, és alkalmaznak is ott bemutatott eszközöket, ismereteket.

5.7. LEVONT KÖVETKEZTETÉSEK

A fejezetben két felmérésem és gyakorlati tapasztalataim felhasználásával bizonyítottam azt a hipotézist, miszerint *„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 hipotézis igazolására a saját fejlesztésű biztonságtudatossági szabadulószoba programomat vontam be a kutatásba, melynek kialakítását és módszertanát jelen fejezetben részletesen bemutattam.
A kutatás eredményei alapján a következő megállapításokat tettem, és alábbi következtetéseket vontam le:

- Az eredmények alapján elmondható, hogy a felhasználói élmény értékelése szerint a biztonságtudatossági szabadulószoba alkalmazható megoldás munkahelyi környezetben, mert a válaszadók 98%-a élvezetesnek, ezen belül is 75%-a kifejezetten élvezetesnek tartotta azt a részvételt követően.
- Az eredmények bemutatták, hogy a felhasználók a programokon való részvételt követően sokkal inkább preferálták a szabadulószobát, mely a rangsorban az 5. helyről az 1. helyre lépett elő.
- Az eredmények alapján elmondható, hogy a résztvevő felhasználók átlag 98%-a ajánlja a programot, mely alapján ismételten elmondhatjuk, hogy a biztonságtudatossági szabadulószoba alkalmazható megoldás munkahelyi környezetben.

- Az eredmények alapján elmondható, hogy a legalább egy új biztonságtudatossági ismeretet szerző felhasználók aránya szerint a biztonságtudatossági szabadulószoba a 3. legjobb biztonságtudatosságot fejlesztő megoldás, ezáltal képes a biztonságtudatosság fejlesztésére, a több biztonságtudatossági ismerettel rendelkező felhasználók számának növelésére munkahelyi környezetben.
- Az eredmények alapján a szabadulószoba érzékenyítés céljából az 50-59 éves korosztály, illetve a 30 év alattiak körében a leghatékonyabb.
- Az eredmények alapján elmondható, hogy 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.
- A fentiek 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 fejlesztésére.
- Összesített eredmények alapján elmondhatom, hogy a biztonságtudatossági szabadulószoba összességében a 3. legjobb biztonságtudatosságot fejlesztő megoldás, melynek használata elsősorban a privát szférában előnyös.
- Az egy hónappal későbbi visszamérés eredménye alapján arra a következtetésre jutottam, hogy a biztonságtudatossági szabadulószoba tartósan is képes fejleszteni a felhasználók biztonságtudatossági ismereteit és legalább az 1 db új ismerettel rendelkező felhasználók számát hatékonyan képes növelni (ez az érték a kutatás során 81,1% volt).
- Saját személyes tapasztalataim is megerősítették, hogy a biztonságtudatossági szabadulószoba nagymértékben elnyerte a felhasználók tetszését, és megfelelő kommunikáció támogatásával szívesen részt vesznek a programokban. Emellett a visszajelzések azt is alátámasztják, hogy a résztvevők tényleg tanulnak a programokból, és alkalmaznak is ott bemutatott eszközöket, ismereteket.

Az előzetesen meghatározott szempontrendszerem szerinti értékelés eredményeit a 37. táblázatban foglaltam össze.

Szempont	*Értékelés*
A felhasználók élvezetesnek tartják a programot.	IGAZ
A felhasználók preferálják a programot.	IGAZ
A felhasználók ajánlják a programot.	IGAZ
A programot követően a résztvevők legalább egy új ismeretet tudnak írni a második kérdőíven (K2).	IGAZ
A programot követően jelentős mértékben bővülnek a résztvevők biztonságtudatossági ismeretei (K2)	RÉSZBEN TELJESÜL
A programot követően nagymértékben fejlődnek a korábban általánosságban hiányosságként azonosított ismeretek (iratmegsemmisítés, közösségi média, telefon és okos eszközök biztonságtudatos használata).	IGAZ
A programot követően a résztvevők egy hónappal később (K3) is írnak olyan ismeretet, melyet a program előtt nem, tehát a tudás tartósan megmaradt.	IGAZ
A személyes tapasztalatok megerősítik a program alkalmazhatóságát	IGAZ

37. táblázat: Összefoglaló táblázat a biztonságtudatossági szabadulószoba értékeléséről (forrás: saját szerkesztés)

A kutatással bizonyítottam, hogy az általam 2014-ben fejlesztett biztonságtudatossági szabadulószoba képes a biztonságtudatossági szint fejlesztésére mind az ismeretek bővítése, mind a biztonságtudatosabb felhasználók számának növelése szempontjából. A módszer a vizsgálatba bevont biztonságtudatosságot fejlesztő módszerek hatékonyság szerinti értékelése során rövidtávon a legjobb 3 megoldás között szerepel, és az eredmények alapján inkább a privát szektor szervezetei számára jelenti a leghatékonyabb megoldást. Ezen túlmenően megállapítottam, hogy a szabadulószoba hosszútávon, bár nem a leghatékonyabban, de képes a biztonságtudatossági ismeretek fejlesztésére.

6. A BIZTONSÁGTUDATOSSÁGI TÁRSASJÁTÉKOK ALKALMAZHATÓSÁGA A BIZTONSÁGTUDATOSSÁGI FEJLESZTÉSÉRE

A disszertáció 3. fejezetében bemutatott kutatás egyik eleme az általam 2021-2022-ben kifejlesztett biztonságtudatossági társasjáték volt, jelen fejezetben kifejezetten ennek alkalmazhatóságát, illetve hatékonyságát vizsgálom a felhasználók biztonságtudatossági fejlesztésének tükrében.

6.1. KAPCSOLÓDÓ 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 hipotézis igazolására szintén az első hipotézishez készített kutatást használtam fel, melynek során hat különböző biztonságtudatosságot fejlesztő módszert, köztük az általam 2021-2022-ben fejlesztett biztonságtudatossági társasjáték hatékonyságát vizsgáltam abból a szempontból, hogy melyiknek milyen hatása van a biztonságtudatossági ismeretek bővülésére (*átlagos új ismeretszám*), vagy a biztonságtudatos felhasználók számának növelésére (*legalább egy új ismeretet szerző résztvevő felhasználók aránya*).
A hipotézishez kapcsolódó új fejlesztés a „*SILENT SIGNAL – A biztonságtudatossági játék*" című, a felhasználók biztonságtudatossági ismereteit fejlesztő kooperációs-stratégiai társasjáték megalkotása és kiadása. (2021-2022)
A vizsgálat során célom annak bizonyítása volt, 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.

6.2. A BIZTONSÁGTUDATOSSÁGI TÁRSASJÁTÉK CÉLJA

A biztonságtudatossági szabadulószobák népszerűségéhez hasonlóan a stratégiai-kooperációs társasjátékok népszerűsége is megnövekedett az elmúlt időszakban. Nem csak a kiadott játékok és kiegészítőik száma nő folyamatosan, hanem olyan szolgáltatók is egyre többen megjelennek,

akik ezen játékok használatának lehetőségét biztosítják például kávézói élmény mellett (például Boardgame Café, BarCraft). Ezen szolgáltatások nagy előnye, hogy a játékosoknak nem kell feltétlenül áttanulmányozniuk egy hosszabb, bonyolultabb társasjáték szabálykönyvét, hanem kérhetnek instruktori segítséget az adott játék kipróbálásához, a szabályok megértéséhez és megtanulásához.

A fentiek, és egy, 2021. januárjában ajándékként kapott stratégiai kooperációs társasjáték (ALIENS – Another Glorious Day in the Corps) adta az ötletet ahhoz, hogy biztonságtudatossági témában is készítsek egy ilyen megoldást. Hiszen, ha olyan sokan hajlandóak viszonylag magas összeget kifizetni hasonló termékekért, a munkahelyeken ingyenesen biztosított biztonságtudatossági programként nyújtott, esetleg ajándékként adott változat a munkavállalók és munkáltatók számára is érdekes lehet. Emellett, ahogyan mind a szakirodalom feltárás során, mind a jelen disszertáció 3. és 4. fejezetében is bemutattam, a játékosítás szervezeti környezetben is egyre népszerűbbé vált, egyben hatékony megoldásnak is bizonyul, sőt megjelentek már kifejezetten biztonságtudatossági játékok is.

Mindezen okokból kifolyólag döntöttem úgy, hogy megvizsgálom annak lehetőségét, lehet-e egy, a biztonságtudatossági ismeretek mérésére-fejlesztésére szolgáló, elsősorban munkahelyi környezetre vonatkozó, de otthon is használható stratégiai-kooperációs társasjátékot készíteni. Ez lett a 2022. májusában első kiadású, végleges formájában megjelent *SILENT SIGNAL – A biztonságtudatossági játék* címet viselő, biztonságtudatosságot fejlesztő társasjáték (Oroszi, 2022).

A játék bemutatását és fejlesztésének menetét a 6.3 alfejezet, biztonságtudatossági képzések során történő használhatóságát pedig a 6.4, 6.5 és 6.6 alfejezetek részletezik.

6.3. A SAJÁT FEJLESZTÉSŰ BIZTONSÁGTUDATOSSÁGI TÁRSASJÁTÉK BEMUTATÁSA

A *SILENT SIGNAL – A biztonságtudatossági játék* (2. kép) alkalmazása során a játékosok hat különböző karakter bőrébe bújva tapasztalhatják meg, milyen információbiztonsági veszélyek leselkednek rájuk egy átlagos munkanap alatt. A résztvevőknek ki kell választaniuk a számukra legfontosabb biztonságtudatossági elemeket, ismereteket és alkalmazni kell azokat, hiszen minden körben más és más biztonsági eseményekkel találkoznak. Ezek, ha nem védik ki megfelelően, könnyen incidensként végződhetnek, azaz a támadók megszerezhetik eszközeiket, jelszavukat, belső vagy bizalmas információikat. Az egyes támadások kapcsolódhatnak bizonyos helyszínekhez, illetve az egyes karakterek kihasználható

tulajdonságaihoz is, így a játékosoknak folyamatosan résen kell lenniük, hogy milyen információbiztonsági ismereteket hasznosíthatnak az adott helyzetben. A játék célja sikeresen végére érni a „munkanapnak”, úgy, hogy közben minél több védendő értékük, információjuk megmaradjon.

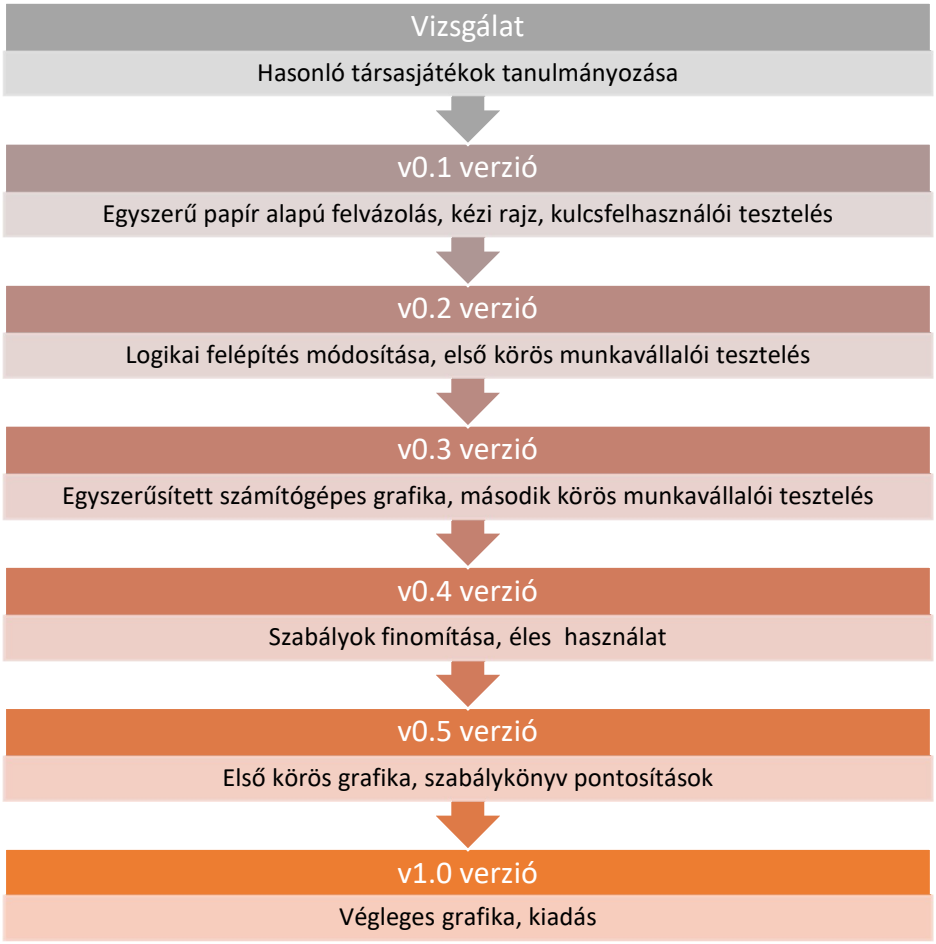
2. kép: SILENT SIGNAL – A biztonságtudatossági játék című társasjáték (forrás: https://silentsignal.hu/termekeink#tarsas, utolsó elérés: 2023.04.09.)

A következő blokkban bemutatom, hogy hogyan milyen lépések mentén történt a játék fejlesztése, milyen elemekből áll a játék, hogyan kerültek ezek kialakításra, milyen módon képes fejleszteni a felhasználók biztonságtudatosságát, valamint hogyan lehet alkalmazni munkahelyi környezetben.

6.3.1. A JÁTÉK FEJLESZTÉSE, KIALAKÍTÁSA

A biztonságtudatossági társasjáték fejlesztése jóval összetettebb folyamat volt, mint az előző fejezetben bemutatott szabadulószoba összeállítása, tekintve, hogy ebben az esetben nem adaptáció készült, hanem önálló játékmenetre épülő megoldás, összetett elemekkel.

A fejlesztés az alábbi fázisokból állt (9. ábra):



9. ábra: A biztonságtudatossági társasjáték fejlesztésének fázisai (forrás: saját szerkesztés)

6.3.1.1. Vizsgálat

A szakirodalom feltárás mellett első lépésként természetesen megvizsgáltam, hogy a stratégiai-kooperációs társasjátékok hogyan működnek, milyen elemekből állnak, és ezeket egy biztonságtudatossági változatban hogyan lehetne megvalósítani. Azt már az elején elhatároztam, hogy nem egy meglevő játék mechanikájára szeretnék biztonságtudatossági adaptációt készíteni (mint például a szakirodalom feltárás során bemutatott, a Ninja Burger játékmechanikájára épülő Control-Alt-Hack), hanem egy saját tervezésű játékmenettel rendelkező, mindinkább a való életet szimbolizáló verziót kialakítani. Ennek egyik oka volt, hogy bár nem vagyok társasjáték-fejlesztő, de nem terveztem licenc vásárlást meglevő játékmechanikára, másrészt olyan mély társasjáték-ismeretekkel sem rendelkezem, hogy megfelelő játékmechanikát tudtam volna választani az elképzeléshez. Továbbá, szintén kiemelném, hogy a fejlesztéssel elsődlegesen egy oktató megoldás, és nem kifejezetten szórakoztató játék kialakítása volt a célom (mondhatni, inkább egy társasjátéknak „kinéző” oktatási segédeszköz készítése).

A mintaként megtekintett 25 darab, különböző tematikájú és megközelítésű társasjátékból az alábbi ötöt választottam ki iránymutatásként és egyfajta mintaként a felsorolt elemekhez (38. táblázat):

Játék megnevezése	*Kapcsolódó biztonságtudatossági társasjáték elem*
ALIENS – Another Glorious Day in the Corps *(GaleForce Nine, 14+, 1-6 fő, 60-120 perc, angol nyelv. 19.990 Ft)*	• játéktábla, • küldetések, • karakterlapok, • karakterek tulajdonságai és korlátozásai, • idegenek mozgása, • későbbi kiegészítési lehetőségek előkészítése
Jurassic Park - DANGER *(Ravensburger, 10+, 2-5 fő, 50 perc, angol nyelv, 28 -68 USD)*	• karakterlapok, • tudatossági elem kártyák, • cselekménykártyák, • idegenek cselekményei, • egyéni célok bevezetése
Jurassic World – A társasjáték *(JustGames – Reflexshop, 12+, 2-6 fő, 60 perc, magyar nyelv, 10.990 Ft)*	• cím • időjelölő, • tudatossági-szint jelölő
PANDEMIC *(Z-MAN Games – Gém Klub, 8+, 2-4 fő, 45 perc, magyar nyelv, 14.990 - 16.995 Ft)*	• eszközjelölők, • cselekménykártyák
CLUEDO *(Hasbro, 8+, 2-6 fő, 40 perc, magyar nyelv, 13.995 – 16.990 Ft)*	• grafika, design • játéktábla

38. táblázat: Vizsgált társasjátékok (forrás: saját szerkesztés)

(Zárójelben a játék kiadója, a feltüntetett korosztály, a játékosok száma, a feltüntetett játékidő, a vizsgált játék nyelve, a játék 2023. március 31-én elérhető ára a következő kereskedőknél: Régió Játékbolt, Reflexshop, Gém Klub, illetve angol nyelvű játékok esetében Amazon).

A választásom a következő szempontok miatt esett ezekre:

- ne kifejezetten információbiztonsági társasjáték legyen (ennek oka, hogy szerettem volna kizárni a saját gondolkodásmenetem befolyásolását)
- stratégiai-kooperációs megközelítés
- célközönség, célzott korosztály: elsősorban 14 éven felüliek, kifejezetten felnőttek számára is élvezhető
- játékosok száma: 5-6 fő, de akár egyedül is végigjátszható
- játékidő: az időráfordítás legalább 60 perc legyen, de lehessen bele építeni rövidítést és hosszabb verziót is
- összetettség: ne kártyajáték, vagy kizárólag „lépegetős" játék legyen
- legyen bennük támadó játékos, illetve anélküli megközelítés
- árazás: a mintaként választott társasjátékok a 10.000 – 25.000 közötti árkategóriába essenek.

A biztonságtudatossági társasjáték általam elvárt paraméterei a fentiek vizsgálatát következők voltak:

- stratégiai-kooperációs megközelítés
- személytelen támadó alkalmazása, vagyis nincsen támadó játékos
- kifejezetten munkahelyi környezetben való alkalmazás támogatása (ugyanakkor ne zárjam ki az otthoni felhasználást, illetve a fiatalabb korosztályt)
- 6 fős játékoslétszám, nem kizárva a kevesebb felhasználót és az egyedüli játékost (több karakter irányítása)
- 1-2 óra időráfordítás
- a vizsgáltaktól egyszerűbb, könnyen megérthető játékmenet, mely valós munkahelyi tevékenységeken alapul (például a játékban bevezetett szabadságolás)
- mutassa be a szükséges biztonságtudatossági ismereteket
- mutassa be a lehetséges fenyegetéseket, támadási technikákat
- mutassa be a legjellemzőbb kihasználható emberi tulajdonságokat

A fenti játékok tanulmányozását és célok meghatározását követően, az átvett ötletek mentén készítettem el a játék következő pontokban bemutatott, biztonságtudatosságot fejlesztő verzióit. A játék szakmai összeállítása során az általam tartott biztonságtudatossági oktatások tapasztalatait, résztvevői kérdéseit, észrevételeit, illetve saját Social Engineering audit tapasztalataimat és valós, publikált incidensek, támadási kísérletek tanulságait építettem be.

6.3.1.2. Biztonságtudatossági társasjáték v0.1 verzió

A játék legelső verziója egy kézzel rajzolt játéktábla, illetve design nélküli és részlegesen kidolgozott, nyomtatott karakterlapok, tudatossági elemek, küldetések és cselekménykártyák voltak. A játéktábla tetején helyezkedett el egy célegyenesnek nevezett, 24 lépcsős sáv, mely a köröket hivatott szimbolizálni, a tudatossági szinteket pedig egyénileg gyűjtögetett tokenekkel mérhették a játékosok, melyeket vagy elvesztettek, és bedobtak a gyűjtőbe, vagy megszereztek és elvettek a gyűjtőből, vagy megtartottak, attól függően, hogy kivédtek-e egy támadást.

A játék ezen verziójának tesztelése 2021. május 15-én történt meg. A tesztelésbe és véleményezésbe olyan 6 fő kulcsfelhasználót vontam be, akik gyakorlottak stratégiai-kooperációs társasjátékok alkalmazásában, de csak részben rendelkeznek információbiztonsági szakértői, azon belül is biztonságtudatosság fejlesztési ismeretekkel (2 fő).

A tesztelő csoport összetétele a játékmesterrel a következő volt (39. táblázat):

Szempont	*Szakértő (db)*	*Átlagfelhasználó (db)*
Gyakorlott társasjátékos	2	3
Nem gyakorlott társasjátékos	1*	1

*39. táblázat: A tesztcsoport összetétele (ahol * a játékmestert jelöli) (forrás: saját szerkesztés)*

A tesztelés eredménye alapján a következők kerültek megváltoztatásra:

- célegyenes átalakításra került egy csökkentett számú időjelölővé,
- a biztonságtudatossági pontok számítása átalakult az időjelölőhöz hasonló mérési skálává és megszűntek az egyéni tokenek,
- a küldetések egyszerűsödtek, az eredetileg tervezett információ-típusonkénti (például projekt anyagok) bontást elvetettem
- a bábuk LEGO figurák lettek.

6.3.1.3. Biztonságtudatossági társasjáték v0.2 verzió

A következő verzió egy színesebb, jobban elrendezett, de szintén saját készítésű és nyomtatású játék lett, melyben a felvázolt módosításokat átvezettem. Ezen verzió tesztelésébe már bevontam a kulcsfelhasználókon kívüli átlagfelhasználókat és más szakértő kollégákat is, így a játékot ismételten 5 fő tesztelte az alábbi bontásban. A tesztre 2021. júliusában került sor.

Az új tesztelő csoport összetétele a játékmesterrel a következő volt (40. táblázat):

Szempont	*Szakértő (db)*	*Átlagfelhasználó (db)*
Gyakorlott társasjátékos	1	1
Nem gyakorlott társasjátékos	2*	2

*40. táblázat: A tesztcsoport összetétele (ahol * a játékmestert jelöli) (forrás: saját szerkesztés)*

Ezen verzió tesztelésének eredménye alapján a következők kerültek módosításra:

- az időjelölő kapott egy rövidebb verziót,
- a játékosok saját biztonságtudatossági szintjüket is tudták mérni a csoporté mellett, ezáltal a játék kapott egy versenyzési lehetőséget is,
- az egyes karakterek kaptak egyéni célokat az iroda területén történő mozgáshoz,
- a tudatossági elemekben és cselekménykártyákban pontosítás történt,
- a tudatossági elem és cselekménykártyák áttekinthetőbb piktogramokat kaptak,
- a cselekménykártyák hátoldalára felkerült, hogy milyen eszközt érintenek,
- a szabályokban módosulás történt (például vírusvédelem működése kockadobás alapján)
- finomodott a játék grafikája.

6.3.1.4. Biztonságtudatossági társasjáték v0.3 verzió

A fenti módosításokat tartalmazó verzió második körös munkavállalói tesztelése 2021. augusztus elején történt, ekkor újabb 5 fő olyan felhasználó tesztelte a játékot, akik különböző korosztályt képviseltek, illetve csak részben rendelkeztek komolyabb biztonságtudatossági ismeretekkel.

A tesztelő csoport összetétele a játékmesterrel a következő volt (41. táblázat):

Szempont	*Szakértő (db)*	*Átlagfelhasználó (db)*
Gyakorlott társasjátékos	0	2
Nem gyakorlott társasjátékos	2*	2

*41. táblázat: A tesztcsoport összetétele (ahol * a játékmestert jelöli) (forrás: saját szerkesztés)*

A teszt eredményeként tovább finomodott a játék és a következő módosításokat tettem meg:

- a választható tudatossági elemek számát 4-4 darabra emeletem a 3-3 helyett,
- a cselekménykártya paklit szétosztottam körülbelül egyenlő arányban a játékosok között,
- tovább finomítottam és pontosítottam a játékszabályokon a kérdéses esetek dokumentálásával,
- laminálásra kerültek a véglegesített lapok és kártyák.

6.3.1.5. Biztonságtudatossági társasjáték v0.4 verzió

Az előző módosításokat követően 2021. augusztus 30-ra kialakult a játékmenet végleges verziója, mely már a biztonságtudatossági kutatás során is alkalmazásra került a képen látható design-nal, egészen a v1.0 verzió megjelenéséig (3. kép).

3. kép: A játék utolsó verziója (v0.4) a grafikai módosítás előtt (forrás: saját fénykép)

A kutatás során, vagy később játékbemutatók alkalmával kapott észrevételeket rögzítettem, és a játékmenetet nem befolyásoló tényezőket a végleges kiadásba beépítettem (például javaslat volt, hogy a mobil-token is jelenjen meg, így a mobiltelefonos változat külön eszközjelölő tokenként jelenik meg, illetve ennek megfelelően apróbb szövegezési módosítások történtek a cselekménykártyákon).

6.3.1.6. Biztonságtudatossági társasjáték v0.5 verzió

A játék v0.5-ös verziója gyakorlatilag már csak a grafikai átalakítás volt, melynek során egy illusztrátor rajzolta meg a kapott információk alapján a játék elemeit. A játék grafikája több körben véglegesedett, ezeket – mivel szoros szakmai tartalom nem kapcsolódik hozzájuk – nem mutatom be az értekezés keretein belül. Ezen túlmenően szövegszerű módosítások, javítások

kerültek a kártyákra és a szabálykönyvbe, de változás nem történt a korábbi szakmai tartalomhoz és játékmenethez képest.

6.3.1.7. Biztonságtudatossági társasjáték v1.0 verzió (SILENT SIGNAL – A biztonságtudatossági játék)

A társasjáték alábbi, grafikailag is véglegesített, illetve címet kapott első kiadása 2022. májusában jelent meg a Silent Signal Kft. kiadásában, és az ISACA Budapest Chapter 2022. évi konferenciáján került bemutatásra.

A játékot azóta munkahelyemen a kutatás mellett több szervezetnél is szolgáltatásként, vagy termékként értékesítettük, illetve demó lehetőséget biztosítottunk. Az itt kapott visszajelzéseket folyamatosan rögzítettem, illetve a mai napig rögzítem, és értékelem a következő kiadásba történő beépítését, vagy kiegészítőként való biztosítását, úgy mint:

- karakterlapokon a fix tulajdonságok helyett választható tulajdonságok biztosítása,
- új karakterek és küldetések,
- új tudatossági elemek és cselekménykártyák beépítése (például üzletfolytonosság-menedzsment, adatvédelem),
- játék cél módosítása: az időkereten túl a maximum tudatossági szint elérésével is megnyerhető legyen a játék.

Az általános javaslatokon túlmutató, olyan igényeket, melyek szervezetspecifikus módosítást jelentenek, egyedi módon tudjuk beépíteni a játékba.

6.3.1.8. A játék továbbfejlesztésének lehetőségei

A folyamatosan érkező visszajelzések, kapcsolódó felmérések és tapasztalatok alapján a következő fejlesztéseket tervezem a társasjátékkal kapcsolatban.

A meglevő társasjáték v2.0 verziójába tervezett:

- karakterlapokon a fix tulajdonságok mellett opcionálisan választható tulajdonságok biztosítása
- szabályok kiegészítése, finomhangolása (például az időkereten túl a maximum tudatossági szint elérésével is megnyerhető legyen a játék)
- cselekménykártyák előválogatásának lehetősége jelölő ellátásával (például, ha specifikus támadási technikákat szeretnénk bemutatni, a kártyán feltüntetett jelölővel rendelkező lapokat alkalmazzuk csak a játék során).

Kiegészítőként tervezett:

- kiegészítő karakterek különböző beosztással

- az alap táblához illeszthető kiegészítő helyszínek (irodaház aula, parkoló, hulladék tároló, park)
- a kiegészítő helyszínekhez illeszkedő cselekménykártyák
- új, témaspecifikus tudatossági elem kártyák és cselekménykártyák (adatvédelem, üzletfolytonosság-menedzsment)
- támadó játékosok, és ezekhez illeszkedő szabálykönyv (önálló játékként vagy a védekező játékosokkal vegyesen)

Új, önálló társasjátékként tervezett és jelenleg a kialakítása folyamatban van:

- otthoni verzió egyszerűsített játékmenettel és specifikusabb, csökkentett számú biztonságtudatossági ismeret és cselekménykártyákkal
- kockázatmenedzsment társasjáték közép- és felsővezetők érzékenyítésére

6.3.2. A JÁTÉK ELEMEI

Ahogyan az előző pontban bemutattam, a társasjáték fejlesztése egy többlépcsős folyamat volt, melynek során a játék folyamatosan módosult, finomodott. Az alábbiakban a jelenleg elérhető, v1.0 verzió alapján mutatom be a játék elemeit. (A jobb megértés segítése érdekében a játékelemekről készült képeket nem külön mellékletben, hanem a vonatkozó pontban tüntetem fel.)

6.3.2.1. Játéktábla

A játéktábla (4. kép) egy iroda alapterületét jeleníti meg, ahol található folyosó, recepció/titkárság, igazgatói iroda, munkaterület, tárgyaló, konyha, szerverterem és mellékhelyiség is. Az egyes karaktereknek megvan az alapállása, a munkavégzésük elsődleges helyszíne, az egyes területek között pedig mozgás körben tudnak közlekedni.

4. kép: Játéktábla (forrás: saját fénykép)

6.3.2.2. Karakterlapok

A játékosok jelenleg 6 különböző karakter közül választhatnak a játékban: igazgató, titkárnő, jogász, HR-es kolléganő, fejlesztő és rendszergazda lehetnek.

Mindegyik karakterhez tartozik egy bábu, mely a játéktáblán mozog, és egy karakterlap (5. kép), mely a játékos előtt helyezkedik el. Ezen a karakterlapon vannak feltüntetve az adott karakter kihasználható tulajdonságai és egyéb információi.

5. kép: Karakterlapok (forrás: saját fénykép)

A kihasználható tulajdonságok közé 10 olyan emberi tulajdonságot emeletem, mely a biztonságtudatossági oktatások során is gyakran elhangzik, ezek a következők:

- Segítőkészség
- Kíváncsiság

- Nyitottság
- Hiszékenység
- Túlterheltség
- Figyelmetlenség
- Megfélemlíthetőség
- Ismeretlenekkel való gyakori kommunikáció
- Új munkatárs
- Rutin feladatok ellátása

Ezek közül minden karakter 5 darabbal rendelkezik, melyek cselekménykártyák esetén lesznek relevánsak. A kihasználható tulajdonságok és kapcsolódó cselekménykártyák úgy kerültek kialakításra, hogy a tapasztalatok alapján leggyakrabban kihasznált tulajdonságokhoz több támadás kapcsolódjon.

Ezen kívül a karakterlapon került feltüntetésre a helyettesítési rend és a karakterre vonatkozó korlátozások (például hová nem mehet), utóbbiakat haladó játékoscsoportoknál célszerű csak alkalmazni.

A karakterlapra kell felhelyezni a játékosokhoz tartozó eszközöket szimbolizáló tokeneket (6.3.2.3), illetve a 4 darab állandó, és 4 darab körönként változtatható tudatossági elemet (6.3.2.5), valamint a szétosztott cselekménykártya paklit lefordítva (6.3.2.6).

Egy kirakott karakterlap a 6. képen látható módon néz ki (természetesen egyénileg szabadon választott biztonságtudatossági ismeret kártyákkal):

6. kép: Kirakott karakterlap (forrás: saját fénykép)

A karakterlapon szintén elhelyezésre került egy 1-10-ig számozott skála, melyen a játékos a saját biztonságtudatossági szintjét, kivédett, illetve áldozatául vált támadásainak a számát tudja mérni (szintén haladó csoportok esetében érdemes az alkalmazása).

6.3.2.3. Eszközjelölő tokenek

Minden karakter ugyanazon védendő értékekkel rendelkezik, melyek eszközjelölő token (7. kép) formájában kerülnek fel a karakterlapra. Ezek a következők:

- Laptop
- Jelszó
- Token/mobiltelefon (attól függően, hogy a szervezetnél mi alkalmazott)
- Belső információ
- Fájl

7. kép: Eszköz-jelölő tokenek (forrás: saját fénykép)

A támadónak ezek megszerzése a célja küldetés függvényében (6.3.2.4), melyeket cselekménykártyák (6.3.2.6) formájában megjelenő támadásokkal tud eltulajdonítani. Amennyiben a játékos valamely védendő értékét elveszti, rá kell helyeznie azt a küldetéslapra (6.3.2.4), és a biztonságtudatossági szintjelölőn (6.3.2.8) vissza kell lépnie egy mezőt. Az elvesztett eszköz fizikailag, új eszközjelölő tokennel ugyan nem kerül pótlásra, de a továbbiakban is védeni kell (hiszen ez a való életben is megtörténik), és elvesztése negatív pontokat ér a szintjelölőn.

6.3.2.4. Küldetéslapok

A játékban jelenleg 4 különböző küldetés van, melyek a támadót, illetve célját szimbolizálják. Ezekkel senki nem játszik, a játék elején egy kerül kiválasztásra és mindenki által látható helyre helyezésre. Mindegyik küldetéslap (8. kép) tartalmazza a támadó célját, hogy mi ellen kell védekeznie a játékos csoportnak, illetve ezeken a küldetéslapokon kerülnek felhelyezésre a megszerzett eszközjelölő tokenek (6.3.2.3) a küldetés céljától függő darabszámban és összetételben.

8. kép: Küldetés lapok (forrás: saját fénykép)

Jelenleg a játékban a következő küldetések érhetőek el:

- Bizalmas adatok megvédése: a támadónak minden védendő értékből egyet kell megszerezni, mely bármely felhasználótól megszerezhető (tehát ez a legnehezebb küldetés).
- Jelszóvadászat kivédése: a támadónak ebben az esetben csak jelszavakra van szüksége, de minden felhasználóét meg kell szereznie ahhoz, hogy résztvevők elveszítsék a játékot.
- Kártékony kód terjedésének megelőzése: a támadónak ebben az esetben bármely felhasználótól származó 2 db fájlra, 2 db belső információra, 2 db jelszóra és 1 db zsarolóvírussal titkosított laptopra van szüksége.
- Social Engineering audit: a legkönnyebb küldetés, hiszen itt a támadót szimuláló auditorok mindent gyűjtenek.

A játékosok idővonaltól függetlenül elveszítik a játékot, amennyiben a küldetéslapra minden szükséges védendő érték eszközjelölő tokenje felkerült.

6.3.2.5. Biztonságtudatossági ismeret kártyák (ismeret elemek)

Minden karakter rendelkezik egy saját biztonságtudatossági ismeret kártyapaklival (9. kép), mely 30 darab biztonságtudatossági ismeretet tartalmaz, rövid leírással.

9. kép: Biztonságtudatossági ismeret kártyák (forrás: saját fénykép)

A játékosoknak ezek közül kell a játék során 4 darab állandót, nem változtathatót kiválasztaniuk és a karakterlap tetején jelölt helyre helyezniük, 4 darab változtathatót, melyet a karakterlap aljára kell tenniük, és melyek közül körönként tetszőleges számút cserélhetnek, attól függően, hogy épp hol helyezkednek el az irodában, a cselekménykártyák hátlapja alapján milyen eszközöket érintő támadások jönnek, vagy milyen eszközöket kell még kiemelten védeniük.

A karakterlapra felhelyezett biztonságtudatossági ismeretekkel lehet kivédeni a cselekménykártyák formájában bekövetkező támadásokat (a tudatossági elem beadása vagy cseréje nem szükséges).

A 30 darab tudatossági kártya a biztonságtudatossági oktatások során elhangzó legfontosabb ismereteket tartalmazza, ezeket a 6.3.3.1 pontban mutatom be.

6.3.2.6. Cselekménykártyák

A cselekménykártyák (10. kép) lehetnek támadások, melyek bizonyos védendő értékeket érintenek, vagy semleges, sőt pozitív események is (ezek hátulján meglepetés doboz látható).

10. kép: Cselekménykártyák (forrás: saját fénykép)

A játék során a támadó által végrehajtott támadásokat a cselekménykártyák testesítik meg, így ezek elsősorban a felhasználókat érintő fenyegetéseket mutatnak be, melyek között főképp általam végrehajtott Social Engineering auditok tapasztalatai, és valós, publikált incidensek és támadási kísérletek köszönnek vissza.
A cselekménykártyák a védendő értékeken túl vonatkozhatnak arra a játékosra, aki húzta azt, bizonyos tulajdonságokkal rendelkező, vagy bizonyos területen elhelyezkedő karakterekre, vagy akár mindenkire is.
Minden cselekménykártyán szerepel, hogy milyen védendő értékre vonatkozik, mi történik, hogyan zajlik a támadás, valamint a biztonságtudatossági ismeret-elemek közül melyekkel lehet kivédeni (ez piktogramként jelenik meg a 11. képen látható módon). Fontos, hogy a felsorolt biztonságtudatossági ismeretek közül egyetlen megléte is elegendő a támadás sikeres kivédéséhez.

11. kép: Cselekménykártya leírása és a kivédéséhez kapcsolódó biztonságtudatossági ismeret piktogramok (forrás: saját fénykép)

A mozgáskört követően minden játékosnak sorban fel kell húznia az előtte levő pakliból a legtetején levő cselekménykártyát és fel kell olvasnia. Eredménytől függően be kell szolgáltatni a védendő értékeket, és lépni a biztonságtudatossági szintjelölőn (6.3.2.8) a megfelelő irányba.

6.3.2.7. Idővonal

A játék egy munkanapot szimbolizál, így a körök is ennek megfelelően zajlanak. A játék választott hosszától függően egy kör egy órát, vagy fél órát szimbolizál, melyek mindegyikében minden felhasználónak mozognia, illetve cselekménykártyát kell húznia. Ha letelt egy cselekménykártya húzás kör, akkor lépni kell egyet előre az idővonalon, és mozgás körben lépni a kockadobás értéke szerint. A 12. alábbi képen a játék hosszabb verziójának idővonala látható.

12. kép: Segédtábla - idővonal (forrás: saját fénykép)

A külön segédlapon feltüntetett idővonalon kerültek felhelyezésre az egyes karakterek egyéni céljai, miszerint bizonyos karaktereknek adott idősávban megfelelő területen kell tartózkodniuk, például megbeszélésre mennek a tárgyalóba, vagy ebédelnek a konyhában. Amennyiben az érintett játékosok nem dobnák meg a jelölt területre történő belépéshez szükséges értéket, anélkül is be kell helyezni őket a területre, viszont a következő cselekménykártya húzás körben nem használhatják a választható tudatossági ismereteiket, le kell fordítaniuk azokat (ezzel a játék azt szimbolizálja, hogy sietség, kapkodás esetén hajlamosak lehetünk elfelejteni bizonyos biztonságtudatossági ismereteket, szabályokat).
Amennyiben a küldetés során nem vesztettük el a játékot, akkor abban az esetben nyerünk, ha elérkezünk a munkanap végére, vagyis az időjelölő utolsó mezőjére, és még az ehhez tartozó cselekménykártya körben sem veszítünk el minden szükséges védendő értékünket.

6.3.2.8. Biztonságtudatossági szintjelölő

Az idővonal segédlapján került elhelyezésre a csoport biztonságtudatossági szintjelölője (13. kép) is, mely pozitív és negatív irányban is egy 10-es skálán teszi lehetővé a biztonságtudatossági szint mérését. Az ehhez kapcsolódó tudatossági szintjelölő tokent a megfelelő irányba kell mozdítani releváns cselekménykártya húzása esetén, annak kivédésének vagy áldozatává válásának függvényében.

13. kép: Biztonságtudatossági szintjelölő a segédtáblán (forrás: saját fénykép)

Lehetőség van a biztonságtudatossági szint egyéni mérésére is, erre a karakterlapon elhelyezett, szintén 10-es skála szolgál a karakterhez kapcsolódó saját biztonságtudatossági szintjelölő tokennel. Ennek alkalmazása gyakorlottabb játékoscsoportok, haladó felhasználók esetében javasolt.

6.3.2.9. Idegenek

Ahogyan a munkahelyen, úgy a játékban is megjelennek idegenek: látogatók, ügyfelek, karbantartók. Az idegenek egyben támadók is lehetnek, akik kizárólag cselekménykártya hatására mozoghatnak és elkövethetnek visszaéléseket, például eltulajdoníthatnak eszközöket. Az idegenek úgy kerülnek fel a játéktáblára, hogy az időjelölő bizonyos mezőjében jelölve van látogató érkezése, melynek során a karakterek mozgását követően fel kell húzni a szintén időjelölő segédletre helyezett, idegen-kártya pakli (14. kép) legfelső lapját, és az ott szereplő instrukcióknak megfelelően kell elhelyezni az érkezőt az irodában.

14. kép: Idegenek érkezésének kártyái (forrás: saját fénykép)

Az idegenek bejövetelét akkor lehet megakadályozni, ha az érintett területen áll olyan karakter, aki már rendelkezik a szükséges biztonsági ismeretek egyikével. Ha a bejutás nem akadályozható meg ilyen módon, az idegenek eltávolítására úgy van lehetőség, hogy bármely karakter, aki a megfelelő ismeretek egyikével rendelkezik, a dobáskörben klasszikus kiütéssel az idegen mezőjére lép.

6.3.3. A JÁTÉK SORÁN FEJLESZTENDŐ ISMERETEK, TÉMAKÖRÖK

A társasjáték célja kifejezetten a biztonságtudatossági ismeretek bemutatása és alkalmazásuknak a begyakoroltatása a résztvevőkkel. Ennek megfelelően a játék során megjelennek a legfontosabb információbiztonsági szabályok és biztonságtudatossági ismeretek, az emberi tényezőt kihasználó támadási technikák, valamint a hamis biztonságérzet kezelése.

Emellett, hogy a játék játék is maradjon, természetesen szükség volt néhány olyan elem beépítésére, melyek a felhasználói élményt fokozták – ezek között van a véletlenek szerepe, illetve a szerencsefaktor. Ezeket a 6.3.3.4 alpontban mutatom be.

6.3.3.1. Információbiztonsági szabályok és ismeretek

Az információbiztonsági szabályok és ismeretek átadása a biztonságtudatossági ismeretelem kártyák keretein belül történik. A játékhoz az általános biztonságtudatosság fejlesztési anyagok alapján 30 darab ilyen elemet szedtem össze, melyek a következők:

- Fizikai biztonság:
    - Iroda zárása
    - Belépőkártya rendeltetésszerű használata
    - Idegenek megszólítása
    - Látogatók felügyelete
    - Tiszta asztal politika betartása
    - Kensington zár alkalmazása
    - Nyomtatás felügyelete
    - Iratmegsemmisítő használata
- Hozzáférés védelme:
    - Tiszta képernyő politika betartása
    - Erős, nehezen kitalálható jelszó választása
    - Csak a felhasználó által ismert, egyedi jelszó választása
    - Jelszószéf alkalmazása
    - Tokenek védelme
- Telefon és okos eszközök:
    - Hívó fél kilétének ellenőrzése
    - Jel/számkód alkalmazása az okos eszközökön
    - Munka és a magánélet szétválasztása
    - Ismeretlenek kezelése a közösségi médiában
    - Nyilvános megosztás kerülése a közösségi médiában
- Adataink védelme:
    - Lokális tárolás mellőzése
    - Biztonsági mentés készítése
    - Titkosított tárolás alkalmazása
    - Frissítések telepítése

    - Biztonságos WiFi használat
- Vírusvédelem és adathalászat elleni védekezés:
    - Vírusvédelmi rendszer
    - Gyanús linkek és tartalmak kerülése
    - Gyanús weboldalak és tartalmak kerülése
    - Gyanús mellékletek megnyitásának mellőzése
    - Ismeretlen eszközök helyes kezelése
- Visszaellenőrzés fontossága
- Incidensek jelentése

A biztonságtudatossági ismeret kártyák mindezen 30 darab ismeret rövid leírását, illetve piktogramos szemléltetését tartalmazzák.

6.3.3.2. Támadási technikák

A legfontosabb biztonságtudatossági ismeretek mindegyike természetesen valamely, a felhasználókat érintő támadási technikához kapcsolódik, ezért a játék cselekménykártyáinak formájában az alábbi, jellemzően emberi tényezőt kihasználó támadási technikákat, fenyegetéseket veszem sorba védendő értékenként:

- Laptop
    - Illetéktelen személy bejutása esetén az eszköz eltulajdonítása
    - Külső helyszínen felügyelet nélkül hagyott eszköz eltulajdonítása
    - Zsarolóvírus támadások
    - Megtévesztéses támadások során történő eltulajdonítás
- Token/okostelefon
    - Jogosulatlan hozzáférés őrizetlenül hagyott eszközökhöz
    - Felügyelet nélkül hagyott eszköz eltulajdonítása
    - Megtévesztéses támadások során történő eltulajdonítás
- Jelszó
    - Gyenge, esetlegesen többször is felhasznált jelszavak kompromittálása
    - Illetéktelen személy bejutása esetén a helytelenül választott vagy tárolt (felírt) jelszó megszerzése a munkakörnyezetből
    - Telefonon keresztüli megtévesztés jelszószerzés céljából
    - Adathalász megkeresések

- Belső információ
    - Illetéktelen személy bejutása esetén az információ megszerzése a munkakörnyezetből
    - Illetéktelen személy bejutása esetén jogosulatlan hozzáférés a nyomtatóban felejtett dokumentumokhoz
    - Szemeteskosárból kihalászott papír alapú dokumentumok
    - Telefonon keresztüli megtévesztés belső információk szerzése céljából
    - Adatszivárgás kártékony kód rendszerbe jutásának következtében
- Fájl (bizalmas információ)
    - Telefonon keresztüli megtévesztés fájl kiküldetése céljából
    - Illetéktelen személy bejutása esetén az információ megszerzése a zárolatlan munkaállomásról
    - Adatszivárgás kártékony kód rendszerbe jutásának következtében
    - Elvesztett vagy eltulajdonított eszközön tárolt adatok elvesztése
    - Elvesztett vagy eltulajdonított eszközön tárolt adatok kompromittálódása
- Általános
    - Belépőkártya elvesztésével vagy eltulajdonításával kapcsolatos visszaélés, épületbe történő illetéktelen bejutás
    - Iroda zárásának mellőzésével jogosulatlan belépés munkaterületre
    - Munkatársak megtévesztése az épületbe történő bejutás során
    - Információgyűjtés a célszemélyekről a közösségi médiában és más forrásokon keresztül, más támadások előkészítése

Az egyes fenyegetések 122 db cselekménykártyán, való életből vett példákkal illusztrálva jelennek meg, a leggyakrabban kihasználható emberi tulajdonságokra és helyzetekre fókuszáltan.

6.3.3.3. Hamis biztonságérzet

Gyakori tapasztalatom mind az oktatások, mind a Social Engineering auditok során a felhasználók hamis biztonságérzete, mely alatt azt értem, hogy sokan abban a tévhitben élnek, hogy az alkalmazott biztonsági eszközök és kontrollok megkerülhetetlenek és 100%-os védelmet nyújtanak, vagyis „megvédenek mindentől”. Tipikusan a fizikai biztonság, illetve a vírusvédelem területén tapasztalom ezeket, melyek esetében a munkatársak vakon megbíznak a beléptetőrendszer és a portaszolgálat megkerülhetetlen működésében, a vírusvédelmi rendszernek köszönhetően pedig bármilyen állományt meg mernek nyitni, és bármilyen

tartalom futtatását merik engedélyezni. Bár az említett megoldások valóban hatékonyak, de nem megkerülhetetlenek, így fontos a munkatársak edukálása, érzékenyítése a témában.
A biztonságtudatossági társasjátékban erre a vírusvédelem esetében van a legszembetűnőbb érzékenyítő példa, mivel a játék során a vírusvédelmi rendszer úgy működik, hogy ha a játékos rendelkezik is ezen kártyával, még akkor is dobnia kell a kockával: ha páros számot dob, a rendszer felismerete a kártékony kódot, páratlan dobás esetén viszont nem működött megfelelően, és a munkatárs eszköze kártékony kóddal fertőződött meg.

6.3.3.4. Szerencsefaktor

Az előző pontban bemutatott, hamis biztonságérzetre figyelemfelhívó kockadobással már láthattuk, hogy a játékba beépítésre került némi szerencsefaktor is. Erre a felhasználói élmény fokozása szempontjából is szükség volt, mert több tesztfelhasználó jelezte a tesztelési fázisban, hogy „nem eléggé játék” a játék.
Szerencsefaktorként a következők kerültek még beépítésre:

- Szabadságról vagy betegállományból való visszatérés kockadobással.
- Idegenek elhelyezése kockadobás függvényében.
- Kivédhetetlen támadások eszköz elvesztésére vonatkozóan. (Edukációs célt is képvisel, annak érdekében került beépítésre, hogy a felhasználók tisztában legyenek vele, a véletlennek köszönhetően is megtörténhet a baj, de az incidensek jelentésével csökkenthetik a károk mértékét.)
- Vírusvédelem kikapcsolása cselekménykártya.
- Valamely másik helyiségbe átirányító cselekménykártya.

A tapasztalatok azt mutatják, hogy ezen szerencse alapon működő elemek egyensúlyba hozzák a tanító célzatot a játékélménnyel, így alkalmazásuknak megvan a létjogosultsága egy oktató jellegű anyag esetében is.

6.3.4. A BIZTONSÁGTUDATOSSÁGI TÁRSASJÁTÉK ALKALMAZÁSA MUNKAHELYI KÖRNYEZETBEN

A biztonságtudatossági társasjáték bár otthoni környezetben is alkalmazható, elsősorban azonban munkahelyi használatra tervezett. Ezt támasztja alá a munkakörnyezet, karakterek, illetve bizonyos biztonságtudatossági ismeretek és cselekménykártyák is. A szervezeti használati lehetőségek közül is megkülönböztethetjük, hogy a munkavállalók milyen formában találkoznak ezen biztonságtudatosságot fejlesztő eszközzel.

6.3.4.1. Instruktor által vezetett program

A biztonságtudatossági társasjáték egyik legkézenfekvőbb lehetősége a biztonságtudatossági szabadulószobához hasonló esemény szervezése például biztonságtudatossági hónap keretein belül, vagy oktatás kiegészítéseként szolgáló kampányelemként. Ennek során a felhasználók ugyanúgy, csoportosan jelentkeznek a játékra, és egy instruktor vezeti végig a társaságot a feladatokon, segítve ezzel a játékmenet megértését, illetve a biztonságtudatossági ismeretek jobb elsajátítását, szükség esetén a kapcsolódó magyarázatokkal. A szabadulószobától eltérően ezen program jóval időigényesebb, 1-1,5 óra, azonban ezen időtartam alatt a résztvevők gyakorlatilag ugyanannyi ismerettel találkoznak, mint egy hasonló terjedelmű előadás során – ráadásul ezen esetben meg is tapasztalhatják az egyes biztonságtudatossági ismeretek alkalmazását, fontosságát. Szintén megjegyzendő, hogy a kapcsolódó kutatás bebizonyította, hogy a társasjáték is lebonyolítható „demó" jelleggel 30 perces blokkokban, az ezeken résztvevők jelentős része azonban azt jelezte, szívesen végigjátszaná egy másik alkalommal a játékot.

A játék hosszabb időráfordításából fakadóan szükség lehet párhuzamos játéklehetőség biztosítására, azaz egy időben több társasjátékkal több csoport is tud játszani. A társasjátékos kávézók mintájára ez teljes mértékben kivitelezhető a megfelelő mennyiségű társasjátékkal, illetve elegendő hellyel, az egyes játékoscsoportok nem zavarják egymást, sőt még segíteni is tudnak a másiknak.

Annak lehetősége is felmerült, hogy a játék során egy karaktert több játékos is irányíthat-e, például párosával növelhető-e a létszám 12 főre. Ebben én a következő kockázatokat látom:

- **passzív résztvevők**: akik ott vannak, de nem szeretnének bevonódni a játékba, csak megfigyelők. Ez nem jelenti azt, hogy nem tanulnak az eseményekből, de a szimulációs környezetből fakadó előnyökből kivonják magukat.
- **domináns résztvevők**: akik elnyomják a játékos párjukat, akkor is, ha az illető nem passzív játékos. A tapasztalat alapján ennek a megszerzett tudásra nem feltétlenül van hatása, a játékélményt viszont nagy mértékben rontja. (Megjegyzem, hogy 6 fős játékoscsoportok esetében is kezelendők a domináns játékosok.)
- **döntésképtelenség és egyet nem értés**: jelentősen növelheti a játékidőt, ha két aktív szereplős játékospár nehezen jut döntésre, vagy nem ért egyet a választandó biztonságtudatossági ismeretekkel kapcsolatban, különösen a körönként változtatható elemek esetében. Ezt javasolt úgy kezelni, hogy ilyen esetben előre rögzítsük, hogy 2-2 „hellyel" rendelkeznek a karakterlapon.

A fenti kockázatokat mindenképpen érdemes mérlegelni, és figyelembe venni a szervezeti kultúrát a nagyobb létszámú csoportok esetében.
A játék instruktora lehet külső szakértő, de akár belső információbiztonsági munkatárs is – ehhez összeállítottam egy instruktori képzést is, melynek anyaga kifejezetten a játékvezetési tapasztalatokat és tanácsokat adja át a leendő játékmestereknek.

6.3.4.2. Munkahelyi társasjáték klub

Egyre több szervezetnél találkozhatunk társasjáték klubokkal, melynek tagjai munkaidőt követően társasjátékos eseményeket szerveznek. Ezek a közösségek az eddigi visszajelzések alapján nyitottak a biztonságtudatossági társasjáték elérhetőségének biztosítására, illetve a szervezet információbiztonsági területe is tud ennek mintájára, akár munkaidőben tartott, rendszeres biztonságtudatossági társasjáték eseményeket szervezni. A programok lehetnek instruktor által vezetett játékok, vagy lehet biztosítani a játék használatát, kikölcsönzésének lehetőségét is az érdeklődő munkavállalóknak.

6.3.4.3. Ajándék

Tekintve, hogy a társasjáték akár otthon, a magánéletben is alkalmazható, szórakoztató tudatosító eszköz, a munkáltató akár ajándékként vagy nyereményként is biztosíthatja azt az alkalmazottainak a biztonságtudatossági kampány során. A nyeremény ösztönző jellegű lehet a többi kampányelemen vagy oktatáson való részvétel során, illetve a más jellegű képzéseken tanultak visszaellenőrzésére is hasznos segédeszköz lehet. Ebben az esetben különösen érdekes lehet a 6.3.4.4 pontban bemutatott szervezetre szabási lehetőségek megfontolása.

6.3.4.4. Szervezetre szabhatóság

Annak érdekében, hogy a felhasználók minél inkább magukhoz közelállónak érezzék az átadni kívánt biztonságtudatossági ismereteket, érdemes megfontolni a társasjáték bizonyos mértékben történő szervezetre szabását. Természetesen ezt nem lehet olyan mértékben megoldani, mint például egy szabadulószoba esetén, viszont az alábbi elemeket szervezetspecifikusan meg lehet változtatni:

- szervezeti logó felhelyezése
- játék elnevezése
- biztonságtudatossági ismeret kártyák módosítása, illetve szövegszerű módosítása
- cselekménykártyák módosítása vagy kiegészítése, beleértve a szövegszerű módosításokat is
- új, a szervezetre jellemző karakterek bevezetése

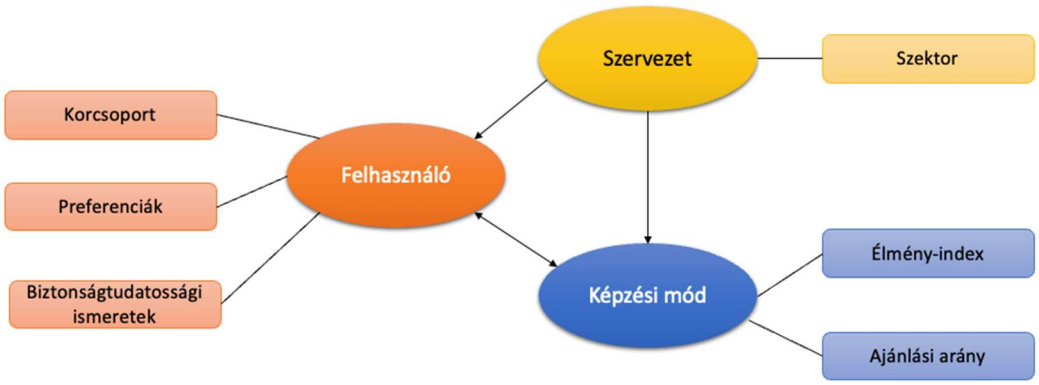
- új, a szervezethez kapcsolódó küldetések bevezetése

Ezen szervezetre szabási lehetőségeket a gyártási költségek miatt elsősorban abban az esetben érdemes megtenni, amennyiben nagyobb példányszámban, például ajándéknak szánjuk azt munkavállalóink részére.

6.4. A DISSZERTÁCIÓHOZ KÉSZÜLT KUTATÁS FELHASZNÁLT ADATAI ÉS EREDMÉNYEI

A biztonságtudatossági társasjáték alkalmazhatóságának vizsgálata során elsődleges forrásként szintén a 3. fejezetben bemutatott kutatás eredményeire támaszkodtam.

A vizsgálat során elsődlegesen a10. ábrán szemléltetett adatokkal dolgoztam:



10. ábra: A kutatásban használt adatok a hipotézis vizsgálata során (forrás: saját szerkesztés)

Az adatok gyűjtése és a kérdőívek kitöltési aránya felhasználói, illetve szervezeti ismérvek vonatkozásában megegyezik a 3. fejezetben bemutatottakkal.

Az egyes képzési módokra vonatkozó kitöltési statisztikákat a 42. táblázat szemlélteti:

Program-típus	K1 kérdőív (db)	K2 kérdőív (db)	K3 kérdőív (db)
E-Learning	42	42	26
Kampány	47	47	31
Online oktatás	49	49	30
Szabadulószoba	48	48	37
Személyes oktatás	50	50	36
Társasjáték	48	48	34
Összesen:	**284**	**284**	**194**

42. táblázat: Kitöltési statisztikák

Ahogyan a gamifikációs programelemek értékelésénél, úgy a társasjáték esetében is az alábbi feltételekhez kötöttem a módszer eredményes alkalmazását:

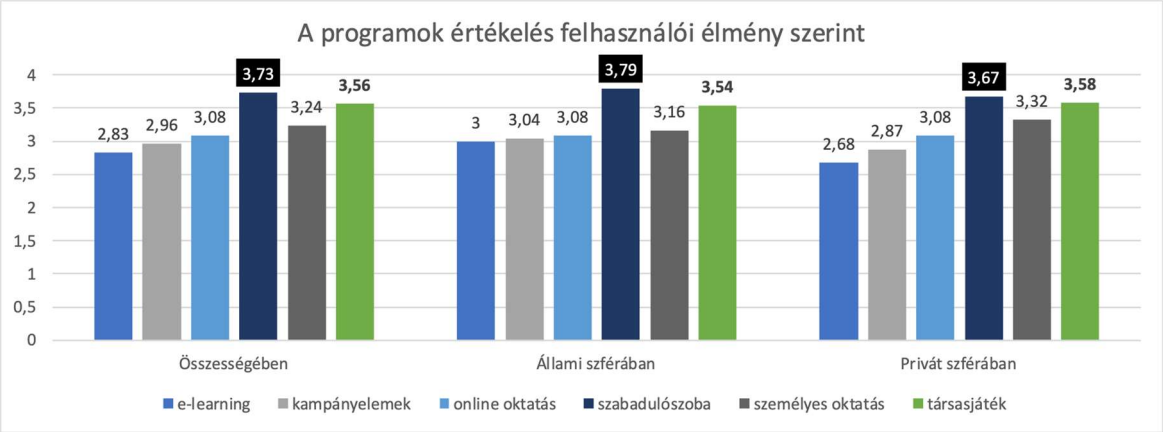
- A felhasználók élvezetesnek tartják a programot.

- A felhasználók preferálják a programot.
- A felhasználók ajánlják a programot.
- A programot követően a résztvevők legalább egy új ismeretet tudnak írni a második kérdőíven (K2).
- A programot követően jelentős mértékben bővülnek a résztvevők biztonságtudatossági ismeretei (K2)
- A programot követően nagymértékben fejlődnek a korábban általánosságban hiányosságként azonosított ismeretek (iratmegsemmisítés, közösségi média, telefon és okos eszközök biztonságtudatos használata).
- A programot követően a résztvevők egy hónappal később (K3) is írnak olyan ismeretet, melyet az első kérdőívben nem rögzítettek, tehát a tudás tartósan megmaradt.
- A személyes tapasztalatok megerősítik a program alkalmazhatóságát.

Fentiek értékelését az alábbiakban mutatom be.

6.4.1. BIZTONSÁGTUDATOSSÁGI TÁRSASJÁTÉK ÉRTÉKELÉSE FELHASZNÁLÓI ÉLMÉNY ALAPJÁN

A disszertáció 3.6 pontjában folytatott vizsgálat alapján megállapítottam, hogy a társasjáték mind az állami, mind a privát szférában a második leginkább élvezetesnek ítélt programelem a szabadulószobát követően (65. diagram).



65. diagram: A biztonságtudatossági társasjáték értékelése felhasználói élmény alapján (élmény-index) (forrás: saját szerkesztés)

Részletes értékelés tekintetében a résztvevők 58,3%-a „*Egyértelműen élvezetes*”-nek értékelte, melyet az alábbi diagram is tükröz. Ez ugyan nem olyan kimagasló eredmény, mint a szabadulószoba esetében, de még mindig inkább a legjobb lehetőség dominált az értékelésben (66. diagram).

66. diagram: A biztonságtudatossági társasjáték részletes értékelése felhasználói élmény alapján (forrás: saját szerkesztés)

Az eredmények alapján elmondható, hogy a felhasználói élmény alapján a biztonságtudatossági társasjáték alkalmazható megoldás munkahelyi környezetben.

6.4.2. A BIZTONSÁGTUDATOSSÁGI TÁRSASJÁTÉK ÉRTÉKELÉSE FELHASZNÁLÓI PREFERENCIA ALAPJÁN

A disszertáció 4.4 pontjában folytatott vizsgálat alapján megállapítottam, hogy a társasjáték a program előtt a 7. legpreferáltabb módszer volt a 10 vizsgált biztonságtudatossági fejlesztési módszer között. A programot követő mérés alapján azonban a 3. legpreferáltabb oktatási módszerré vált.

Az eredmények alapján elmondható, hogy a felhasználói preferencia változása alapján a biztonságtudatossági társasjáték alkalmazható megoldás munkahelyi környezetben.

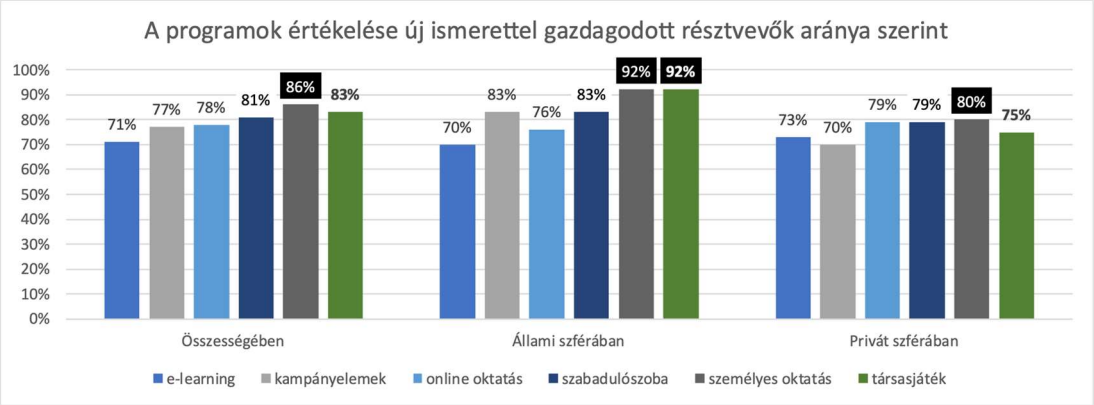
6.4.3. BIZTONSÁGTUDATOSSÁGI TÁRSASJÁTÉK ÉRTÉKELÉSE FELHASZNÁLÓI AJÁNLÁS ALAPJÁN

A disszertáció 4.5 pontjában folytatott vizsgálat alapján megállapítottam, hogy a felhasználók 98%-a ajánlja a programot, ezzel ugyanolyan ajánlási értéket ért el, mint a szabadulószoba. Állami szektorban 100%-kal a leginkább ajánlott megoldás, privát szférában pedig 96%-os ajánlási aránnyal a leginkább ajánlott megoldás.

Az eredmények alapján elmondható, hogy a felhasználói ajánlás alapján a biztonságtudatossági társasjáték alkalmazható megoldás munkahelyi környezetben.

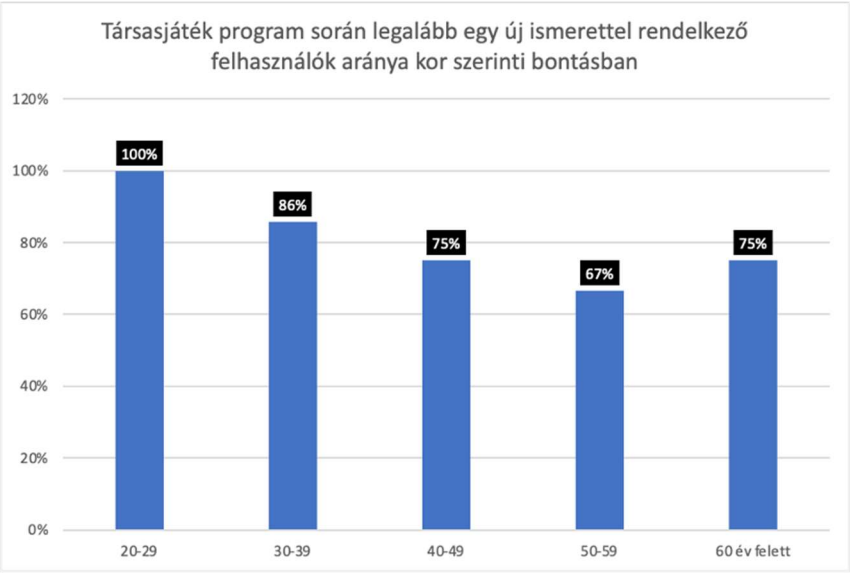
6.4.4. A MÓDSZER HATÉKONYSÁGÁNAK ÉRTÉKELÉSE A BIZTONSÁGTUDATOSABB FELHASZNÁLÓK SZÁMÁNAK NÖVELÉSÉBEN

Hatékonyság szempontjából megnéztem, hogy a társasjáték program hány százalékát fejlesztette a résztvevőinek, azaz a résztvevők hány százaléka írt a programot követő kérdőíven (K2) legalább egy új ismeretet. Ahogyan a 67. diagram is szemlélteti, ezen a téren összességében 2. helyen végzett a személyes oktatás után, állami szférában ezzel holtversenyben az első, míg privát szférában pedig a szabadulószoba és online oktatást követő 3. helyet foglalta el.



67. diagram: A biztonságtudatossági társasjáték hatékonyságának értékelése a legalább 1 db új ismerettel rendelkező résztvevők aránya szerint (forrás: saját szerkesztés)

Kor szerinti bontásban a 68. diagram alapján leginkább a 30 év alatti korcsoport (100%), valamint a 30-39 éves korosztály (86%) profitált belőle és gazdagodott legalább 1 új biztonságtudatossági ismerettel, legkevésbé pedig az 50-59 éves korosztályt érte el, melyet viszont a szabadulószoba jól fejlesztett.



68. diagram: A biztonságtudatossági társasjáték programban résztvevő, legalább 1 db új ismerettel rendelkező felhasználók aránya korosztály szerint (forrás: saját szerkesztés)

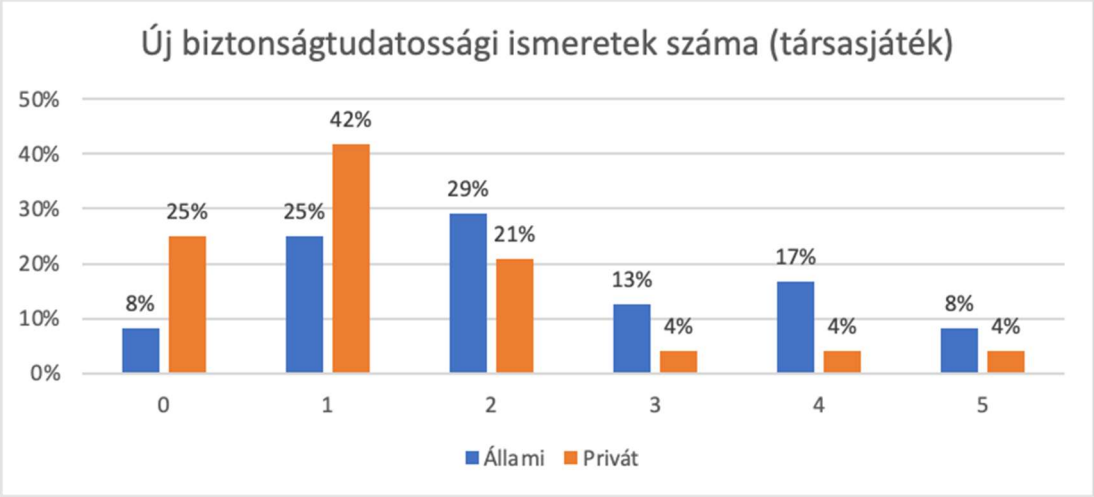
Az eredmények alapján elmondható, hogy a legalább egy új biztonságtudatossági ismeretet szerző felhasználók aránya alapján a biztonságtudatossági társasjáték a 2. legjobb biztonságtudatosságot fejlesztő megoldás, ezáltal képes a biztonságtudatosság fejlesztésére, a több biztonságtudatossági ismerettel rendelkező felhasználók számának növelésére munkahelyi környezetben.

6.4.5. A MÓDSZER HATÉKONYSÁGÁNAK ÉRTÉKELÉSE A BIZTONSÁGTUDATOSSÁGI ISMERETEK SZÁMÁNAK NÖVELÉSÉBEN

A társasjáték programon résztvevők összesen 87 db új ismeretet írtak, ez azt jelenti, hogy minden résztvevő átlagosan 1,81 db ismerettel írt többet a programot követően. Szektor szerinti bontásban ez állami szféra esetében átlag 2,29 db, privát szféra esetében pedig átlag 1,33 db új tudatossági elemet jelent, mely alapján elmondható, hogy a társasjáték alkalmazása az állami szektorban hatékonyabb volt az átadott tudásmennyiség alapján.

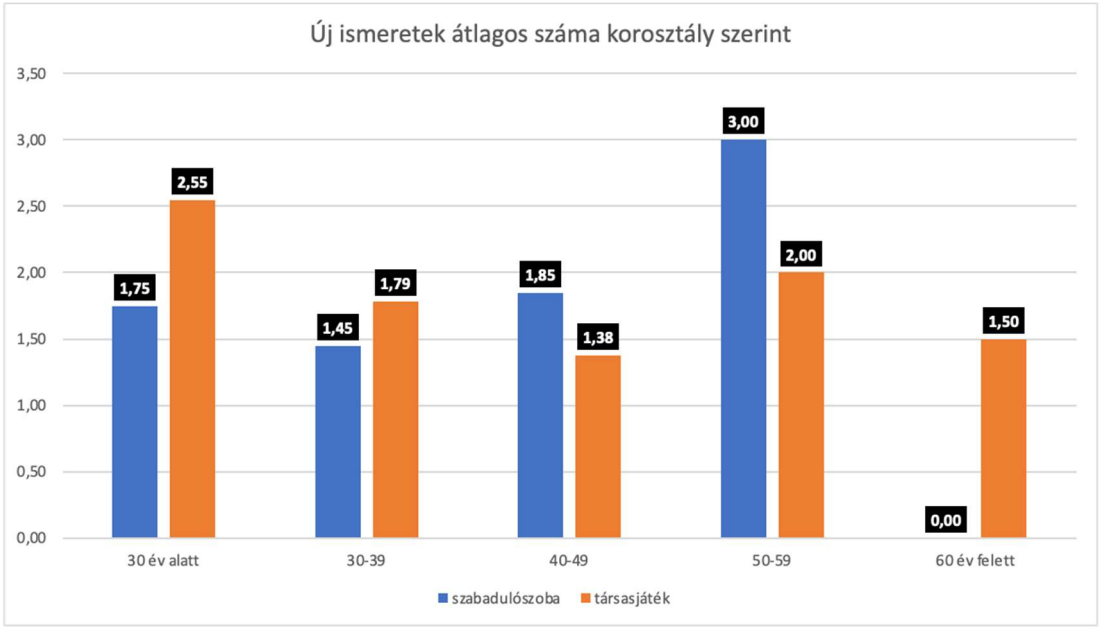
Ez alapján összességében a leghatékonyabb megoldásnak tekinthető a társasjáték, mely az állami szférában szintén az 1., míg privát szférában az az utolsó helyet foglalja el.

A 69. diagram azt szemlélteti, hogy résztvevő felhasználók hány százaléka írt adott mennyiségű új biztonságtudatossági ismeretet szektor szerinti bontásban, mely szintén azt erősíti meg, hogy az állami szféra munkavállalói több ismeretet szereztek.



69. diagram: A biztonságtudatossági társasjáték programban résztvevő felhasználók aránya új ismeretek szerzésének bontásában, szektor szerinti megkülönböztetéssel (forrás: saját szerkesztés)

A korosztály szerinti csoportosítást nézve a 70. diagram alapján megállapítható, hogy az átlagosan legtöbb (2,55 db) ismeretet a 30 év alatti korosztály szerezte a társasjáték program során.

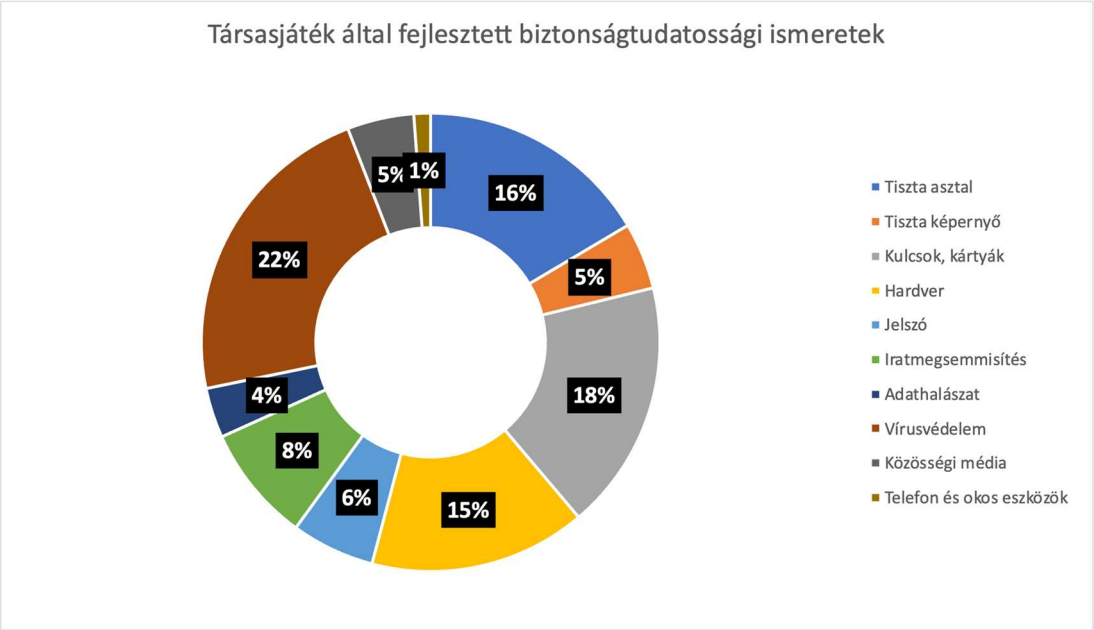


70. diagram: A biztonságtudatossági szabadulószobában és társasjátékon résztvevő felhasználók által szerzett új ismeretek átlaga (db) korosztály szerinti bontásban (forrás: saját szerkesztés)

Az eredmények alapján elmondható, hogy a biztonságtudatossági ismeretek számának növelése alapján a biztonságtudatossági társasjátéknak is megosztó az értékelése szektoronként. Állami szférában ezen vizsgálati pont alapján a társasjáték a leginkább hatékony megoldás, míg privát szektorban a legkevésbé hatékony módszer a tudatossági ismeretek számának növelésére.

6.4.6. A MÓDSZER HATÉKONYSÁGÁNAK ÉRTÉKELÉSE A LEGINKÁBB HIÁNYOSNAK BIZONYULT BIZTONSÁGTUDATOSSÁGI ISMERETEK SZÁMÁNAK NÖVELÉSÉBEN

Az értékelésem egyik szempontja itt is az volt, hogy a korábban legjellemzőbb hiányosságként azonosított ismeretek milyen mértékben fejlődtek. Az alábbi diagram alapján elmondható, hogy a telefon és okos eszközök biztonságtudatos használatát (1%) nagyon alacsony mértékben, az iratmegsemmisítést (8%), mind pedig a közösségi média biztonságtudatos használatát (5%) viszonylag csekély mértékben adta át a program. A felhasználók leginkább a vírusvédelem (22%), kulcsok és kártyák használata (18%) és a tiszta asztal politikával (16%) kapcsolatban szereztek új ismeretet (71. diagram).



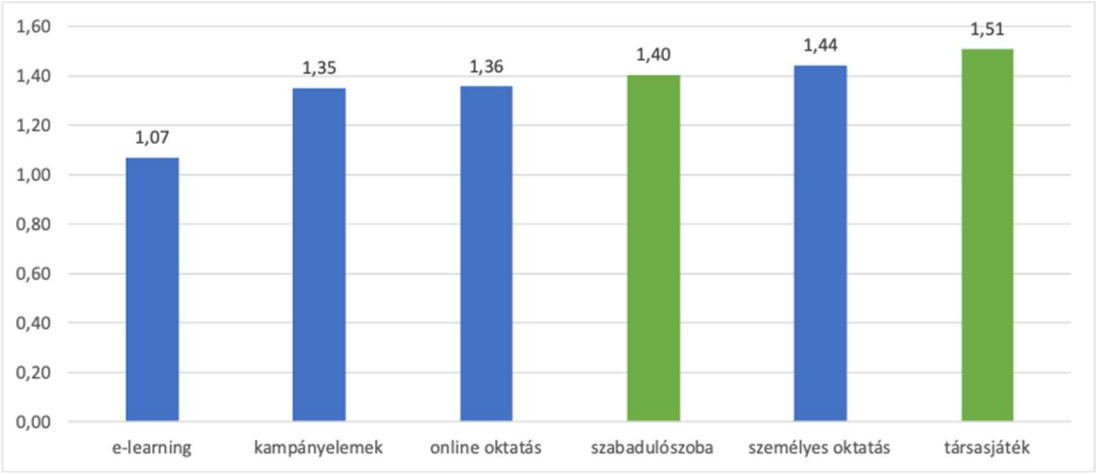
71. diagram: A biztonságtudatossági társasjáték által fejlesztett új ismeretek (forrás: saját szerkesztés)

A fentiek alapján megállapítható, hogy a társasjáték programot követően csak kis mértékben fejlődnek a korábban általánosságban hiányosságként azonosított ismeretek (iratmegsemmisítés, közösségi média, telefon és okos eszközök biztonságtudatos használata). Ez alapján elmondható, hogy a társasjáték jellegéből fakadóan inkább az általános ismeretek bővítését támogatja, tekintve, hogy a cselekménykártya-lapok nem szabhatóak olyan könnyen szervezetre, mint egy szabadulószoba (bár előválogatásuk célirányosan is lehetséges).

6.4.7. HATÉKONYSÁG ÖSSZESÍTETT ÉRTÉKELÉSE KÖZVETLENÜL A PROGRAMON VALÓ RÉSZVÉTELT KÖVETŐEN

A biztonságtudatossági programok hatékonyságát a fentiek szerint abból a szempontból külön értékeltem, hogy hány felhasználó biztonságtudatossági ismereteit növelték legalább egy új ismerettel, illetve milyen mértékben növelték átlagosan az ismeretek számát. Szerettem volna azonban azt is valamilyen módon értékelni, hogy összességében mit lehet mondani, melyik bizonyul a leghatékonyabb oktatási módszernek. Ennek megállapítására az egyes módszerek átlagos új ismereteinek a számának, valamint a legalább egy új ismeretet szerzett felhasználók arányának a szorzatát vettem alapul.

Az eredmények alapján összességében a következő sorrend alakult ki (72. diagram):



72. diagram: A biztonságtudatossági társasjáték hatékonysága az összesített rangsor szerint (összesített hatékonyság-index) (forrás: saját szerkesztés)

Fentiek alapján elmondhatjuk, hogy a biztonságtudatossági társasjáték összességében a legjobb biztonságtudatosságot fejlesztő megoldás, ezáltal képes a biztonságtudatosság fejlesztésére munkahelyi környezetben.

6.4.8. HATÉKONYSÁG ÖSSZESÍTETT ÉRTÉKELÉSE 1 HÓNAPPAL A PROGRAMON VALÓ RÉSZVÉTELT KÖVETŐEN

A biztonságtudatosság fejlesztési programok természetesen akkor hatékonyak, ha a felhasználók nem csak a programot követően, hanem később is emlékeznek a tanultakra, illetve alkalmazni is tudják azokat.

Azt ugyan nem tudtam tesztelni, hogy a tanultakat ténylegesen elsajátították-e készség szinten, és alkalmazzák-e a mindennapokban, a 4. fejezetben leírt vizsgálat során viszont értékeltem a kutatásban résztvevők 1 hónappal a program után kitöltött kérdőíveit.

A társasjáték ennek alapján összességében a résztvevők 79,4%-át fejlesztette legalább egy tudatossági elemmel, és kiemelendő, hogy az állami szektorban a társasjáték program minden résztvevője (100%) tudott írni legalább egy új biztonságtudatossági ismeretet az utolsó kérdőívre (K3) is.

Ismeretek számát tekintve itt is átlag 1,71 db új ismeretet írtak az ezen résztvevő válaszadók, mely ezen a téren szintén a legkevésbé hatékony megoldásnak minősíti a szabadulószoba mellett, az állami szférában azonban 2,36 db átlag új ismerettel a leghatékonyabb megoldás.

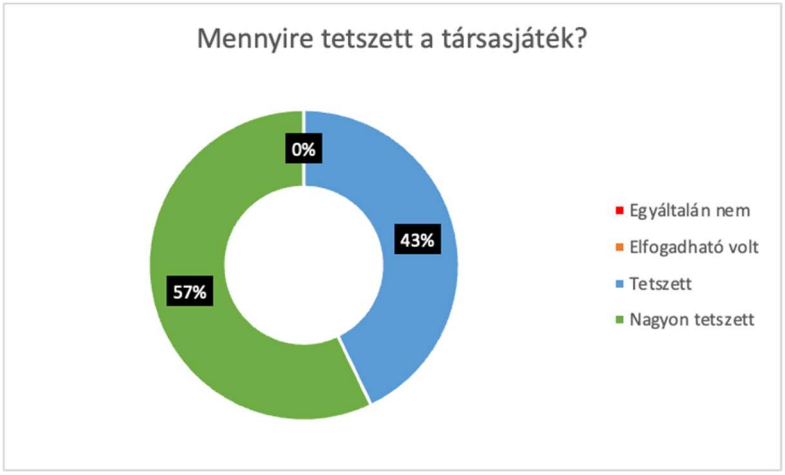
Fentiek alapján elmondhatjuk, hogy a biztonságtudatossági társasjáték tartósan is képes fejleszteni a felhasználók biztonságtudatossági ismereteit és legalább az 1 új ismerettel rendelkező felhasználók számát hatékonyan képes növelni.

6.5. KAPCSOLÓDÓ KIEGÉSZÍTŐ FELMÉRÉS EREDMÉNYEI

A kutatás társasjáték programeleménél egy kiegészítő kérdőívet is alkalmaztam, mely nagyon röviden azt mérte fel, hogy a résztvevőknek mennyire tetszett a játék, illetve, hogy szívesen használnák-e a jövőben, valamint milyen javaslatuk van az esetleges továbbfejlesztéssel kapcsolatban. Ezen kérdőívben nem alkalmaztam nemre, korra, szervezetre vonatkozó megkülönböztetést, ezekkel kapcsolatos statisztikai adatokat csak az elsődleges kutatás során gyűjtöttem és csak annak eredményei alapján értékeltem. A kiegészítő felmérés vonatkozásában ezért ezt elhanyagolhatónak véltem, és a célom inkább a játék továbbfejlesztésének segítése volt.

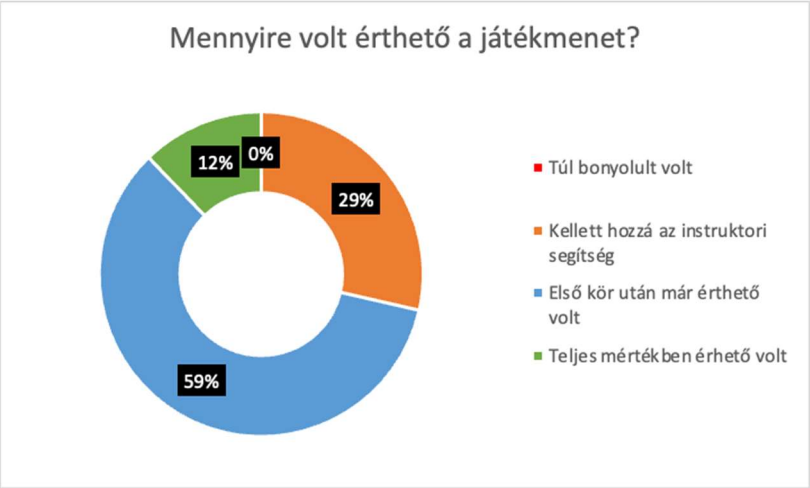
A kérdőívet a résztvevők 100%-a (48 fő) kitöltötte, és az alábbi eredmények születtek.

A társasjáték minden résztvevőnek elnyerte a tetszését, negatív visszajelzés nem érkezett rá (73. diagram).



73. diagram: Mennyire tetszett a résztvevőknek a társasjáték? (forrás: saját szerkesztés)

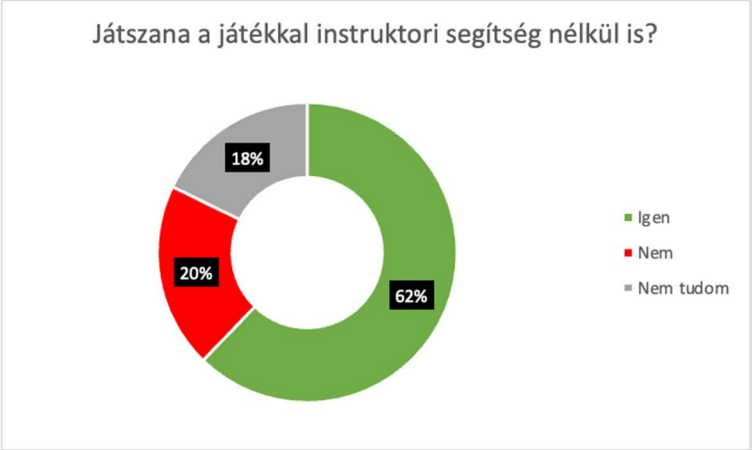
A játékmenet bonyolultsága már megosztóbb volt. Ahogyan a játék fejlesztését bemutató fejezetben leírtam, törekedtem a minél egyszerűbb, a valós munkanaphoz és cselekményekhez leginkább illeszkedő játékmenetet megalkotni, ezt igazolta, hogy egyetlen résztvevő sem jelölte „*túl bonyolult*”-ként a játékmenet érthetőségére vonatkozó kérdést. A válaszadók 29%-a azonban azt nyilatkozta, hogy szerinte kell hozzá az instruktori segítség, és egy játékot követően a résztvevők 12%-a tudta kijelenteni, hogy teljes mértékben értette a játék lépéseit. A többség (59%) egy próbakör után már rájött az alkalmazásra (74. diagram).



74. diagram: Mennyire érthető a résztvevők szerint a játékmenet? (forrás: saját szerkesztés)

A résztvevők 98%-a a 30 perces demót követően szívesen végigjátszaná a teljes játékot a kollégáival, 2%-uk pedig semlegesen „*nem tudom*”-mal nyilatkozott.

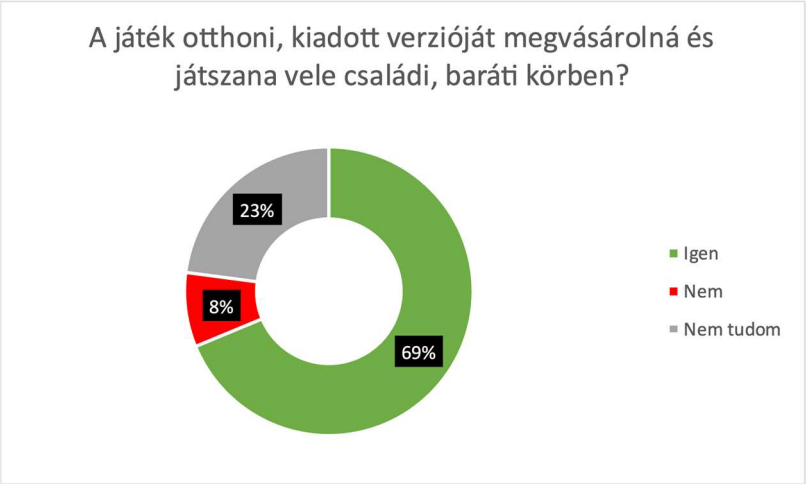
Hogy minél jobban átlássam a használhatóságot, kicsit másképpen is megfogalmaztam a kérdést és rákérdeztem, hogy instruktori segítséggel is szívesen játszanának-e a játékkal. Erre a válaszadók többsége (62%) egyértelműen pozitívan nyilatkozott, és csupán a válaszadók 20%-a zárkózott el egyértelműen az önálló játéktól (75. diagram).



75. diagram: Játszanának-e a résztvevők instruktori segítség nélkül is a játékkal? (forrás: saját szerkesztés)

Mindezek alapján elmondható, hogy a játékmenet fejlesztése sikeres volt és egy, az átlagfelhasználók által is könnyen felhasználható segédeszköz született.

A játék továbbfejlesztésére gondolva még azt a kérdést is feltettem, hogy a játék esetleges otthoni verzióját szívesen megvásárolnák-e a résztvevők, melyre a többség (69%) pozitív választ adott, és csupán a válaszadók 8%-a zárkózott el egyértelműen az otthoni használat igényétől (76. diagram).



76. diagram: Érdeklődés az otthoni verzió iránt (forrás: saját szerkesztés)

A szabadszöveges visszajelzések is nagyon pozitívak voltak:

- Volt olyan felhasználó, aki úgy nyilatkozott „*Nem szeretem a társasjátékokat. Soha nem is játszok. De ez tetszett. :)*”. Ezzel megerősítette, hogy elértem azt a célt, hogy ne pusztán egy társasjáték készüljön, hanem sokkal inkább oktatási módszer.
- Értékelték az oktatási módszert is, illetve a grafikát és kivitelezést többen pozitívumként tüntették fel. („*Köszönet az élvezetes, szokványostól eltérő oktatásért! Remek design, ötletes megoldás*.”)
- Visszajelzések érkeztek arról is, hogy online vagy mobil verzióban is látnának fantáziát – ez kérdőívtől függetlenül is több felhasználó javaslata.
- Egyetlen negatívumként feltüntetett komment a kivédhetetlen támadások beépítése volt, melyet azonban a fejlesztés során zajló tesztek indukáltak, így ezen a továbbiakban nem változtatok.

A felhasználói visszajelzések alapján a játék fejlesztése elérte célját, és megerősített abban, hogy a további fejlesztésekre, melyeket a 6.3.1.8 pontban is bemutattam, van igény.

6.6. SZEMÉLYES TAPASZTALATOK AZ ALKALMAZÁS SORÁN

Az általam kialakított biztonságtudatossági társasjátékkal, illetve vezetett programokkal kapcsolatos visszajelzések, valamint a fentieken túl szerzett tapasztalatok az alábbiakkal járultak hozzá az értékeléshez:

- Több szervezet információbiztonsági munkatársa is megjegyzete, hogy nagyon pozitív visszhangja volt a biztonságtudatossági társasjáték programnak és a munkavállalóknak kifejezetten tetszett a megoldás.
- A társasjátékot több szervezet is megvásárolta instruktori képzéssel, mellyel célja, hogy rendszeres biztonságtudatossági programot biztosítson a játék használatával munkavállalóinak.
- A játékot bár 6 főre terveztem, és személyesen nem láttam értelmét, így nem is preferáltam, hogy többen vegyenek részt benne (például egy karaktert egyszere két játékos irányítson), azonban volt szervezet, mely a kutatástól függetlenül ezt az elgondolásomat megdöntötte, és a résztvevők hatékonyan játszottak párosával is egy-egy karakter képviselésében.
- A társasjáték iránt magánszemélyek is nagymértékben érdeklődnek, bár számukra optimálisabb lenne egy kisebb méretű, otthoni témakörökre szűkített, kedvezőbb árú megoldás.
- Több játékoscsoport már rögtön a demó programot követően megkérdezte, hogy mikor lesz a következő alkalom, és több résztvevő külön is megkeresett a várható következő lehetőséggel kapcsolatban.
- A szabadulószobához hasonlóan a társasjáték tapasztalatait sokszor felemlegetik a résztvevők a mindennapokban is (például vírusvédelem működése, talált pendrive, elvesztett eszköz, „visszaellenőrzés” kártya).
- Több résztvevő később rám, mint instruktorra, úgy is emlékezett, hogy teljesen külsősként vezettem a játékot.
- A játékosok visszajelzései alapján a játékban szereplő események tényleg a való életet tükrözik, így a biztonságtudatosság fontossága megfelelően demonstrálható.
- A szerencsefaktor során bekövetkezett kivédhetetlen támadások vagy negatív értékelések nem kedvtelenítik el a játékosokat, inkább motiválják őket az ismételt játékokra.
- A kutatás utolsó (K3) kérdőívének társasjáték programban résztvevő válaszadóinak egy része szintén láthatóan követte azt a gyakorlatot, hogy annak mentén rögzítette biztonságtudatossági ismereteit, hogy milyen ismereteket alkalmaztak vagy milyen cselekménykártyák voltak a játék során. (Volt olyan résztvevő, aki a tudatossági elem kártyák címszavait szó szerint tudta idézni a felsorolás során.)

Fentiek alapján elmondhatom, hogy a biztonságtudatossági társasjáték nagymértékben elnyerte a felhasználók tetszését és nyitottak ezen új megoldás alkalmazására. Emellett a visszajelzések azt is alátámasztják, hogy a résztvevők tényleg tanulnak a programokból, és saját bevallásuk szerint alkalmaznak is ott bemutatott eszközöket, ismereteket.

6.7. LEVONT KÖVETKEZTETÉSEK

A fejezetben két felmérésem és gyakorlati tapasztalataim felhasználásával bizonyítottam azt a hipotézist, miszerint *„Egy újszerű, általam fejlesztett 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 hipotézis igazolására a saját fejlesztésű biztonságtudatossági társasjátékomat, mint instruktor által vezetett programot vontam be a kutatásba, melynek kialakítását és alkalmazását jelen fejezetben részletesen bemutattam.

A kutatás eredményei alapján a következő megállapításokat tettem és alábbi következtetéseket vontam le:

- Az eredmények alapján elmondható, hogy a felhasználói élmény értékelése szerint a biztonságtudatossági társasjáték alkalmazható megoldás munkahelyi környezetben, mert a válaszadók 98%-a élvezetesnek, ezen belül is 58,3%-a kifejezetten élvezetesnek tartotta azt a részvételt követően.
- Az eredmények bemutatták, hogy a felhasználók a programokon való részvételt követően sokkal inkább preferálták a társasjátékot, mely a rangsorban a 7. helyről a 3. helyre lépett elő.
- Az eredmények alapján elmondható, hogy a résztvevő felhasználók átlag 98%-a ajánlja a programot, mely alapján ismételten elmondhatjuk, hogy a biztonságtudatossági társasjáték alkalmazható megoldás munkahelyi környezetben.
- 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, a több biztonságtudatossági ismerettel rendelkező felhasználók számának növelésére munkahelyi környezetben.
- Az eredmények alapján a társasjáték érzékenyítés céljából a 30 év alattiak, illetve a 30-39 éves korosztály számára a leghatékonyabb.

- Az eredmények alapján elmondható, hogy a biztonságtudatossági ismeretek számának növelése alapján a biztonságtudatossági társasjátéknak is megosztó az értékelése szektoronként. Állami szférában ezen vizsgálati pont alapján a leghatékonyabb az alkalmazása, míg privát szektorban a legkevésbé hatékony megoldás a tudatossági ismeretek számának növelésére.
- A fentiek alapján elmondható, hogy a társasjáték programot követően csak kis mértékben, de fejlődnek a korábban általánosságban hiányosságként azonosított ismeretek (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.
- Összesített eredmények alapján elmondhatom, hogy a biztonságtudatossági társasjáték összességében a legjobb biztonságtudatosságot fejlesztő megoldás, melynek használata elsősorban az állami szférában előnyös.
- Az egy hónappal későbbi visszamérés eredménye alapján elmondhatjuk, hogy a biztonságtudatossági szabadulószoba tartósan is képes fejleszteni a felhasználók biztonságtudatossági ismereteit és legalább az 1 új ismerettel rendelkező felhasználók számát hatékonyan képes növelni (ez az érték a kutatás során 79,4% volt).
- A kiegészítő felmérés eredményei alapján a felhasználók szívesen játszanak a játékkal, és a játékmenetet sem tartják túl bonyolultnak, valamint az otthoni iránt is érdeklődnek.
- Saját személyes tapasztalataim is megerősítették, hogy a biztonságtudatossági társasjáték nagymértékben elnyerte a felhasználók tetszését és nyitottak ezen új megoldás alkalmazására. Emellett a visszajelzések azt is alátámasztják, hogy a résztvevők tényleg tanulnak a programokból, és saját bevallásuk szerint alkalmaznak is ott bemutatott eszközöket, ismereteket.

Az előzetesen meghatározott szempontrendszerem szerinti értékelés eredményeit a 43. táblázatban foglaltam össze.

Szempont	*Értékelés*
A felhasználók élvezetesnek tartják a programot.	IGAZ
A felhasználók preferálják a programot.	IGAZ
A felhasználók ajánlják a programot.	IGAZ
A programot követően a résztvevők legalább egy új ismeretet tudnak írni a második kérdőíven (K2).	IGAZ
A programot követően jelentős mértékben bővülnek a résztvevők biztonságtudatossági ismeretei (K2)	RÉSZBEN IGAZ
A programot követően nagymértékben fejlődnek a korábban általánosságban hiányosságként azonosított ismeretek (iratmegsemmisítés, közösségi média, telefon és okos eszközök biztonságtudatos használata).	NEM IGAZ
A programot követően a résztvevők egy hónappal később (K3) is írnak olyan ismeretet, melyet a program előtt nem, tehát a tudás tartósan megmaradt.	IGAZ
A személyes tapasztalatok megerősítik a program alkalmazhatóságát	IGAZ

43. táblázat: Összefoglaló táblázat a biztonságtudatossági társasjáték értékeléséről (forrás: saját szerkesztés)

A kutatással bizonyítottam, 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. A módszer a vizsgálatba bevont biztonságtudatosságot fejlesztő módszerek hatékonyság szerinti összesített értékelése során a legjobb megoldásnak bizonyul, és az eredmények alapján inkább az állami szektor szervezetei számára jelenti a leghatékonyabb megoldást. Ezen túlmenően megállapítottam, hogy a társasjáték hosszútávon, bár nem a leghatékonyabban, de képes a biztonságtudatossági ismeretek fejlesztésére.

7. ÖSSZEGZÉS

7.1. MEGÁLLAPÍTÁSOK ÉS KÖVETKEZTETÉSEK

Disszertációmban célul tűztem ki annak vizsgálatát, hogy az élmény alapú biztonságtudatosságot fejlesztő módszerek, azon belül is a gamifikációs megoldások milyen hatékonysággal képesek a felhasználók információbiztonsági ismereteit bővíteni. Kialakítottam továbbá két gamifikációs megoldást, melyet a munkám során is aktívan alkalmazok a felhasználók biztonságtudatossági edukálására, érzékenyítésére, a disszertációhoz készült kutatásban ezen eszközök hatékonyságának igazolása is célom volt.

A szakirodalom feltárás során megállapítottam, hogy a legtöbb hazai szervezet számára valamilyen jogszabály előírja a biztonságtudatosság fejlesztésének szükségességét, ezek azonban minimális követelményeket tartalmaznak, az oktatások módjára nem alkalmaznak semmilyen kitételt. Emellett, bár a gamifikációs biztonságtudatosság-fejlesztő megoldások nemzetközi szinten elterjedtek, hazai viszonylatban pedig egyre inkább megjelennek legalább vizsgálat, illetve szolgáltatások szintjén a feltárt források alapján, ezek alkalmazására azonban egységes módszertan vagy segédanyag a hivatkozott publikációkon túl nem áll rendelkezésre. Látható azonban, hogy a gamifikációs lehetőségekre, azon belül is elsődlegesen a játék-alapú megközelítésekre, vagy komoly játékokra számos szolgáltatás és termék lelhető fel a piacon.

A gamifikáció alkalmazása azonban hazai viszonylatban még mindig vet fel kérdéseket azok munkakörnyezetben történő alkalmazhatóságával, illetve hatékonyságával kapcsolatban. Ugyan a szakirodalom feltárásban hivatkozott szerzők mindegyike azonosítja a játékosított módszerek előnyeit, és alkalmazhatónak véli azokat a biztonságtudatossági fejlesztések során, illetve nemzetközi szinten készültek a különböző biztonságtudatosságot fejlesztő oktatási módszerek hatékonyságát vizsgáló tanulmányok, ezek többsége, bár pozitívan értékeli a játékosítást, de nagyon eltérő eredményeket és megállapításokat mutat. Hazai viszonylatban nem tártam fel olyan forrást, mely kifejezetten Magyarországon vizsgálná a különböző biztonságtudatosság-fejlesztési módszerek, köztük a gamifikációs megoldások hatékonyságát, emellett a vizsgált szervezetek munkavállalói által adott válaszok alapján is megállapítottam, hogy a gamifikációs módszerek hazánkban még nem terjedtek el a biztonságtudatosságot fejlesztő módszerek között. Mindezek miatt szükségesnek láttam egy saját felmérés készítését a témában, mely legalább a Kirkpatrick-modell *Reakció* és *Tanulás* szintjén képes a vizsgált megoldások alkalmazhatóságának és hatékonyságának igazolására.

Az általam kialakított, a disszertáció 3. fejezetében részletesen bemutatott felmérési módszer azon túl, hogy a felhasználók biztonságtudatossági ismereteinek bővülését mérte, lehetővé tette az egyes, vizsgálatba bevont képzés-típusok értékelését felhasználói preferencia, élvezetesség és hasznosság vonatkozásában is.

A kutatás során megállapítottam, hogy az előzetes felhasználói preferencia nem befolyásolja a képzés hatékonyságát. Ebből kifolyólag azok a munkavállalók, akik előzetesen nem preferált képzésen vesznek részt, nagy valószínűséggel nem fognak kevesebb ismeretet szerezni, illetve a preferált képzésen résztvevők esetében sem számíthatunk kiemelkedő fejlődésre. Így a képzések tervezésére ne a felhasználói preferencia legyen az elsődleges szempontunk. Ahogyan az első hipotézisem igazolása során is vizsgáltam, a felhasználói élmény viszont már befolyásolni tudja egy biztonságtudatossági program hatékonyságát és az ott megszerzett ismeretek mennyiségét, valamint a biztonságtudatosabbnak mondható felhasználók számát. Az eredmények alapján feltételezhető, hogy akik olyan programon vesznek részt, melyet élveznek, nagyobb valószínűséggel tanulnak is a képzés során, mint akik kevésbé élvezetes oktatásban részesülnek. Emellett megvizsgáltam azt is, hogy az, hogy a felhasználók mennyire vélik hasznosnak a képzési módszert, szintén nem befolyásolja jelentős mértékben a biztonságtudatosságuk fejlődését. A preferencia, élmény és hasznosság közül legnagyobb befolyásoló ereje a felhasználói élménynek van. Ebből kifolyólag érdemes olyan programelemet is beillesztenünk a biztonságtudatossági fejlesztésekbe, mely magasabb felhasználói élményt nyújt.

A képzések által nyújtott felhasználói élmény értékelése és a biztonságtudatossági ismeretekkel gazdagodott résztvevők aránya között mind összességében, mind az állami és privát szféra esetében szoros pozitív kapcsolatot azonosítottam, tehát az élvezetesebb programok elsősorban érzékenyítésre, több felhasználó elérésére alkalmasak. Ezzel szemben a felhasználói élmény értékelése és az új ismeretek számának bővülése között már jóval gyengébb a kapcsolat, tehát az élvezetesebb programok minimális szinten ugyan, de pozitív irányba befolyásolják a megszerzett ismeretek számának gyarapodását, tehát aki élvezetesebb programon vesz részt, valószínűleg minimális mértékben, de többet tanul. Mindezek alapján elmondhatom, hogy amennyiben az a szervezet, vagy oktatás célja, hogy minél több felhasználót érjen el és érzékenyítsen a témában, esetleg konkrét, szűkebb témakörben szeretne információbiztonsági ismereteket átadni, érdemes megvizsgálnia például kulcsfelhasználók bevonásával, hogy mely biztonságtudatosságot fokozó programok milyen élvezeti értékkel bírnak a munkavállalóink körében és aszerint kiválasztani az alkalmazott módszereket. Mindezek mellett természetesen továbbra is fenntartom, hogy érdemes több különböző programot is alkalmazni, mert ahogyan

a kutatásban is bemutatom, hatékonyság szempontjából nagyon különböző értékekkel bírnak az egyes módszerek akár csak szektor szerinti bontásban is.

A kutatás során egyértelműen igazolódott, hogy a gamifikációs módszerek bizonyultak a legmagasabb felhasználói élményt nyújtó képzési megoldásoknak, a felhasználók a programon való részvételt követően inkább a gamifikációs lehetőségeket részesítenék előnyben, miszerint a játékosított módszerek alkalmazásának van igénye és létjogosultsága munkahelyi környezetben a biztonságtudatosság fejlesztése céljából. Vizsgálataim azt is alátámasztották, hogy a gamifikációs módszereket minden szervezetnél, annak jellegétől, méretétől függetlenül lehet alkalmazni, illetve a munkavállalók korosztálya és neme szerinti bontásban is bármely munkavállalói réteg számára alkalmazható lehet a játékosítás, sőt a válaszadók szektortól, szervezeti mérettől, korosztálytól és nemtől függetlenül ajánlják a gamifikációs módszerek alkalmazását - még azon résztvevők is, akik egyébként negatívan értékelték a programot felhasználói élmény szempontjából. Az eredményeim alapján ki lehet zárni azon tévhiteket, miszerint ezek a módszerek szűkebb felhasználói réteg elérésére lehetnek alkalmasak.

Hatékonyság tekintetében a felmérésem alapján a gamifikációs módszerek közvetlenül a programban való részvételt követően összességében legalább olyan hatékonyan képesek a biztonságtudatossági ismeretek átadására azok számosságának növelése szempontjából, valamint rövid távon jobban teljesítenek a biztonságtudatosabb felhasználók számának növelésében, mint az egyéb hagyományos oktatási formák, így alkalmazásuk megalapozott nem csak a felhasználók pozitív értékelése miatt. Ugyan a vizsgálatom hosszútávon azt bizonyította, hogy általánosságban az előadás jellegű, akár online vagy személyesen tartott programok fejlesztik a legtöbb felhasználó biztonságtudatossági ismereteit, kiegészítésként érdemes azonban alkalmazni gamifikációs lehetőségeket is, hiszen alábontva a módszereket, illetve szektor szerinti hatékonyságot vizsgálva látható, hogy az állami szférában a társasjáték, a privát szektorban pedig a szabadulószoba jelenthet hatékony kiegészítő megoldást hosszú távon is. A különböző távlatokon elért vizsgálati eredmények alapján érdemes megfontolni a biztonságtudatossági programok tervezése esetén a vegyes programelemek alkalmazását, és mind rövid, mind hosszútávon fejlesztő megoldásokat alkalmazni. Tekintve az eredmények során azonosított jelentős különbségeket az egyes gamifikációs módszerek között (állami szektorban a társasjáték, privát szférában pedig a szabadulószoba bizonyul hatékonyabbnak), kulcsfelhasználók bevonásával érdemes vizsgálni a különböző játékosított módszereket, és a szervezet számára legideálisabbat kiválasztani.

Kutatásom során külön kitértem a két, általtam fejlesztett gamifikációs megoldás, az 5. fejezetben bemutatott biztonságtudatossági szabadulószoba, valamint a 6. fejezetben ismertetett

társasjáték hatékonyságának vizsgálatára is. Ezekhez általános tapasztalataim, megfigyeléseim mellett korábbi, illetve más kiegészítő felméréseimet is segítségül hívtam. Ezek alapján megállapítottam, hogy a két módszernek egyaránt pozitív fogadtatása van, a felhasználók többsége üdvözítően fogadja lehetőséget, és nyitott az új megoldások alkalmazásának irányába.
Az eredmények alapján elmondható, hogy a felhasználói élmény értékelése szerint a biztonságtudatossági szabadulószoba és a társasjáték is alkalmazható megoldás munkahelyi környezetben, mert a válaszadók 98%-a mindkettő esetében élvezetesnek tartotta azokat, ezen belül is a résztvevők többsége kifejezetten élvezetesnek értékelte a programot követő kérdőíven.
Az eredmények azt mutatták, hogy a felhasználók a programokon való részvételt követően átrendezték a módszerek közötti preferencia sorrendet, és sokkal inkább elmozdultak a gamifikációs lehetőségek irányába, ezt az is igazolja, hogy mindkét módszert a résztvevők átlag 98%-a ajánlaná más felhasználóknak is, mely a legmagasabb értékelés a vizsgált programok között.
A hatékonyságot vizsgáló eredmények alapján elmondható, hogy a biztonságtudatossági ismeretek számának növelése szempontjából mind a biztonságtudatossági szabadulószobának, mind a társasjátéknak nagyon megosztó az értékelése szektoronkénti bontásban. Állami szférában a társasjáték, míg privát szektorban a biztonságtudatossági szabadulószoba bizonyult ezen a téren a leghatékonyabb megoldásnak. A legalább egy új biztonságtudatossági ismeretet szerző felhasználók aránya alapján a személyes oktatást követően a társasjáték, majd a biztonságtudatossági szabadulószoba a legjobb biztonságtudatosságot fejlesztő megoldás, ezáltal hatékonyan képes a biztonságtudatosság fejlesztésére, a több biztonságtudatossági ismerettel rendelkező felhasználók számának növelésére munkahelyi környezetben.
Ezen belül az eredmények azt tükrözik, hogy a szabadulószoba érzékenyítés céljából az 50-59 éves korosztály, illetve a 30 év alattiak körében a leghatékonyabb, míg a társasjáték a 30 év alattiak, illetve a 30-39 éves korosztály esetében teljesített legjobban.
Annak vizsgálata során, hogy melyik módszer mennyire képes hosszútávon is fenntartani az ismereteket, ugyan mind a biztonságtudatossági szabadulószoba, mind a társasjáték lecsúsztak a „dobogóról”, de még így is igazolták, hogy képesek a biztonságtudatossági ismeretek bővítésére, még ha összességében alacsonyabb hatásfokkal is, mint a hagyományos oktatási módszerek.

7.2. 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, 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 hipotézist, 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 bizonyítottam, hogy az általam 2014-ben fejlesztett biztonságtudatossági szabadulószoba, mint újszerű biztonságtudatosság fejlesztési megoldás, képes a biztonságtudatossági szint fejlesztésére mind az ismeretek bővítése, mind a biztonságtudatosabb felhasználók számának növelése szempontjából.**
(Az eredmények korábban részlegesen publikálásra kerültek: Oroszi, 2017; Oroszi, 2019; Oroszi, 2020a; Oroszi, 2020c)

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 bizonyítottam, hogy az általam 2021-2022-ben fejlesztett biztonságtudatossági társasjáték, mint újszerű biztonságtudatosság fejlesztési megoldás, képes a biztonságtudatossági szint fejlesztésére mind az ismeretek bővítése, mind a biztonságtudatosabb felhasználók számának növelése szempontjából.**
(Az eredmények korábban részlegesen publikálásra kerültek: Oroszi, 2021b; Oroszi, 2022; Oroszi, 2023)

7.3. 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 a kutatásom eredményei szerint rövid távon kiemelkedően hatékonynak bizonyult, hosszabb távon azonban, bár 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 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 bemutatott felmérés módszere is nagy segítséget nyújthat.

A disszertációhoz készített kutatás számomra is nagyon érdekes és tanulságos eredményekkel szolgált, melyek mentén a következő továbbfejlesztéseket tervezem:

- 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 a minta-nagyság miatt nem volt rá lehetőség, de érdekes lehet annak vizsgálata is, hogy a gyakorlatban 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 6.3.1.8 alfejezetben bemutatott továbbfejlesztési lehetőségeknek, a meglevő játék tökéletesítésének, illetve kiegészítőkkel való ellátásának, valamint specializáltabb (otthoni, illetve menedzsmentnek szóló) változatok kialakításának.

8. KÖSZÖNETNYILVÁNÍTÁS

Mindenekelőtt köszönettel tartozom **Ale Évának**, az ÁNTK Közigazgatás-Tudományi Doktori Iskola Főreferensének, aki precíz munkájával, megértő, türelmes támogatásával segített eligazodni a doktori iskola követelményei között, és nagymértékben hozzájárult, hogy ez a disszertáció elkészülhessen.

Köszönettel tartozom **a kutatásba bevont tíz szervezet információbiztonsági munkatársainak**, akik támogatták a disszertációhoz kapcsolódó felmérések lefolytatását, az események megszervezését, valamint természetesen azon önként jelentkező, vagy delegált **kollégáiknak**, akik idejüket áldozták a programokon való részvételre, illetve a kérdőívek kitöltésére.

Ezúton is köszönöm az általam fejlesztett biztonságtudatossági **társasjáték tesztelőinek** munkáját, ötleteit, észrevételeit!

Köszönöm a **Silent Signal Kft.** csapatának a társasjáték elkészülésének szakmai támogatását, kivitelezését, kiadását, melynek köszönhetően ez a játék nem maradt meg a koncepció szintjén, és egy bárki által elérhető élmény alapú oktatási eszközzé vált.

Külön köszönettel tartozom minden, **információbiztonsági szakmában elhelyezkedő kollégának**, aki iránymutatásával, ötletével, támogatásával segítette a disszertációm elkészítését.

Végül, de nem utolsó sorban külön köszönettel tartozom **Anyukámnak,** aki nagy mértékben biztosította a disszertáció megírásához szükséges nyugodt körülményeket.

9. IRODALOMJEGYZÉK

9.1. KÖNYVEK ÉS FOLYÓIRATCIKKEK

ABAWAJY, J.: *User preference of cyber security awareness delivery methods*. - In. Behaviour & Information Technology, 2014, Vol. 33, No. 3, p. 236–247,

ALDAWOOD, H., SKINNER, G.: *Reviewing Cyber Security Social Engineering Training and Awareness Programs – Pitfalls and Ongoing Issues*. - In. Future Internet, 2019, Vol. 11, No. 3., p. 16.

ALHABRI, A., ALOTAIBI, A., ALGHOFAILI, L., ALSALAMAH, M., ALWASIL, N., ELKHEDIRI, S.: *Security in Social-Media: Awareness of phishing attacks techniques and Countermeasures.* – In. 2022 2nd International Conference on Computing and Information Technology (ICCIT), Tabuk, Saudi Arabia, 2022, p. 10-16.

ALHASHMI, A. A., DAREM, A., ABAWAJY, J.: *Taxonomy of Cybersecurity Awareness Delivery Methods: A Countermeasure for Phishing Threats*. - In. International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 12, No. 10, 2021, p. 29-35.

ANADEA: *How Gamification in the Workplace Impacts Employee Productivity*, 2018 (https://medium.com/swlh/how-gamification-in-the-workplace-impacts-employee-productivity-a4e8add048e6, utolsó elérés: 2020.02.26)

BÁLITY, Cs., CSERHÁTI, Z., LÁM, J., PALICZ, T., SAFADI, H: *Humán szolgáltatások képzési programjainak értékelési rendszere.* - In. IME – Interdiszciplináris Magyar Egészségügy, XIX. évfolyam, 3. szám, 2020. augusztus – szeptember, p. 9-14.

BÁNYÁSZ P., BÓTA, B., CSABA, Z.: *A social engineering jelentette veszélyek napjainkban.* - In. Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében, Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat, Budapest, p. 12-37. ISBN 9786158056793

BARANOWSKI, T., CULLEN, K. W., NICKLAS T., THOMPSON, D., BARANOWSKI, J.: *Are current health behavioral change models helpful in gui- ding prevention of weight gain efforts?* - In. Obesity Research Volume 11, Issue S10, Special Issue: Obesity, Lifestile, and Weight Management, 2003 October, p. 23–43.

BECKERS, K., PAPE, S.: *A Serious Game for Eliciting Social Engineering Security Requirements*. – In. IEEE 24th International Requirements Engineering Conference, 2016

BEGUIN, E., BESNARD, S., CROS, A., JOANNES, B., LECLERC-ISTRIA, O., et al.: *Computer-Security-Oriented Escape Room*. - In. IEEE Security and Privacy Magazine, Institute of Electrical and Electronics Engineers, 2019, 17 (4), p. 78-83.

BELÁZ, A.: *A közigazgatás információbiztonság: megjósolhatók az incidensek?* – In. Hadtudomány, 2019, 3, p. 92-104.

BHARDWAJ, J.: *Design of a game for cybersecurity awareness*. North Dakota State University, 2019

BORREGO, C., FERNÁNDEZ, C., BLANES, I., ROBLES, S.: *Room escape at class: Escape games activities to facilitate the motivation and learning in computer science.* - In. Journal of Technology and Science Education. 2017, 7, p. 162–171

BURKE, Brian.: *Gamify: How Gamification Motivates People to Do Extraordinary Things*. - Gartner, 2014

CANOVA, G., VOLKAMER, M., BERGMANN, C., & BORZA, R.: *NoPhish: An Anti-Phishing Education App*. - In. International Workshop on Security and Trust Management, 2014 September

CHAPPLE, M., STEWART, J. M., GIBSON, D.: *CISSP Certified Information Systems Security Professional Official Study Guide.* – Sybex, 2021

CHEN, S. L., MICHAEL, D. R.: *Serious games: Games that educate, train, and inform*. - In. Muska & Lipman/Premier-Trade, 2005, p. 17.

CHITRA, A. P., RAJ, M. A.: *E-Learning*. - In. Journal of Applied and Advanced Research, 2018, 3(Suppl. 1) p. 11-13.

CIAMPA, M.: *A comparison of password feedback mechanisms and their impact on password entropy*. - In. Information Management & Computer Security, 2013, 21. évfolyam, 5. szám, p. 344-359.

CLARKE, S. J., PEEL, D. J., ARNAB, S., MORINI, L., KEEGAN, H., WOOD, O. *EscapED: A Framework for Creating Educational Escape Rooms and Interactive Games to For Higher/Further Education.* - In. International Journal of Serious Games, 2017, 4. évfolyam, 3. szám, p. 73-86.

COOK, A., SMITH, R., MAGLARAS, L., JANICKE, H.: *Using Gamification to Raise Awareness of Cyber Threats to Critical National Infrastructure.* - In. 4th International Symposium for ICS & SCADA Cyber Security Research (ICS-CSR 2016), Belfast, 2016

DEÁK, V.: *A social engineering humán alapú támadási technikái*. - In. Biztonságpolitika.hu, 2017, p. 11.

DEÁK, V.: *Kártékony programok terjedése social engineering technikákon keresztül.* - In. Hadmérnök, 2019, 14. évfolyam, 2. szám, p. 256-271. ISSN 1788-1919

DENNING, T., LERNER, A., SHOSTACK, A., KOHNO, T.: *Control-Alt-Hack: The Design and Evaluation of a Card Game for Computer Security Awareness and Education.* - In. CCS '13: Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, 2013, p. 915–928.

DJAOUTI, D., ALVAREZ, J., JESSEL, J.P.: *Classifying Serious Games: the G/P/S model*. - In. Handbook of Research on Improving Learning and Motivation through Educational Games: Multidisciplinary Approaches, IGI-Global, 2011, p. 19., ISBN 9781609604950

DE PASQUALE, F.: *63 Terrifying Cyber Security Statistics from 2022.* – Tekspace, 2023 (https://www.tekspace.com.au/blog/cyber-security-stats-2022/, utolsó elérés: 2023.06.30)

DURUGY, A.: *A T-csoportos módszerre támaszkodó készségfejlesztés eredményességének vizsgálata*, Doktori (PhD) értekezés, Szent István Egyetem, Gödöllő, 2019

FINDLAY, J.: *Game-Based Learning vs. Gamification: Do You Know the Difference?*,2016 (https://trainingindustry.com/articles/learning-technologies/game-based-learning-vs-gamification-do-you-know-the-difference/, utolsó elérés: 2021.08.08)

FISHBEIN, Martin, AJZEN, I.: *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. - Addison-Wesley, 1975

DE FRIETAS, S., LIAROKAPIS, F.: *Serious Games: A New Paradigm for Education?* - In. Serious Games and Edutainment Applications. Springer, 2011., p. 9-23.

FROMANN, R., DAMSA, A.: *Digitális pedagógia – A gamifikáció (játékosítás) motivációs eszköztára az oktatásban*. - In. Új Pedagógiai Szemle 2016/3- 4., p. 76-81.

GJERTSEN, E. G. B., GJÆRE, E. A., BARTNES, M., ROCHA FLORES, W.: *Gamification of Information Security Awareness and Training.* - In. 3rd International Conference on Information Systems Security and Privacy., 2017

GRAGG, D.: *A Multi-LEvel Defense Against Social Engineering*, SANS Institute whitepaper, 2003

GRANGER, S.: *Social Engineering fundamentals, Part I: Hacker Tactics.* – SecurityFocus, 2001 (http://www.securityfocus.com/infocus/1527, utolsó elérés: 2008.12.08)

GUENTHER, M.: *Social Engineering – Security Awareness Series.* Előadás, 2001 (http://www.iwar.org.uk/comsec/resources/sa-tools/Social-Engineering. pdf, utolsó elérés: 2008.12.08)

HADNAGY, C.: *Social Engineering: The Art Of Human Hacking*. - Wiley, 2011

HAEUSSINGER, F. J., KRANZ, J. J.: *Information security awareness: Its antecedents and mediating effects on security compliant behavior* – In. Thirty Fourth International Conference on Information Systems, Milan, 2013

HAMARI, J., KOIVISTO, J., SARSA, H.: *Does Gamification Work?* - In. 47th Hawaii International Conference on System Sciences, Hawaii, USA, 2014

HARL, G.: *People Hacking – The Psychology of Social Engineering*. 1997 (http://www.psihoworld.co.ba/The%20Psychology%20of%20Social%20Engineering.pdf, utolsó elérés: 2008.12.08)

HART, S., MARGHERI, A., PACI, F., Vladimiro, S.: *Riskio: A Serious Game for Cyber Security Awareness and Education.* - In. Computers & Security, Volume 95, August 2020

HEIKKINEN, O., SHUMEYKO, J.: *Designing an escape room with the Experience Pyramid model,* 2016 (https://www.theseus.fi/handle/10024/112798, utolsó elérés: 2023.04.09)

HENDRIX, M., AL-SHERBAZ, A., BLOOM, V.: *Game Based Cyber Security Training: are Serious Games suitable for cyber security training?* - In. International Journal of Serious Games, 2016, 3. évfolyam, 1. szám, p. 53-61.

HILL, W. A, Jr., FANUEL, M., YUAN, X., ZHANG, J., SAJAD, S.: *A Survey of Serious Games for Cybersecurity Education and Training.* - In. KSU Proceedings on Cybersecurity Education, Research and Practice, 2020

HUBER, M., KOWALSKI, S., NOHLBERG, M., TJOA, S.: *Towards Automating Social Engineering Using Social Networking Sites.* - Computational Science and Engineering, 2009, 3. szám, p. 117-124.

IRWIN, L.: *Data Breaches and Cyber Attacks in 2022: 408 Million Breached Records.* - IT Governance Blog, 2023 (https://www.itgovernance.co.uk/blog/data-breaches-and-cyber-attacks-in-2022-408-million-breached-records, utolsó elérés: 2023.06.30)

JAIN, A., TAILANG, H., GOSWAMI, H., DUTTA, S., SANKHLA, M. S., KUMAR, R.: *Social Engineering: Hacking a human being through technology.* – In. IOSR Journal of Computer Engineering, 2016, 18. évfolyam, 5. szám, p. 94-100.

JASENSZKY, N., REGÉNYI KUND, M., LIPPAI, Zs.: *A biztonságtudatosság fogalma, fejlődése nemzetbiztonsági, terrorelhárítási és magánbiztonsági szempontból.* – In. Nemzetbiztonsági Szemle, 2021, 9. évfolyam, 4. szám, p. 3-17.

KARAGIANNIS, S., PAPAIOANNOU, T., MAGKOS, E., TSOHOU, A.: *Game-Based Information Security/Privacy Education and Awareness: Theory and Practice.* - In, EMCIS 2020 Conference, Dubai, 2020

KATO, P. M., COLE, S. W., BRADLYN, A. S., POLLOCK, B. H.: *A Video Game Improves Behavioral Outcomes in Adolescents and Young Adults With Cancer: A Randomized Trial.* - In. Pediatrics 2008, 122 (2) p. 305–317.

KHAN, B., ALGHATHBAR, K. S., NABI, S. I, & KHAN, M. K.: *Effectiveness of information security awareness methods based on psychological theories.* - In. African Journal of Business Management, 2011, 5(25), 10862-10868.

KHANDO, K., GAO, S., ISLAM, S. M., SALMAN, A.: *Enhancing employees information security awareness in private and public organisations: A systematic literature review.* – In. Elsevier Computer & Security, 2021, 106, 12267

KIRKPATRICK, Donald L., Kirkpatrick, James D..: *Evaluating Training Programs: TheFour Levels*. – In. Berrett-Koehler Publishers, 2006

KLIMMT, C.: *Serious games and social change: Why they (should) work.* - In. Serious games: Mechanisms and effects, U. Ritterfeld, M. Cody, and P. Vorderer, Eds. Routledge, 2009.

KOBIS, P.: *Human factor aspects in information security management in the traditional IT and cloud computing model.* – In. Operations Research and Decisions, 2021, p. 61-76.

KOLLÁR, Cs., ZAKAR, Á.: *A Social Engineering és a manipulációs technikák és módszerek.* - In. Biztonságtudományi Szemle, 2020. 2. évfolyam, 3. szám, p. 31-46.

KRAUSE, M., MOGALLE, M., POHL, H. & WILLIAMS, J.: *A Playful Game Changer: Fostering Student Retention in Online Education with Social Gamification*. - In. Learning at Scale L@S 2015 (konferencia kiadvány), 2015

KRUGER H.A., KEARNEY W.D.: *A prototype for assessing information security awareness*. - In. Journal of Computer Security, 2006, 25. évfolyam, 4. szám, p. 289-296.

LEANING, M.: *A study of the use of games and gamification to enhance student engagement, experience and achievement on a theory-based course of an undergraduate media degree*. – In. Journal of Media Practice, 2015, 16. évfolyam, 2. szám, p. 155–170

LACZKÓ, A., OROSZI E., D.: *2022, 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)

LEGÁRD, I. (2020). *Célpont vagy! – a közszolgálat felkészítése a kiberfenyegetésekre*. – In. Hadmérnök, 2020, 15. évfolyam, 1. szám, p. 91–105.

LEGÁRD, I.: *Játék a jövőért. Az információbiztonsági tudatosság fejlesztési lehetősége egy gamifikált applikáció segítségével*. – In. Polgári Szemle, 2021, 17. évfolyam, 1–3. szám, p. 358–373.

LEGÁRD, I.: *Információbiztonsági incidenstrendek a közigazgatásban.* – In. Nemzetbiztonsági Szemle, 2023, 11. évfolyam, 1. szám, p. 78-107.

LÖFFLER, E., SCHNEIDER, B., ASPRION, P. M., ZANWAR, T.: *CySecEscape 2.0—A Virtual Escape Room To Raise Cybersecurity Awareness*. – In. International Journal of Serious GamesVolume 8, Issue 1, March 2021, p. 59-70

LONG, J.: *No Tech Hacking.* – Syngress, 2008

MANN, I.: *Hacking the Human*. – Gower, 2008

MAQOUSI, A., BALIKHINA, T., MACKAY, M.: *An effective method for information security awareness raising initiatives.* – In. IJCSIT, 2013, 5. szám, p. 63-72.

MÁRKUS D., RÁCZ, I.: *Munkahelyi képzés hatékonyságának mérése egy nagyvállalat példáján*. – In. REISINGER, A., HAPP, É., IVANCSÓNÉ HORVÁTH, Zs., BUICS, L. (szerk.) "Sport - Gazdaság - Turizmus" Kautz Gyula Emlékkonferencia 2017. június 8., konferenciakötet 2018 ISBN 978-615-5837-18-0

MCGONIGAL, Jane.: *Reality Is Broken: Why Games Make Us Better and How They Can Change the World*. – Penguin Books, 2011

MITNICK, Kevin D.; SIMON, William L.: *The Art of Deception: Contolling the Human Element of Security.* – USA, Wiley, 2003

NEMESLAKI, A., SASVÁRI, P.: *Empirical Analysis of Information Security Awareness in the Business and Public Sectors in Hungary*. – In. Central and Eastern European e|Dem E|Gov Days 2015, p. 405-418

NICHOLSON, S.: *Creating engaging escape rooms for the classroom*. – In Childhood Education, 2008, 94(1), p. 44–49

OROSZI, E. D.: *Social Engineering – Az emberi erőforrás, mint az információbiztonság kritikus tényezője*, Szakdolgozat, Budapesti Corvinus Egyetem, Budapest, 2008

OROSZI, E. D.: *Social Engineering audit – A biztonságtudatosság tesztelése*, Szakdolgozat, Budapesti Corvinus Egyetem, Budapest, 2011

OROSZI, E.: *A humán erőforrás védelme – védelem a humán erőforrás ellen*. - In. LEITOLD, F. (szerk.) Információ és adatvédelem a közigazgatásban, 2014, p. 27-37.

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

OROSZI, E. D.: *Biztonságtudatossági szabaduló szoba, mint a felhasználók biztonságtudatosságának új fejlesztési eszköze*, ISACA második szerdai előadás, Budapest, 2017.05.10

OROSZI, E. D.: *Social Engineering technikák.* - In. DEÁK, V. (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, E. D.: *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, E. D.: *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, E. D.: *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, E. D.: *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, E. D.: *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, E. D.: *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, E. D.: *A biztonság nem játék... de játszva fejleszthető!,* Hétpecsét Információvédelem Menedzselése CI. Szakmai Fórum, Budapest, 2022.05.18

OROSZI, E. D.: *Gamifikáció az információbiztonságban.* Silent Signal Kft, szakértői képzés tananyag, 2023

PACSI, D., SZABÓ, Z.: *A gamifikáció fejlődése és a magyar gamifikációs trend alakulása.* - In. Studia Munkdi – Economica, Vol. 4. No. 1., 2017, p. 57-68.

PAPAIOANNOU, T., TSOHOU, A., BOUNIAS, G., KARAGIANNIS, S.: *A Constructive Approach for RaisingInformation Privacy Competences: The Caseof Escape Room Games.* – In. KATSIKAS, S., FURNELL, S. (szerk.): 2022: TrustBus, Springer Nature Switzerland AG 2022, LNCS 13582, p. 33–49, 202

PATEL, C. S.: *E-Learning: Concept, Features and it's Types*- - In. International Journal of Research in Humanities & Social Sciences, Vol. 4, Issue: 1, January, 2016 ISSN:(P) 2347-5404 ISSN:(O)2320 771X 8

PATRÍCIO, R., MOREIRA, A. C., ZURLO, F.: *Gamification approaches to the early stage of innovation.* – In. Creativity and Innovation Management, 2018, Vol. 27., Issue 4, p. 499-511.

POÓR, J., KOLLÁR P., KOVÁCS, I. É., SUHAJDA, Cs. J., FARKAS, P., TÓTH, K., SZABÓ, K.: *Szervezeti képzések gyakorlata Magyarországon a nemzetközi adatok tükrében.* – In. Vezetéstudomány / Budapest Management Review, 2018, XLIX. évfolyam, 10 –11. szám, ISSN 0133-0179

ROCHA FLORES, W., EKSTEDT, M.: *Shaping intention to resist social engineering through transformational leadership, information security culture and awareness.* – In. Computers and Security, 2016, 59, p. 26-44.

SADIQ, A., ANWAR, M., BUTT, R. A., MASUD, F., SHAHZAD, M. K., NASEEM, S., YOUNAS, M.: *A review of phishing attacks and countermeasures for internet of things-based smart business applications in industry 4.0.* – In. Human Behavior and Emerging Technologies, 2021, 3, p. 854-864.

SAJTOS, L. és MITEV, A.: *SPSS Kutatási és adatelemzési kézikönyv.* - Alinea Kiadó, 2007

SCHNEIDER, B., ZANWAR, T.: *CySecEscape – Escape Room Technique to Raise Cybersecurity Awareness in SMEs.* – In. The Future of Education International Conference, edited by Pixel, 2020

SCHNEIER, B.: *Secrets and Lies*. – Wiley, 2000

SCHOLEFIELD, S., SHEPHERD, L. A.: *Gamification Techniques for Raising Cyber Security Awareness.* – In. MOALLEM, A. (szerk.), HCI for Cybersecurity, Privacy and Trust, HCI-CPT 2019, Held as Part of HCI International 2019, Orlando, Florida, USA, July 26-31, 2019, Springer.

SINGLEY, B. D., HURST, C.: *Comparing E-Learning, Tele-Classes, and Live Trainings: An Analysis of Cost and Training Effectiveness*, Whitepaper, 2011 https://www.menexcel.com/wp-content/uploads/2014/06/ProvidenceStudyWhitePaper-Jan2011.pdf (utolsó elérés: 2023.03.26)

SIPONEN, T., M.: *A conceptual foundation for organizational information security awareness*. - In. Information Management & Computer Security, 2000, Volume 8, Issue 1, p. 31-41.

SITZMANN, T., KRAIGER, K., STEWART, D., WISHER, R.: *The comparative effectiveness of Web-based and classroom instruction: A meta-analysis.* – In. Personnel Psychology, 2006, 59, p. 623–64.

TARJÁN, G.: *Az információbiztonsági tudatosság érettségi szintjének mérése szervezetekben,* doktori értekezés, 2020

THOMPSON, M., IRVINE, C.: *Active Learning with the CyberCIEGE Video Game*. 2011, https://calhoun.nps.edu/handle/10945/40296 (utolsó elérés: 2021.08.08)

TSCHAKERT, K. F., NGAMSURIYAROJ, S.: *Effectiveness of and user preferences for security awareness training methodologies*. – In. Heliyon 2019, Volume 5, Issue 6

TSOHOU, A., KARYDA, M., KOKOLAKIS, S., KIOUNTOUZIS, E.: *Analyzing information security awareness through networks of association.* - In: International Conference on Trust, Privacy and Security in Digital Business. Springer; 2010. p. 227–37.

VAN DEN BOER, P: *Introduction to Gamification.* Whitepaper. 2019. https://cdu.edu.au/olt/ltresources/downloads/whitepaper-introductiontogamification-130726103056-phpapp02.pdf (utolsó elérés: 2019.01.15.)

WEN, Z. A., LIN, Z., CHEN, R., ANDERSEN, E.: *What.Hack: Engageing Anti-Phishing Training Through a Role-playing Phishing Simulation Game* – In. CHI 2019 Conference, Glasgow, Scotland, UK, 2019

WILSON, M. HASH, J.: *NIST 800-50 Building an Information Technology Security Awareness and Training Program*, 2003

ZICHERMANN, Gabe és LINDER, Joselin: *Gamification – Az üzleti játékok forradalmasítása*, - Miskolc, Z-Press Kiadó Kft., 2013

9.2. WEBES HIVATKOZÁSOK

Adam Shostack Tabletop Security Games and Cards, https://adam.shostack.org/games.html (utolsó elérés: 2021.08.08)

Anti-Phishing Phil https://cups.cs.cmu.edu/antiphishing_phil/ (utolsó elérés: 2021.08.08)

Aware https://aware.eccouncil.org (utolsó elérés: 2021.08.08)

CGI Cyber Escape https://www.cgi.com/uk/en-gb/cyberescape (utolsó elérés: 2023.03.26)

Control-Alt-Hack http://www.controlalthack.com (utolsó elérés: 2021.08.08)

Cre8tive Cyber Security Escape Room https://www.tes.com/teaching-resource/cyber-security-escape-room-12733865 (utolsó elérés: 2023.03.26.)

CyberCIEGE https://nps.edu/web/c3o/cyberciege (utolsó elérés: 2021.08.08)

Cyex Awareness Platform https://cyex.io/cyex-platform/ (utolsó elérés: 2023.03.26)

DEVPOST Cyber Security Escape Room, https://devpost.com/software/cyber-security-escape-room-menx73 (utolsó elérés: 2023.03.26)

[d0x3d!] https://d0x3d.com/d0x3d/welcome.html (utolsó elérés: 2021.08.08)

eLearning Industry kutatás: https://financesonline.com/gamification-statistics (utolsó elérés: 2021.08.08)

ENISA – AR-in-a-Box: https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-raising-in-a-box (utolsó elérés: 2023.06.30)

ENISA Threat Landscape 2022: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (utolsó elérés: 2023.06.30)

Enter – IT Security Game https://entergame.ch/de (utolsó elérés: 2021.08.08)

Fandi, A. "Cybersecurity Is More Than Bits and Bytes, It's Also People and Process," LinkedIn, 30 September 2019, https://www.linkedin.com/pulse/cybersecurity-more-than-bits-bytes-its-also-people-process-fandi (utolsó elérés: 2021.08.08)

Információbiztonsági Helyzetkép 2019, ISACA Budapest Chapter, https://engage.isaca.org/budapestchapter/informaciobiztonsagi-helyzetkep (utolsó elérés: 2023.03.26)

Információbiztonsági Helyzetkép 2021, ISACA Budapest Chapter, https://engage.isaca.org/budapestchapter/informaciobiztonsagi-helyzetkep (utolsó elérés: 2023.03.26)

Infosequre Cyber Security Escape Room, https://www.infosequre.com/security-awareness-escape-room (utolsó elérés: 2023.03.26)

Living Security CyberEscape Online https://www.livingsecurity.com/security-awareness-training-games/cyberescape-cybersecurity-escape-room (utolsó elérés: 2023.03.26)

Microsoft Elevation of Privilege https://www.microsoft.com/en-us/SDL/adopt/eop.aspx (utolsó elérés: 2023.04.03)

OWASP Cornucopia https://owasp.org/www-project-cornucopia (utolsó elérés: 2021.08.08)

Pro Bono – Közigazgatási Továbbképzési Intézet: https://eib.uni-nke.hu (utolsó elérés: 2023.06.30)

PurpleSec Cyber Security Statistics https://purplesec.us/resources/cyber-security-statistics/ (utolsó elérés: 2021.03.01)

Riskio https://www.riskio.co.uk (utolsó elérés: 2021.08.08)

Silent Signal Awareness Game https://silentsignal.hu/termekeink#ag (utolsó elérés: 2023.04.03)

TalentLMS Gamification ar Work felmérés, https://www.talentlms.com/blog/gamification-survey-results (utolsó elérés: 2021.08.08)

Thales Cyber Escape Room https://www.thalesgroup.com/en/cyber-escape-room (utolsó elérés: 2023.03.26)

Thinkfun: Hacker https://www.thinkfun.com/learn-coding/hacker (utolsó elérés: 2023.04.03)

TPT Cyber Security Ecape Room https://www.teacherspayteachers.com/Product/Cyber-Security-Escape-Room-8528112 (utolsó elérés: 2023.04.03)

Verizon Data Breach Investigations Report 2020, https://www.cisecurity.org/wp-content/uploads/2020/07/The-2020-Verizon-Data-Breach-Investigations-Report-DBIR.pdf (utolsó elérés: 2021.03.04)

Verizon Data Breach Investigations Report 2022, https://www.verizon.com/business/resources/T178/reports/dbir/2022-dbir-data-breach-investigations-report.pdf, utolsó elérés: 2023.06.30.)

9.3. JOGSZABÁLYOK, SZABVÁNYOK ÉS AJÁNLÁSOK

2003. évi C. törvény az elektronikus hírközlésről

2007. évi LXXXVI. törvény a villamos energiáról

2007. évi CXXXVIII. törvény a befektetési vállalkozásokról és az árutőzsdei szolgáltatókról, valamint az általuk végezhető tevékenységek szabályairól

2008. évi XL. törvény a földgázellátásról

2011. évi CCIX. törvény a víziközmű-szolgáltatásról

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról és végrehajtási rendeletei

2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról

2014. évi LXXXVIII. törvény a biztosítási tevékenységről

41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről végrehajtási rendelet

42/2015. (III. 12.) Korm. rendelet a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről

A Magyar Nemzeti Bank 8/2020. (VI.22.) számú ajánlása az informatikai rendszer védelméről

A Magyar Nemzeti Bank 12/2020. (XI.6.) számú ajánlása a távmunka és távoli hozzáférés informatikai biztonsági követelményeiről

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete, (2016. április 27.), a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (GDPR)

AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE a pénzügyi ágazat digitális működési rezilienciájáról és az 1060/2009/EK rendelet, a 648/2012/EU rendelet, a 600/2014/EU rendelet, valamint a 909/2014/EU rendelet módosításáról (DORA rendelet)

AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2555 IRÁNYELVE az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv)

CISA – Cybersecurity Awareness Month Publications, https://www.cisa.gov/resources-tools/resources/cybersecurity-awareness-month-publications (utolsó elérés: 2023.03.26)

CISA – Cybersecurity Awareness Month Partner Toolkit, https://www.cisa.gov/sites/default/files/publications/Cybersecurity%2520Awareness%2520Month_Partner%2520Toolkit_Final.pdf (utolsó elérés: 2023.03.26)

ISO/IEC 27001:2013 Information technology. Security techniques. Information security management systems. Requirements (2013)

NIST SP 800-16 Rev. 1. (Draft) A Role-Based Model for Federal Information Technoligy/Cybersecurity Training (3rd Draft), https://csrc.nist.gov/publications/detail/sp/800-16/rev-1/draft (utolsó elérés: 2023.03.26)

NIST 800-53 Revision 5. Security and Privacy Controls for Information Systems and Organizations, (2020) https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (utolsó elérés: 2023.03.26)

SANS – Leveraging the SANS Security Awareness Maturity Model to Effectively Manage Human Risk (e-book), https://go.sans.org/lp-ebook-maturity-model (utolsó elérés: 2023.03.26)

SANS – Útmutató a biztonságtudatossági intézkedések bevezetéséhez – A biztonságos otthoni munkavégzés, https://www.sans.org/security-awareness-training/work-home-guide/ (utolsó elérés: 2023.03.26)

PCI Security Standards Council Security Awareness Program Special Interest Group, , 2014, Information Supplement: Best Practices for Implementing a Security Awareness Program, https://listings.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf (utolsó elérés: 2023.03.26)

10. 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.

11. ÁBRÁK, DIAGRAMOK, KÉPEK ÉS TÁBLÁZATOK JEGYZÉKE

11.1.ÁBRÁK

11.2.DIAGRAMOK

11.3.KÉPEK

11.4.TÁBLÁZATOK

12. MELLÉKLETEK

1. számú melléklet: A kutatásban vizsgált 10 biztonságtudatossági ismeret megjelenése a kutatás során vizsgált, különböző biztonságtudatossági programokban.

2. számú melléklet: Kérdőív a biztonságtudatossági programon való részvétel előtt (K1)

3. számú melléklet: Kérdőív közvetlenül a biztonságtudatossági programon való részvételt követően (K2)

4. számú melléklet: Kérdőív 1 hónappal a biztonságtudatossági programon való részvételt követően (K3)

5. számú melléklet: Biztonságtudatossági ismeretek arányának változása vizsgált típusonként közvetlenül a programot követően

6. számú melléklet: Kiegészítő diagramok

1. számú melléklet

A kutatásban vizsgált 10 biztonságtudatossági ismeret megjelenése a kutatás során vizsgált, különböző biztonságtudatossági programokban.

Ismeret/módszer	***Személyes oktatás Online oktatás***	***e-Learning***	***Kampányelemek***	***Szabadulószoba***	***Társasjáték***
Tiszta asztal	Mit rejthet az íróasztalom? (19. slide)	Mit rejthet az íróasztalom? (15. slide)	Poszter Memóriajáték	Információk az íróasztalon	Tiszta asztal kártya
Tiszta képernyő	Mit rejthet az íróasztalom? (19. slide)	Mit rejthet az íróasztalom? (15. slide)	Poszter Memóriajáték	Lezárt, jelszavas munkaállomás az íróasztalon	Tiszta képernyő kártya
Kulcsok, kártyák	Illetéktelen bejutás az épületbe (16-17. slide)	Illetéktelen bejutás az épületbe (13. slide) Teszt (24. slide)	Memóriajáték	Belépőkártya ottfelejtve az íróasztalon	Belépőkártya, Iroda zárása kártyák
Hardver eszközök	Mit tehet egy, az épületbe bejutott támadó? (18. slide) Mit rejthet az íróasztalom? (20. slide)	Mit tehet egy támadó az épületben? (14. slide) Mit rejthet az íróasztalom? (15. slide)	Memóriajáték	Titkosított pendrive, Kensington nélküli laptop	Kensington zár, Ismeretlen eszközök, Token mindig nálam kártyák
Jelszavak	Mit rejthet az íróasztalom? (20. slide) Ha már ismét a jelszavaknál járunk (31. slide)	Mit rejthet az íróasztalom? (15. slide) Ha már a jelszavaknál járunk (21. slide) Teszt (24. slide)	Poszter Jelszókódoló Memóriajáték	Jelszó képzési konvenció felírva, jelszó a jegyzetek közé felírva, jelszó e-mail-ben küldve	Erős, nehezen kitalálható jelszó, Csak általam ismert jelszó, Jelszószéf kártyák
Iratmegsemmisítés	Információk a szemetesből (14-15. slide)	Információk a szemetesből (12. slide)	Poszter Memóriajáték	Belső információk a kukában	Iratmegsemmisítő kártya
Adathalászat	Adathalászat (29-30. slide)	Adathalászat (20. slide)	Poszter Memóriajáték	Adathalász megkeresés az e-mail-ek között (időbüntetés)	Gyanús linkek és tartáblázatban kerül bemutatásra.talmak,

Ismeret/módszer	*Személyes oktatás*	*Online oktatás*	*e-Learning*	*Kampányelemek*	*Szabadulószoba*	*Társasjáték*
						Gyanús weboldalak és tartalmak kártyák
Vírusvédelem	Kártékony kódok terjesztése (27-28. slide)		Kártékony kódok, vírusvédelem (19. slide) Teszt (24. slide)	Hírlevél Poszter Kameratakaró Memóriajáték	Gyanús csatolmány az e-mail-ek között (időbüntetés)	Vírusvédelem, Gyanús mellékletek, Gyanús linkek és tartalmak, Gyanús weboldalak és tartalmak, Ismeretlen eszközök kártyák
Közösségi média	Információgyűjtés (12-13. slide)		Információgyűjtés (11. slide)	Rejtvény Poszter Memóriajáték	Facebook-on elérhető információk gyűjtése	Ismeretlenek a közösségi médiában, Nyilvános megosztás kerülése kártyák
Telefon és okos eszközök	Telefonon keresztüli megtévesztés (23-24. slide) Kártékony kódok terjesztése (27-28. slide)		Telefonon keresztüli megtévesztés (17. slide)	Hírlevél Memóriajáték	Okostelefon PIN kód megszerzés, mobil applikációk	Jel/számkód a mobilon, Ellenőrzöm a hívófél kilétét kártyák

3. táblázat: A kutatásba bevont biztonságtudatossági ismeretek megjelenése a különböző programokban (forrás: saját szerkesztés)

2. számú melléklet

Kérdőív a biztonságtudatossági programon való részvétel előtt (K1)

Biztonságtudatosság mérése és fejlesztése kutatás
Felhasználói kérdőív a program ELŐTT

Program: .....

Azonosító: _ _ _ _ _ _ _ _ _ _ _ _ _ _
(Mai dátum 8 karakter, telefonszám utolsó 3 számjegye, születésnap 2 számjegye)
Szervezeti egység:.....

I. Általános kérdések

Válaszadó neme:

- ☐ Férfi
- ☐ Nő

Válaszadó kora:

- ☐ 20 év alatt
- ☐ 20-29 év
- ☐ 30-39 év
- ☐ 40-49 év
- ☐ 50-59 év
- ☐ 60 év felett

Válaszadó beosztása:

- ☐ Felsővezető
- ☐ Középvezető
- ☐ Alkalmazott
- ☐ Külső munkavállaló

II. Biztonságtudatossági képzésre vonatkozó kérdések

Mikor vett részt utoljára biztonságtudatossági oktatáson, tréningen, e-Learning tanfolyamon? (Kérjük, egy választ jelöljön!)

- ☐ Még sosem vettem részt ilyen jellegű képzésen.
- ☐ Több, mint 5 éve vettem részt ilyen jellegű képzésen.
- ☐ Csak az elmúlt 3-5 évben vettem részt ilyen jellegű képzésen.
- ☐ Csak az elmúlt 2 évben vettem részt ilyen jellegű képzésen.
- ☐ Az elmúlt 1 évben részt vettem ilyen jellegű képzésen.

Az előző pontban teljesített képzés mely kategóriába tartozott az alábbiak közül? (Több választ is megjelölhet!)

- ☐ Tantermi oktatás, személyes előadás
- ☐ Online oktatás, előadás
- ☐ E-Learning tanfolyam
- ☐ E-mail-es vagy intranetes tájékoztatás
- ☐ Biztonságtudatossági kampány (plakátok, ajándéktárgyak, játékok)
- ☐ Gamifikációs megoldás

Mely típusú képzéseket, tudatosító elemeket részesítené előnyben az alábbiak közül, melyeket venné igénybe? (Több választ is megjelölhet!)

- ☐ Tantermi oktatás, személyes előadás
- ☐ Online oktatás, előadás
- ☐ E-Learning tanfolyam
- ☐ E-mail-es vagy intranetes tájékoztatás
- ☐ Biztonságtudatossági kampány (plakátok, ajándéktárgyak)
- ☐ Kvízjátékok, rejtvények biztonságtudatossági témában
- ☐ Biztonságtudatossági szabadulószoba
- ☐ Biztonságtudatossági társas, kártya és egyéb játékok
- ☐ Biztonságtudatosságot fejlesztő mobil applikáció
- ☐ Biztonságtudatosságot fejlesztő online játék

III. Biztonságtudatossági ismeretekre vonatkozó kérdések

Kérjük, írja le, hogy milyen információbiztonsági szabályok, előírások, ajánlások jutnak az eszébe, például amennyiben egy újonnan érkező kollégának kellene elmondania, mit mondana, mire figyeljen, hogyan legyen biztonságtudatos a munkavégzés során, vagy akár otthon.

3. számú melléklet

Kérdőív közvetlenül a biztonságtudatossági programon való részvételt követően (K2)

Biztonságtudatosság mérése és fejlesztése kutatás
Felhasználói kérdőív a program UTÁN

Programelem: .....

Azonosító: _ _ _ _ _ _ _ _ _ _ _ _ _ _
(Mai dátum 8 karakter, telefonszám utolsó 3 számjegye, születésnap napjának 2 számjegye)

Mennyire érzi **hasznosnak** a programot, amin részt vett, hogy érzi, bővültek a biztonságtudatossági ismeretei? (Kérjük, egy választ jelöljön!)

- ☐ Egyáltalán nem tartom hasznosnak, felesleges időráfordítás volt, minden előírás ismerős volt, amivel találkoztam a program alatt.
- ☐ Voltak benne hasznos elemek, újdonságok, de azokat nem tartom fontosnak vagy relevánsnak.
- ☐ Voltak benne olyan hasznos elemek, újdonságok, melyeket alkalmazni is fogok a jövőben.
- ☐ Kifejezetten hasznosnak tartom, még akkor is, ha egy része a témának ismerős volt.

Mennyire volt **élvezetes** a program? Kérjük, egy választ jelöljön!)

- ☐ Egyáltalán nem élveztem, unalmas volt.
- ☐ Részt vettem, mert kötelező, de átlagosnak eseménynek tartottam.
- ☐ Jobban élveztem, mint más hasonló jellegű eseményeket.
- ☐ Kifejezetten élveztem, szívesen részt vennék hasonlón máskor is.

Javasolná-e a programot, melyen részt vett a kollégáinak?

- ☐ Igen
- ☐ Nem
- ☐ Nem tudom/nem szeretnék válaszolni

Melyik programon venne még részt szívesen? (Több választ is megjelölhet!)

- ☐ Tantermi oktatás, személyes előadás
- ☐ Online oktatás, előadás
- ☐ E-Learning tanfolyam
- ☐ E-mail-es vagy intranetes tájékoztatás
- ☐ Biztonságtudatossági kampány (plakátok, ajándéktárgyak)
- ☐ Kvízjátékok, rejtvények biztonságtudatossági témában
- ☐ Biztonságtudatossági szabadulószoba
- ☐ Biztonságtudatossági társas, kártya és egyéb játékok
- ☐ Biztonságtudatosságot fejlesztő mobil applikáció
- ☐ Biztonságtudatosságot fejlesztő online játék

IV. Biztonságtudatossági ismeretekre vonatkozó kérdések

Kérjük, most is írja le, hogy milyen információbiztonsági szabályok, előírások, ajánlások jutnak az eszébe, például amennyiben egy újonnan érkező kollégának kellene elmondania, mit mondana, mire figyeljen, hogyan legyen biztonságtudatos.

4. számú melléklet

Kérdőív 1 hónappal a biztonságtudatossági programon való részvételt követően (K3)

Biztonságtudatosság mérése és fejlesztése kutatás
Felhasználói kérdőív a program UTÁN 1 HÓNAPPAL

Programelem: .....

Azonosító: _ _ _ _ _ _ _ _ _ _ _ _ _ _
(Mai dátum 8 karakter, telefonszám utolsó 3 számjegye, születésnap 2 számjegye)

Részt vett-e az elmúlt hónapban más biztonságtudatossági programon?

- ☐ Nem
- ☐ Igen, a következőn: _____

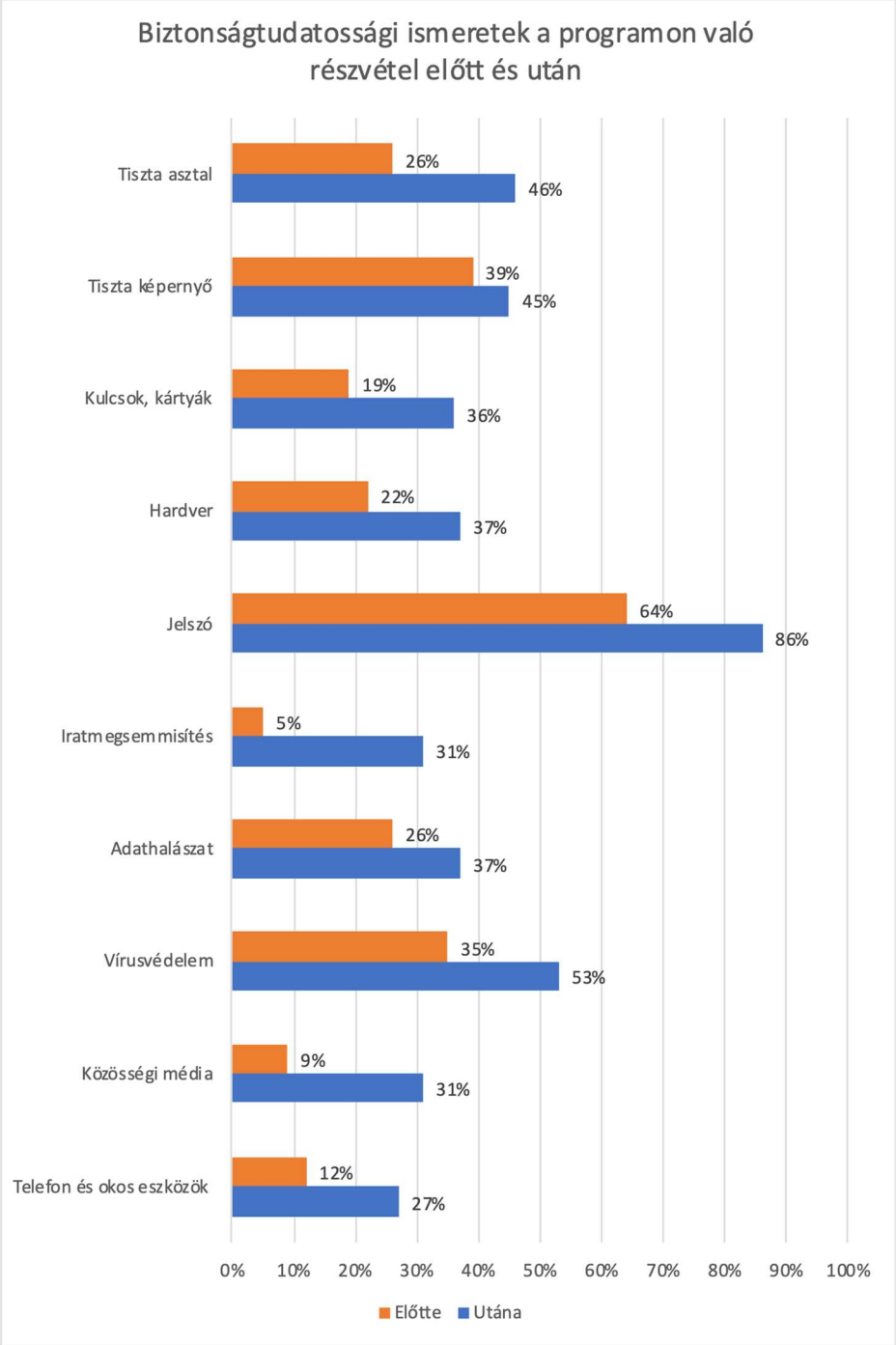
V. Biztonságtudatossági ismeretekre vonatkozó kérdések

Kérjük, most is írja le, hogy milyen információbiztonsági szabályok, előírások, ajánlások jutnak az eszébe, például amennyiben egy újonnan érkező kollégának kellene elmondania, mit mondana, mire figyeljen, hogyan legyen biztonságtudatos. (Kérjük, a korábban írt ismereteket is írja le legalább címszavakban, amennyiben ilyen is eszébe jut!)

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

5. számú melléklet

Biztonságtudatossági ismeretek arányának változása vizsgált típusonként közvetlenül a programot követően (forrás: saját szerkesztés)

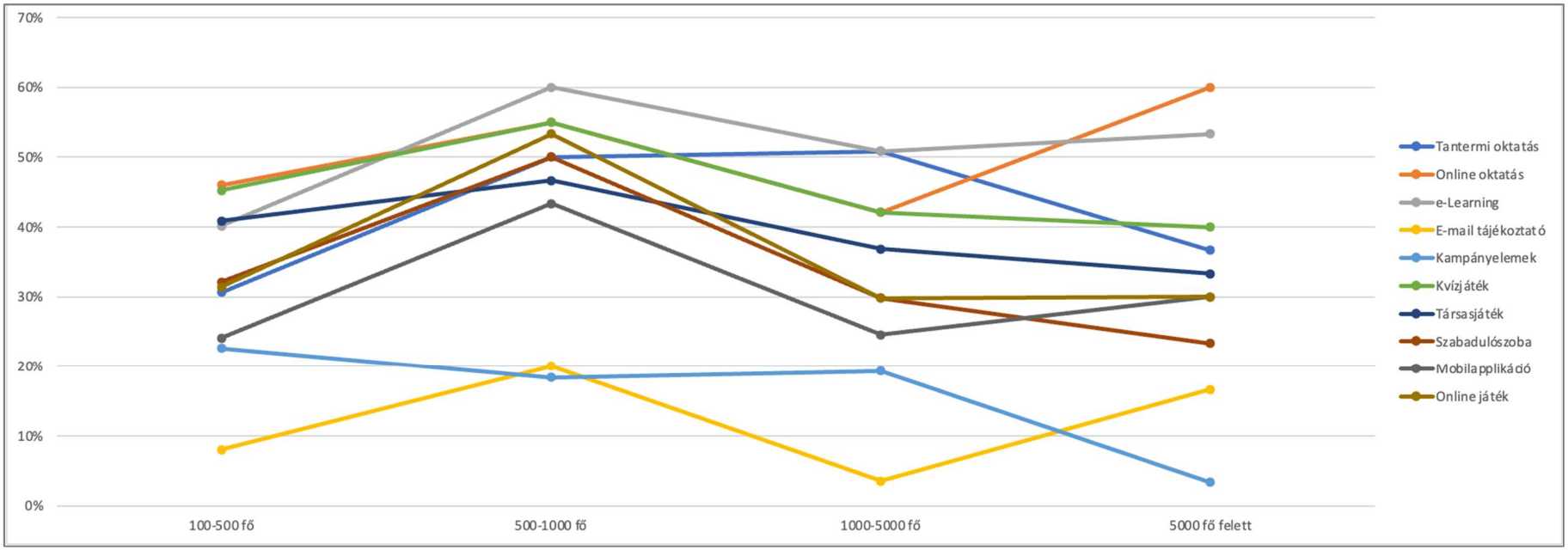


6. számú melléklet

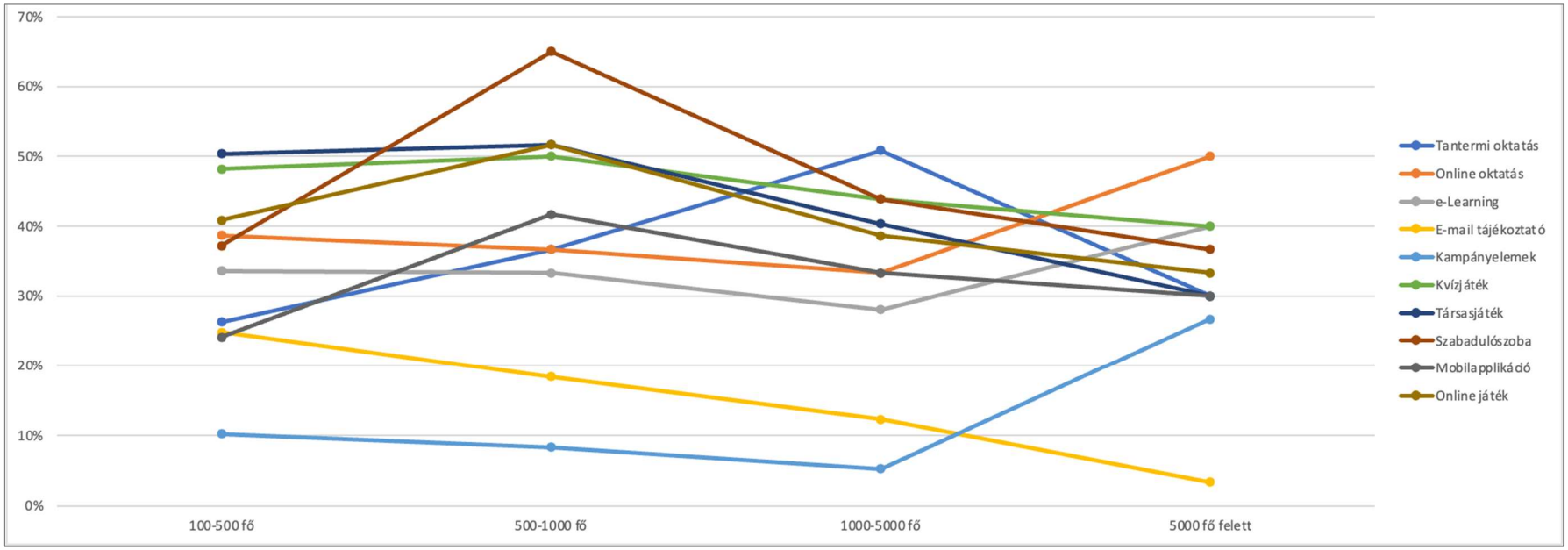
Kiegészítő diagramok.

- *A kutatásban vizsgált képzési módszerek preferencia változása a szervezetek mérete szerint, a programon való részvétel előtt (forrás: saját szerkesztés)*
- *A kutatásban vizsgált képzési módszerek preferencia változása a szervezetek mérete szerint, a programon való részvételt követően (forrás: saját szerkesztés)*
- *A kutatásban vizsgált képzési módszerek preferencia változása korosztály szerint, a programon való részvétel előtt (forrás: saját szerkesztés)*
- *A kutatásban vizsgált képzési módszerek preferencia változása korosztály szerint, a programon való részvételt követően (forrás: saját szerkesztés*

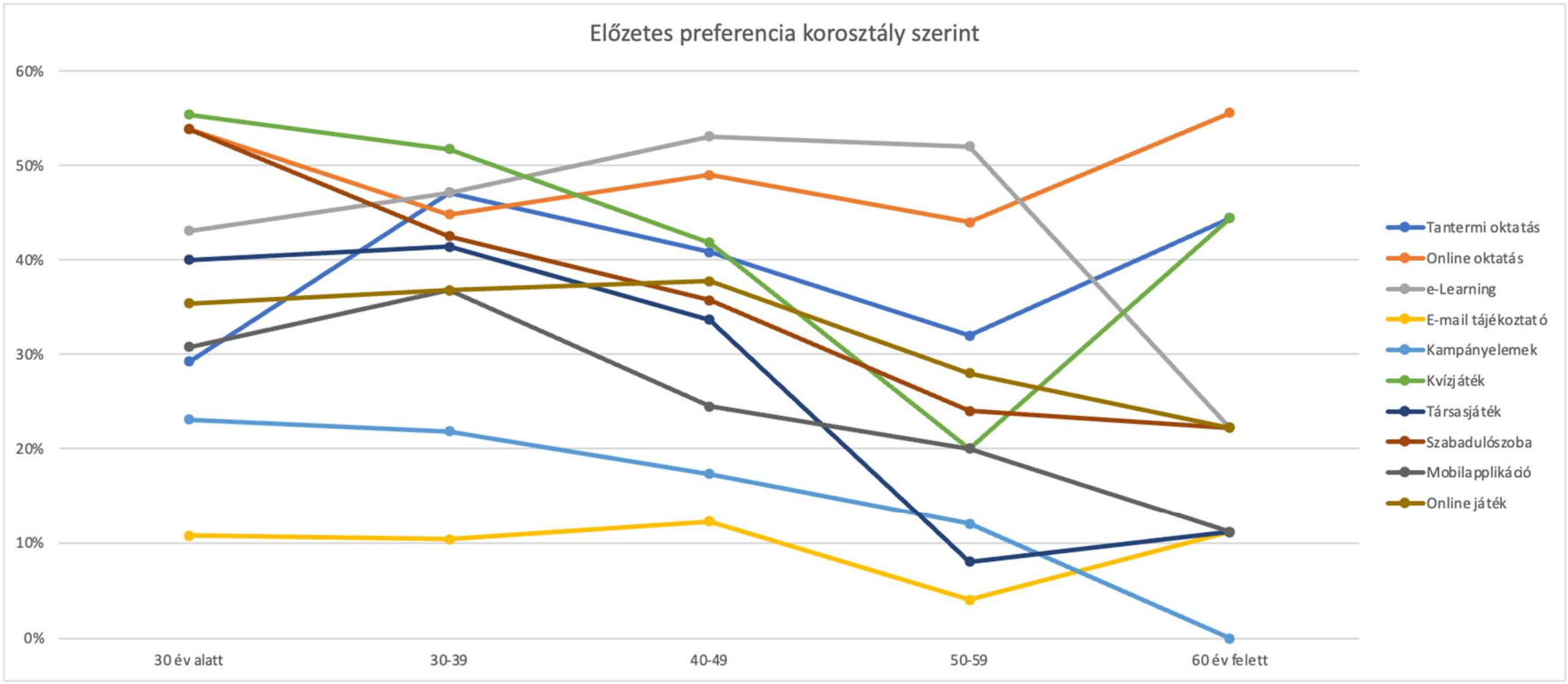
A kutatásban vizsgált képzési módszerek preferencia változása a szervezetek mérete szerint, a programon való részvétel előtt (forrás: saját szerkesztés)



A kutatásban vizsgált képzési módszerek preferencia változása a szervezetek mérete szerint, a programon való részvételt követően (forrás: saját szerkesztés)



A kutatásban vizsgált képzési módszerek preferencia változása korosztály szerint, a programon való részvétel előtt (forrás: saját szerkesztés)



A kutatásban vizsgált képzési módszerek preferencia változása korosztály szerint, a programon való részvételt követően (forrás: saját szerkesztés)